Cisco Prime Infrastructure 2.0 Quick Start Guide

1 About This Guide, page 3
2 Product Overview, page 3
3 Key Features, page 4
4 About Cisco Prime Infrastructure Licensing, page 7
5 Pre-Installation Tasks, page 8
6 Upgrading Cisco Prime Infrastructure, page 18
7 Installing Cisco Prime Infrastructure, page 22
8 Getting Started, page 25
9 Installing the Plug and Play Gateway on Standalone Servers, page 25
10 Removing the Prime Infrastructure Virtual Appliance, page 31
11 Navigation and Documentation Reference, page 31
12 Reinstalling Cisco Prime Infrastructure on a Physical Appliance, page 32
13 Related Documentation, page 32
14 Obtaining Documentation and Submitting a Service Request, page 32

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: CISCO PRIME INFRASTRUCTURE

IMPORTANT-READ CAREFULLY: This Supplemental License Agreement ("SLA") contains additional limitations on the license to the Software provided to Customer under the End User License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the End User License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence.

By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download or otherwise use the Software.

ADDITIONAL LICENSE RESTRICTIONS:

- Installation and Use. The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product. Customer may install and use the following Software components:
  - Cisco Prime Infrastructure: May be installed on a server in Customer's network management environment.

  For each Software license granted, customers may install and run the Software on a single server to manage the number of network devices and codecs specified in the license file provided with the Software, or as specified in the Software License Claim Certificate. Customers whose requirements exceed the network device and codec limits must purchase upgrade licenses or additional copies of the Software. The network device and codec limits are enforced by license registration.
- Reproduction and Distribution. Customers may not reproduce nor distribute the Software.

DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Refer to the Cisco Systems, Inc. End User License Agreement.

1 About This Guide

This guide explains how to install Prime Infrastructure 2.0.

This guide is intended for administrators who configure, monitor, and maintain Prime Infrastructure, and troubleshoot problems that may occur. These administrators must be familiar with VMware OVA applications, virtualization concepts and virtualized environments.

For detailed information about configuring and managing this product, see the *Cisco Prime Infrastructure 2.0 Administrator Guide* and the *Cisco Prime Infrastructure 2.0 User Guide*.

2 Product Overview

Cisco Prime Infrastructure provides a single integrated solution for comprehensive lifecycle management of the wired/wireless access, campus, and branch networks, and rich visibility into end-user connectivity and application performance assurance issues. Cisco Prime Infrastructure accelerates the rollout of new services, secure access and management of mobile devices, making “Bring Your Own Device” (BYOD) a reality for corporate IT. Tightly coupling client awareness with application performance visibility and network control, Cisco Prime Infrastructure helps ensure uncompromised end-user quality of experience. Deep integration with the Cisco Identity Services Engine (ISE) further extends this visibility across security and policy-related problems, presenting a complete view of client access issues with a clear path to solving them.

Prime Infrastructure is organized into a lifecycle workflow that includes the following high-level task areas:

- Design—The design phase focuses on the overall design of feature or device patterns or *templates*. The design area is where you create reusable design patterns such as configuration templates. Prime Infrastructure provides predefined templates, but you can also create your own. These patterns and templates are intended for use in the deployment phase of the lifecycle.
- Deploy—The deployment phase focuses on deploying previously defined designs or *templates* into your network. The deploy area is where you specify how to deploy features, making use of the templates created in the design phase. The deploy phase allows you to push configurations defined in your templates to one or many devices.
- Operate—The Operate area is where you monitor your network on a daily basis, as well as perform other day-to-day or ad hoc operations relating to network device inventory and configuration management. The Operate tab contains dashboards, the Device Work Center, and the tools you need for day-to-day monitoring, troubleshooting, maintenance, and operations.
- Report—Prime Infrastructure also provides reports that you can use to monitor the system and network health as well as troubleshoot problems. The Prime Infrastructure Report Launchpad provides report access and scheduling for all types of reporting functions.
- Administration—The Administration area is where you specify system configuration settings, manage access control, and specify data collection settings.
- Workflows—Use workflows to set up Plug and Play to configure new devices and allow any newly connected Cisco IOS device to be discovered, inventoried, and configured. Workflows also allow you to set up switches or wireless LAN controllers after they have been added to Prime Infrastructure.

3 Key Features

Table 1 details the key features of Prime Infrastructure.

Table 1 Prime Infrastructure: Key Features

Feature	Benefits
Global Platform	
Operational Efficiency	• Streamlined workflows that facilitate design, deploy, and operate lifecycle tasks which align with user roles. • Contextual dashboards and 360 views display only the most relevant information for fast and efficient troubleshooting • Flexible user experience accommodates novice and experienced IT administrators, reducing the investment in multiple tools • Cisco Prime Infrastructure Toolbar client widget for real-time at-a-glance updates of network status from your browser or Microsoft Outlook clients. • Cisco Prime Infrastructure mobile application for Apple iOS devices enables fingertip access to view, troubleshoot, and resolve network issues anywhere and anytime.
Integrated Cisco Best Practices	• Integration with Cisco knowledge base to ensure optimal service and support, product updates, best practices and reports to improve network availability • Support of new Cisco platforms and technologies the day they ship • Smart Interactions streamline service request creation reducing time required to fix problems
Improved Operations	• Flexible virtual machine and physical appliance solutions provide cost effective, easy to install options for small to global enterprise class networks • Built-in high availability maximizes uptime for services delivery and improves operational efficiency
Administration	• Role-based access control provides flexibility to segment the network into one or more virtual domains controlled by a single Cisco Prime Infrastructure platform. Virtual domains help deploy both large, multisite networks and managed services • Flexible AAA allow for local, RADIUS, TACACS+, or Single Sign-on options

Table 1 Prime Infrastructure: Key Features (continued)

Feature	Benefits
Lifecycle View	
Converged Management	Single-pane-of-glass for managing complete end-to-end infrastructure management no need for multiple tools, reduces operating expenses and training costs
Complete Lifecycle Management	• Day 1 Support of new Cisco devices and software releases to ensure up to date coverage with no manageability gaps • Extensive discovery protocol support for improved accuracy and completeness, including ping, CDP, LLDP, ARP, BGP, OSPF, and route table look ups • Flexible Grouping and Site Profiles help to manage large networks by associating network elements to user definable groups or to a hierarchical campus > building > floor model. • Device Work Center simplifies access to the tools and features necessary to easily manage the network inventory, including discovery, manual and bulk import, software image management • Customizable out-of-the-box Cisco best practices and validated design configuration templates enable quick and easily device and service deployment • Composite Templates allow greater flexibility and packaging of individual templates into larger, reusable, purpose built configurations, for more consistent and quicker network designs • Automated Deployment workflows simplify the rollout of new devices or entire sites, accelerating service availability • Centralized monitoring of branch, campus and WLAN access networks helps maintain robust performance and optimal access connectivity experience • Integration with Cisco ISE and Cisco Secure Access Control Server (ACS) View provides a simple way to collect and analyze additional data relevant to endpoints • Integrated workflows and tools help IT administrators quickly assess service disruptions, receive notices about performance degradation, research resolutions, and take action to remedy non-optimal situations • Robust out-of-the-box compliance rules engine for customizable compliance auditing based on Cisco and industry best practice rules.
Assurance	
Network-based end-user experience monitoring	• Dedicated dashboards and views to present high-level and granular analytical data to monitor end-user experience of business critical applications • Site-based tracking of users' endpoints • Dedicated dashboard to present contextual data for a given user endpoint. Operators can set up rules to assign incoming endpoints to physical locations such as a remote branch or a site • Rich set of dashlets to track health of key KPIs, especially those of rich media applications • Time-based filtering of data lets users narrow the issue down to a particular timeframe or to look at related network/application events given a timeframe in which the problem was observed
Flexible NetFlow Version 9 support and advanced troubleshooting	• Support for collecting Flexible NetFlow templates and raw records, which network engineers use for troubleshooting • Trigger packet captures on multiple NAMs based on common software filters • All-encompassing solution integrated with Cisco platforms to simplify operational manageability • Access to packets, flows, and MIBs for exhaustive granular analysis

Table 1 Prime Infrastructure: Key Features (continued)

Feature	Benefits
Configuration/monitoring templates	• Predefined collection plans to collect application response time, traffic analysis, and Real-time Transport Protocol (RTP) metrics • Predefined device/interface health templates to collect KPI for monitoring health of network elements • Threshold templates to monitor key indicators and alert the operator/engineer of any anomalies • NAM configuration templates to configure NAM devices' system and monitoring parameters • Removes the complexity involving setting of complex data sources and collecting the right KPIs • Good categorization of metrics into device health, application health, and thresholds helps the user in organizing and planning for data collection more efficiently
Dedicated dashboard for voice, video monitoring and analysis	• Analysis of voice, video and real-time transport protocol (RTP) traffic in general at branch or individual user level • Multiple data sources for voice video analysis, including Network Analysis Module and Medianet • Monitor RTP conversations at branch and client levels
Classic View - Wireless	
Support for WLC 7.3 release	• Supports new hardware and software features introduced in WLC 7.3 release. This includes WLC 8500 controller, virtual WLC platforms, AP 2600, AP 1550 with EPON interface, HA with sub-second failover, Proxy Mobile IPv6 and other features.
Next Generation Maps	• New maps engine supports high resolution images with much improved pan & zoom controls. Search within Maps is also supported. The new maps combined with search offers a faster and smoother navigation experience with quicker access to information.
Automatic Hierarchy Creation	• Automatically create maps and assign APs to maps using regular expressions. This feature automates the tedious work of creating campus>building>floor hierarchies and assigning APs to the floor.
Auto-Switch Port Tracing	• Ability to automatically identify the Cisco switch and port information for a rogue AP connected to the Cisco switch, which allows quickly identifying and mitigating the threat posed by a rogue AP.
Third Party Support	• Ability to discover and monitor third-party (non-Cisco) switches that support RFC 1213 and wireless controllers/access points from Aruba Networks.
Branch and WAN	
Configuration Management	• Feature Configuration Templates for: DMVPN, GETVPN, ACL, and ScanSafe • Device Level Support (Device Work Center) for: DMVPN, GETVPN, ACL, EIGRP, RIP, OSPF, Static Routes, Ethernet Interfaces, NAT, and Zone Based Firewall

For detailed information about Prime Infrastructure features, see the *Cisco Prime Infrastructure 2.0 User Guide.*

4 About Cisco Prime Infrastructure Licensing

You must purchase Lifecycle licenses to access Prime Infrastructure features and Assurance licenses to access Assurance features in Prime Infrastructure. Each license also controls the number of devices you can manage using those features.

If you have installed Prime Infrastructure for the first time, you may access Lifecycle and Assurance management features using the built-in evaluation license. The default evaluation license is valid for 60 days and a maximum of 100 devices. Send a request to licensing@cisco.com if:

- You need to extend the evaluation period.
- You need to increase the device-count limit.
- You already have a particular feature license and need to evaluate other feature licenses.

You will need to purchase the base license and the corresponding feature licenses before the evaluation license expires.

Purchase the following feature licenses based on the features you need to access and the number of devices you want to manage:

- Base license— Each Prime Infrastructure management node requires a single base license as a pre-requisite for adding feature licenses.
- Lifecycle license—The Lifecycle license type is based on the number of managed devices. The Lifecycle license provides full access to the following Prime Infrastructure Lifecycle management features:
  - Device configuration management and archiving
  - Software image management
  - Basic health and performance monitoring
  - Event management
  - Troubleshooting

  You must order a single Base license, and then purchase Lifecycle licenses as necessary to access the Prime Infrastructure Lifecycle management features. Lifecycle licenses are available in bundle sizes of 25, 50, 100, 500, 1000, 2500, 5000, 10000, and 15000 devices and can be combined.
- Assurance license—The Assurance license is based on the number of NetFlow-monitored devices. The Assurance license provides access to the following Assurance management features in Prime Infrastructure:
  - End-to-end application, network, and end-user experience visibility
  - Multi-NAM management
  - Monitoring of WAN optimization
  - Assurance dashlets and application troubleshooting

  You must order a single Base license, and then purchase Assurance licenses as necessary to access the Prime Infrastructure Assurance management features. Assurance licenses are available in bundle sizes of 25, 50, 100, 500, 1000, 2500, 5000, 10000, and 15000 devices and can be combined.
- Collector License—The Collector license is based on NetFlow processing in flows per second. By default, the Assurance license provides a Collector license to process NetFlow data collection for up to 20,000 flows per second. You can also purchase a Collector license to support up to 80,000 flows per second.

Prime Infrastructure is deployed using a physical or virtual appliance. You use the standard license center GUI to add new licenses. The new licenses are locked using the standard Cisco Unique Device Identifier (UDI) for a physical appliance and a Virtual Unique Device Identifier (VUDI) for a virtual appliance. You can view this information in the Prime Infrastructure web interface by choosing **Administration > Licenses**.

For more information about:

- Cisco Prime Infrastructure features, see the *Cisco Prime Infrastructure 2.0 User Guide*.
- Ordering Prime Infrastructure licenses, see the *Cisco Prime Infrastructure 2.0 Ordering and Licensing Guide*.

5 Pre-Installation Tasks

Complete the tasks in the following sections before installing Prime Infrastructure.

System Requirements

Server Requirements

Prime Infrastructure is pre-packaged in three different system-size options. Table 2 summarizes the minimum server requirements for each option.

Table 2 Prime Infrastructure Minimum Requirements

Requirement	Express	Custom Express[1]	Standard	Pro
VMWare Version	ESXi 4.1 or later	ESXi 4.1 or later	ESXi 5 or ESXi 5.1	ESXi 5 or ESXi 5.1
Virtual CPUs	4	8	16	16
Memory (DRAM)	12GB	16GB	16GB	24GB
HDD Size	300GB	600GB	900GB	1200GB
Throughput (Disk I/O)	200 MB/s	200 MB/s	200 MB/s	200 MB/s

1. Custom Express is not available as a separate OVA download. You will need to download the Express OVA and customize it for Custom Express. Please contact your Cisco Sales Representative for details on customization.

You can install any of the three Prime Infrastructure options as an Open Virtual Appliance (OVA), running under VMWare ESXi or ESX, on your own hardware. If you choose this implementation, the server you supply must meet or exceed the requirements shown in the table for the option you select.

Prime Infrastructure is also available pre-installed on Cisco-supplied hardware as a physical appliance that meets or exceeds the Standard option requirements.

Please note:

- The Express option replaces the Medium and Small options supplied in previous versions of Prime Infrastructure.
- The Standard option replaces the Large option supplied in previous versions of Prime Infrastructure.
- The Pro option replaces the Extra Large option supplied in previous versions of Prime Infrastructure.

If you install Prime Infrastructure as an OVA on a server that exceeds the minimum requirements for a selected option (or if you increase CPU, memory or disk resources after installation) you can tune the OVA to use the additional resources and improve product performance. See Improving Prime Infrastructure Performance in the *Cisco Prime Infrastructure 2.0 Administrator Guide*.

For maximum management capacities for each option, see Scaling Prime Infrastructure, page 9.

Web Client Requirements

Prime Infrastructure users access the product using a web browser client. Web client requirements are:

- Hardware—A Mac or Windows laptop or desktop compatible with one of the following tested and supported browsers:
  - Google Chrome 27.
  - Microsoft Internet Explorer 8.0 or 9.0 with Google Chrome Frame plugin (users logging in to the simplified Lobby Ambassador interface do not need the plugin).
  - Mozilla Firefox ESR 10 or ESR 17 (ESR 17 is recommended).
  - Mozilla Firefox 22.
- Display resolution—We recommend that you set the screen resolution to 1280 x 800 or higher.
- Adobe Flash Player—You must install Adobe Flash Player on the client machine for Prime Infrastructure features to work properly. We recommend that you download and install the latest version of the Adobe Flash Player from the Adobe website.

Scaling Prime Infrastructure

Prime Infrastructure comes with a variety of server installation options (see System Requirements, page 8). You will want to ensure that you have selected an option appropriate for the size and complexity of your network.

Table 3 gives the maximum number of devices, clients, events, Netflow data flows, and other scale parameters for each option.

Table 3 Supported Scale for Prime Infrastructure Installation Options (includes Assurance)

Parameter	Express	Custom Express[1]	Standard	Pro
Max Unified APs	300	2,500	5,000	20,000
Max Autonomous APs	300	500	3,000	3,000
Max Wired Devices	300	1,000	6,000	13,000
Max NAMs	5	5	500	1,000
Max Controllers	5	5	500	1,000
Max Wired Clients	6,000	50,000	50,000	50,000
Max Wireless Clients	4,000	30,000	75,000	200,000
Max Changing Clients	1,000	5,000	25,000	40,000
Events Sustained Rate (events/second)	100	100	300	1,000
NetFlow Rate (flows/second)	3,000	3,000	16,000	80,000
Max Interfaces	12,000	50,000	250,000	350,000
Max NAM Data Polling Enabled	5	5	20	40
Max Number of Sites/Campus	200	500	2,500	2,500
Max Groups (User-Defined + Out of the Box + Device Groups + Port Groups)	50	100	150	150
Max Virtual Domains	100	500	1,000	1,000
Max Concurrent GUI Clients	5	10	25	25
Max Concurrent API Clients	2	2	5	5

1. Custom Express is not available as a separate OVA download. You will need to download the Express OVA and customize it for Custom Express. Please contact your Cisco Sales Representative for details on customization.

Scaling limits for the pre-installed Cisco-supplied hardware appliance match the Standard option.

Ports Used

Table 4 lists the ports used by Prime Infrastructure and Assurance. These ports must be open in firewalls.

Table 4 Ports Used by Prime Infrastructure and Assurance

Port	Protocol	Direction	Usage
7	TCP/UDP	Server to endpoints	Endpoint discovery via ICMP
20, 21	TCP	Bidirectional server/devices	FTP transfer of files to and from devices
		Server to Cisco.com	FTP download of files from Cisco.com
22	TCP	Server to endpoints	To initiate SSH connection to endpoints during troubleshooting processes.
		Client to server	To connect to the Prime Infrastructure server.
23	TCP	Server to devices	Telnet communication with devices
25	TCP	Server to SMTP server	SMTP email routing

Table 4 Ports Used by Prime Infrastructure and Assurance (continued)

Port	Protocol	Direction	Usage
49	TCP/UDP	Server to TACACS server	Authenticate users using TACACS
53	TCP/UDP	Server to DNS server	DNS
69	UDP	Devices to server	TFTP
161	UDP	Server to devices	SNMP polling
162	TCP/UDP	Endpoints to server.	SNMP Trap receiver port
443	TCP	Client to server	Browser access to Prime Infrastructure via HTTPS (enabled by default). This port is also used to check for software updates between the Prime Infrastructure server and cisco.com.
514	UDP	Devices to server	Syslog server
1099	TCP/UDP	AAA server to server	RMI registry
1522	TCP/UDP	Primary to secondary server, Secondary to primary server	To configure high availability database connection between the primary and secondary Prime Infrastructure
1645	UDP	Server to RAS	Authenticate Prime Infrastructure users via RADIUS Remote Access Server
1646		RAS to server	
1812		Server to RAS	
1813		RAS to server	
4444	TCP	AAA server to server	RMI server
8080	TCP	Client to server	Browser access to Prime Infrastructure via HTTP (disabled by default)
8082	TCP	Server to client	Health Monitor web interface, Apache/Tomcat JSP engine
8087			Secondary server software update page when the secondary server is in Sync mode
8443[1]	TCP	Server to call processors	HTTPS connectivity for RTMT and Cisco Unified CM registration
		Client to server	Browser access to Prime Infrastructure via HTTPS (enabled by default)
9991[1]	UDP	Devices to server	NetFlow and NAM data receiver
10022 to 10041	TCP	Devices to server	Range of ports used for passive FTP file transfers (controller backups, device configurations, report retrieval, etc.)
11011[2]	TCP	Endpoints to server	Plain text dispatcher port for the Plug and Play Gateway
11012			SSL dispatcher port for the Plug and Play Gateway
11013			Plain text plug and play port
11014			SSL port for the Plug and Play Gateway
1315-1319	TCP/UDP	Primary to secondary server, Secondary to primary server	You should reserve solid database ports from 1315 to 1319, to configure high availability database connection between the primary and secondary Prime Infrastructure.
16113	TCP	Controller to Location Server, LS to Controller	Cisco Network Mobility Services Protocol messaging
20514[1]	UDP	Endpoints to server	Syslog receiver
61617[3]	TCP	Server to endpoints	SSL port for Java Message Service connections

1. Used by Prime Infrastructure with Assurance only.
2. Used when the Plug and Play Gateway is enabled on the Prime Infrastructure server.
3. Used by the Prime Infrastructure Plug And Play Gateway only.

Ports Used by the Plug and Play Gateway on Standalone Servers

Table 5 lists the ports that are used by the Plug and Play Gateway on standalone servers.

Table 5 Ports Used by the Plug and Play Gateway

Ports	Protocol	Direction	Usage
80	HTTP	Endpoints to gateway	HTTP service port for the Plug and Play Gateway.
443	HTTPS	Endpoints to gateway	HTTP service port for the Plug and Play Gateway.
21	FTP	Endpoints to gateway	FTP service port for Internal Plug and Play Gateway.
11012	TCP	Device to server	SSL dispatcher port for the Plug and Play Gateway
11014			SSL event port for the Plug and Play Gateway
11016			
11018			
11020			
11022			
11011	TCP	Device to server	Plain text dispatcher port for the Plug and Play Gateway
11013			Plain text event port for the Plug and Play Gateway
11015			
11017			
11019			
11021			
22	SSH	—	Port for admin user to log in and monitor the Plug and Play Gateway.
62616	SSL	—	Plug and Play Gateway internal message server port
61617	SSH	—	Plug and Play Gateway port to connect to Prime Infrastructure 2.0
69	TFTP	—	Used for downloading the device's image and configuration from Prime Infrastructure 2.0 to the Plug and Play Gateway.

Maximum Device Connections For Plug and Play Gateway

The Plug and Play Gateway has limits on the maximum number of device connections to the event ports (11011-110XX) that it can manage on the integrated and standalone server setups. Table 6 gives the maximum number of devices connections and the number of port information for Plug and Play Gateway solution. Each event port opened can support up to a maximum of 1000 device connection. The Prime infrastructure can support Plug and Play activation between 100 to 200 devices at the same time with the following.

Table 6 Maximum Number of Device Connections

Configuration	Maximum Devices	Total Ports (SSL and Plain Text)	Comments
Plug and Play Gateway Integrated within Prime Infrastructure	2000	2	Ports are fixed. One open port for SSL and one for plain text.
Plug and Play Standalone Gateway	1000	10	The number of ports in SSL and plain text can be configured during the setup. However, the total number of ports configured should not exceed 10.

Setting Up Devices for Prime Infrastructure

Before installing, you must enable devices to provide Prime Infrastructure with the data it requires, such as SNMP. When you configure your devices for SNMP and NTP, Prime Infrastructure can provide fault, application, and performance data.

Required Software Versions and Configurations

To work with Prime Infrastructure, your devices must run at least the minimum required software versions shown in the list of supported devices you can access from the Prime Infrastructure user interface by clicking **Help**, then selecting **Supported Devices List**.

You must also configure your devices to support SNMP traps and syslogs, and the Network Time Protocol (NTP), as explained in the following sections.

Configuring SNMP

To ensure that Prime Infrastructure can query SNMP devices and receive traps and notifications from them, you must:

- Set SNMP credentials (community strings) on each device you want to manage using Prime Infrastructure.
- Configure these same devices to send SNMP notifications to the Prime Infrastructure server.

Use the following IOS configuration commands to set read/write and read-only community strings on an SNMP device:

```
snmp-server community private RW
snmp-server community public RO
```

where *private* and *public* are the community strings you want to set.

After you set the community strings, you can specify that device notifications be sent as traps to the Prime Infrastructure server using the following IOS global configuration command on each SNMP device:

```
snmp-server host PIHost traps version community notification-type
```

where:

- *PIHost i*s the IP address of the Prime Infrastructure server.
- *version* is the version of SNMP that is used to send the traps.
- *community* is the community string sent to the server with the notification operation.
- *notification-type* is the type of trap to send. You may need to control bandwidth usage and the amount of trap information being sent to Prime Infrastructure server using this parameter. For more information,

You may need to control bandwidth usage and the amount of trap information being sent to the Prime Infrastructure server using additional commands.

For more information on configuring SNMP, see the snmp-server community and snmp-server host sections of the IOS Command Reference. Also see the "Configuring SNMP Support" section of the Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2, and the list of notification-type values.

Configuring NTP

Network Time Protocol (NTP) synchronization must be configured on all devices in your network as well as on the Prime Infrastructure server. You must specify the NTP servers during server installation (see Installing the Server, page 23).

Note that NTP must be configured and synchronized across all Prime Infrastructure-related servers, including any remote FTP servers you use for backups, secondary Prime Infrastructure high-availability servers, the Plug and Play Gateway, VMware vCenter and the ESX virtual machine, etc. Failure to organize time synchronization across your network can result in anomalous results in Prime Infrastructure.

Configuring Data Sources for Prime Infrastructure With Assurance

If you are licensing Assurance, you must complete pre-installation tasks so that Assurance can monitor your network interfaces and services. See Supported Assurance Data Sources for information about these tasks. These tasks are in addition to those covered in Ports Used by the Plug and Play Gateway on Standalone Servers, page 11.

Supported Assurance Data Sources

Prime Infrastructure with Assurance needs to collect data from your network devices using the exported data sources shown in Table 7. For each source, the table shows the devices that support this form of export, and the minimum version of IOS or other software that must be running on the device in order to export the data.

Use Table 7 to verify that your network devices and their software are compatible with the type of data sources Prime Infrastructure uses. If needed, upgrade your hardware or software. Note that each software version given is a *minimum*. Your devices can run any later version of the same software or IOS release train.

You might also need to make changes to ensure that Prime Infrastructure can collect data using SNMP, as explained in "Configuring SNMP".

Configuring Assurance Data Sources

Before installing, you should enable the supported devices shown in Table 7 to provide Prime Infrastructure with fault, application, and performance data, and ensure that time and date information are consistent across your network. The following topics provide guidelines on how to do this.

Table 7 Prime Infrastructure Assurance: Supported Data Sources, Devices and Software Versions

Device Type	Cisco IOS Releases That Support NetFlow	Supported NetFlow Export Types	NetFlow Configuration
Catalyst 3750-X / 3560-X	15.0(1)SE IP base or IP services feature set and equipped with the network services module.	TCP and UDP traffic	See the "Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches" section in the *Cisco Prime Infrastructure 2.0 User Guide*.
Catalyst 3850	15.0(1)EX	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, see the "Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches" section in the *Cisco Prime Infrastructure 2.0 User Guide*. To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**
Catalyst 4500	15.0(1)XO and 15.0(2)	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, see the "Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches" section in the *Cisco Prime Infrastructure 2.0 User Guide*. To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**
Catalyst 6500	SG15.1(1)SY	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, see the "Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches" section in the *Cisco Prime Infrastructure 2.0 User Guide*. To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**
ISR	15.1(3) T	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI > Collecting Traffic Statistics** To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**
ISR G2	15.2(1) T and 15.1(4)M	TCP and UDP traffic, application response time, Voice and Video	To configure TCP, UDP, and ART, see the "Configuring NetFlow on ISR Devices" section in the Cisco Prime Infrastructure User Guide. To configure Voice & Video, use this CLI template: **Design > Feature Design > CLI Templates > System Templates - CLI >Medianet - PerfMon**

Table 7 Prime Infrastructure Assurance: Supported Data Sources, Devices and Software Versions (continued)

Device Type	Cisco IOS Releases That Support NetFlow	Supported NetFlow Export Types	NetFlow Configuration
ISR G2	15.2(4) M2 or later, 15.3(1)T or later	TCP and UDP traffic, application response time, Voice and Video	To configure TCP, UDP, and ART, see the "Configuring Application Visibility" section in the *Cisco Prime Infrastructure 2.0 User Guide*.
ASR	15.3(1)S1 or later	TCP and UDP traffic, application response time, Voice & Video, HTTP URL visibility	
ISR G3	15.3(2)S or later		

Enabling Medianet NetFlow

To ensure that Cisco Prime Infrastructure can make use of Medianet data, your network devices must:

- Enable Medianet NetFlow data export for the basic set of statistics supported in Prime Infrastructure.
- Export the Medianet NetfFlow data to the Prime Infrastructure server and port.

Use a configuration like the example below to ensure that Prime Infrastructure gets the Medianet data it needs:

```
flow record type performance-monitor PerfMonRecord
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
! For the flow record, match on source/destination *address* only.
! Assurance will not collect data for matches on source/destination prefix or mask.
  match transport source-port
  match transport destination-port
  match transport rtp ssrc
  collect application media bytes counter
  collect application media bytes rate
  collect application media packets counter
  collect application media packets rate
  collect application media event
  collect interface input
  collect interface output
  collect counter bytes
  collect counter packets
  collect routing forwarding-status
  collect transport packets expected counter
  collect transport packets lost counter
  collect transport packets lost rate
  collect transport round-trip-time
  collect transport event packet-loss counter
  collect transport rtp jitter mean
  collect transport rtp jitter minimum
  collect transport rtp jitter maximum
  collect timestamp interval
  collect ipv4 dscp
  collect ipv4 ttl
  collect ipv4 source mask
  collect ipv4 destination mask
  collect monitor event
flow monitor type performance-monitor PerfMon
  record PerfMonRecord
  exporter PerfMonExporter
flow exporter PerfMonExporter
  destination PrInIP
  source Loopback0
  transport udp PiInPort
policy-map type performance-monitor PerfMonPolicy
  class class-default
! Enter flow monitor configuration mode.
```

```
  flow monitor PerfMon
! Enter RTP monitor metric configuration mode.
  monitor metric rtp
!Specifies the minimum number of sequential packets required to identify a stream as being an RTP flow.
  min-sequential 2
! Specifies the maximum number of dropouts allowed when sampling RTP video-monitoring metrics.
  max-dropout 2
! Specifies the maximum number of reorders allowed when sampling RTP video-monitoring metrics.
  max-reorder 4
! Enter IP-CBR monitor metric configuration mode
  monitor metric ip-cbr
! Rate for monitoring the metrics (1 packet per sec)
  rate layer3 packet 1
interface interfacename
  service-policy type performance-monitor input PerfMonPolicy
  service-policy type performance-monitor output PerfMonPolicy
```

In this example configuration:

- *PrInIP* is the IP address of the Prime Infrastructure server.
- *PiInPort* is the UDP port on which the Prime Infrastructureserver is listening for Medianet data (the default is 9991).
- *interfaceName* is the name of the interface (such as `GigabitEthernet0/0` or `fastethernet` 0/1) sending Medianet NetFlow data to the specified *PrInIP*.

For more information on Medianet configuration, see the *Medianet Reference Guide*.

Enabling NetFlow and Flexible NetFlow

To ensure that Prime Infrastructure can make use of NetFlow data, your network devices must:

- Have NetFlow enabled on the interfaces you want to monitor.
- Export the NetFlow data to the Prime Infrastructure server and port.

Use the commands below to enable NetFlow on Cisco IOS devices:

```
interface interfaceName
ip route-cache flow
```

where *interfaceName* is the name of the interface (such as “fastethernet” or “fastethernet0/1”) on which you want to enable NetFlow.

Note that you must enable NetFlow on each *physical* interface for which you want Prime Infrastructure to collect data. These will normally be Ethernet or WAN interfaces. This applies to physical interfaces only. You do not need to enable NetFlow on VLANs and Tunnels, as they are included automatically whenever you enable NetFlow on a physical interface.

Use the following commands to see NetFlow working on the device:

```
show ip flow export
show ip cache flow
show ip cache verbose flow
```

Once NetFlow is enabled, you can configure the device to export NetFlow data to Prime Infrastructure using these IOS configuration-mode commands:

```
ip flow-export version 5
ip flow-export destination PrInIP PiInPort
ip flow-export source interfaceName
```

where:

- *PrInIP* is the IP address of the Prime Infrastructure server
- *PiInPort* is the UDP port on which the Prime Infrastructure server is listening for NetFlow data (the default is 9991)
- *interfaceName* is the name of the interface sending NetFlow data to the specified *PrInIP*. This will cause the source interface’s IP address to be sent to Cisco Prime Infrastructure as part of NetFlow export datagrams.

For more information on NetFlow configuration, see:

- *Cisco IOS Switching Services Configuration Guide, Release 12.1*
- *Flexible NetFlow Configuration Guide, Cisco IOS Release 15.1M&T*
- *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*
- *Catalyst 6500/6000 Switches NetFlow Configuration and Troubleshooting*

Deploying Network Analysis Modules (NAMs)

Ensure that your NAMs are placed appropriately in the network. For more information, see:

- *Cisco Network Analysis Module Software 5.1 User Guide*—Includes deployment scenarios and covers a variety of topics, including deploying NAMs in the branch, and deploying NAMs for WAN optimization.
- *Cisco Network Analysis Module Deployment Guide*—See the topic "Places in the Network Where NAMs Are Deployed".

If your NAMs are deployed properly, then no other pre-installation work is required. When you conduct discovery using Cisco Prime AM, you will need to enter HTTP access credentials for each of your NAMs.

Note Prime Infrastructure uses a more efficient REST interface to query NAMs. For this reason, it does not support the direct export of NetFlow data from NAMs. Any device exporting NetFlow data must export that NetFlow data directly to Prime Infrastructure, not via a NAM. Exporting NetFlow data from any NAM to Cisco Prime Infrastructure will result in data duplication.

Enabling Performance Agent

To ensure that Prime Infrastructure can collect application performance data, use the IOS *mace* (for Measurement, Aggregation and Correlation Engine) keyword to configure Performance Agent (PA) data flow sources on your branch-office and data center routers.

For example, use the following commands in IOS global configuration mode to configure a PA flow exporter on a router:

```
flow exporter mace-export
destination 172.30.104.128
transport udp 9991
```

Use commands like the following to configure flow records for applications with flows across the router:

```
flow record type mace mace-record
collect application name
collect art all
```

where *application name* is the name of the application whose flow data you want to collect.

To configure the PA flow monitor type:

```
flow monitor type mace mace-monitor
record mace-record
exporter mace-export
```

To collect traffic of interest, use commands like the following:

```
access-list 100 permit tcp any host 10.0.0.1 eq 80
class-map match-any mace-traffic
match access-group 100
```

To configure a PA policy map and forward the PA traffic to the correct monitor:

```
policy-map type mace mace_global
class mace-traffic
flow monitor mace-monitor
!
```

Finally, enable PA on the WAN interface:

```
interface Serial0/0/0
mace enable
```

For more information on configuring Performance Agent, see the *Cisco Performance Agent Deployment Guide*.

6 Upgrading Cisco Prime Infrastructure

You can upgrade the following Cisco Prime Infrastructure (and predecessor) products to Cisco Prime Infrastructure 2.0:

- Cisco Prime Infrastructure 1.3.0.20
- Cisco Prime Infrastructure 1.2.1.12 (You must first install available point patches as explained in Installing Point Patches, page 18.)
- Cisco Prime Network Control System 1.1.1.24 (You must first install available point patches as explained in Installing Point Patches, page 18.)

If your product/version is not in this list: To upgrade to 2.0, you must first upgrade to one of the releases in this list. You may be able to do so by installing one or more point patches using the instructions in Installing Point Patches, page 18.

If your product/version is in this list: Before attempting to upgrade to 2.0, make sure that you download and install the appropriate point patch listed in Table 8. These patches fix critical problems with Prime Infrastructure backup and restore features, which are part of every upgrade. You can download and install the critical patches using the instructions in Installing Point Patches, page 18. Once you have installed the appropriate critical patch, you will also need to take a new application backup before performing a system migration or inline upgrade.

Table 8 Critical Backup/Restore and Upgrade Patches

If you are using...	Then you must install this backup/restore patch...
Prime Infrastructure 1.3.0.20	PI_1_3_0_20_Update.1.12.tar.gz and/or PI_1_3_0_20_Update.4-16.tar.gz
Prime Infrastructure 1.2.1.12	PI_1_2_1_12-Update.1.0.tar.gz
Prime Infrastructure 1.2.1.12 (migrated from 1.2.0.103)	PI_1_2_1_12u-Update.1.tar.gz
Network Control System 1.1.1.24	ncs_1_1_1_24-Update.13.4.tar.gz

You can upgrade these product/versions to 2.0 using either of the following methods:

1. **System Migration**—Install Cisco Prime Infrastructure 2.0 as a new system on a new host, and restore the existing system's data to the new system. You can then decommission the old host. This option is preferred if you want to migrate to a larger OVA, have a large network, or cannot disturb your production system. For details, see Migrating to a New System, page 20.
2. **Inline Upgrade**—Upgrades your existing system to version 2.0. All existing data is retained and you will be using the same size OVA when the upgrade is complete. The existing product will not be operational until the upgrade is complete. This option is preferred when you want to keep the same size OVA and interruption of service during the upgrade is acceptable. For details, see Performing an Inline Upgrade, page 21.

Prime Infrastructure application backups include licenses, so reinstalling on a new system or virtual machine does not require you to rehost your licenses, so long as you use a *recent application backup to restore your data from the old system to the new system*. In any other case, you must email a request to licensing@cisco.com to rehost your licenses. You will need to Include your VUDI details and existing license details, including the number of licenses in your request.

Installing Point Patches

You may need to install point patches to get your version of Prime Infrastructure to the level at which upgrade is supported. Different point patch files are provided for each version of Prime Infrastructure and its predecessor products. Download and install only the patch files that match the version of your existing system and that are required before you upgrade to a higher version. You can find the appropriate patches by pointing your browser to the Cisco Download Software Navigator.

You can check the Prime Infrastructure version and patch version you are running by using the commands **show version** and **show application**.

Before installing a point patch, you will need to copy the patch file to your Prime Infrastructure server's default repository. Many users find it easy to do this by first downloading the patch file to a local FTP server, then copying it to the repository. You can also copy the patch file to the default repository using any of the following methods:

- cdrom—Local CD-ROM drive (read only)
- disk—Local hard disk storage
- ftp—URL using an FTP server.
- http—URL using an HTTP server (read only)
- https—URL using an HTTPS server (read only)
- nfs—URL using an NFS server
- sftp—URL using an SFTP server
- tftp—URL using a TFTP server

Step 1 Download the appropriate point patch to a local resource in your environment:

a. With the Cisco Download Software navigator displayed in your browser, select **Products > Cloud and Systems Management > Routing and Switching Management > Network Management Solutions >** Cisco Prime Infrastructure.

b. Select the version of Cisco Prime Infrastructure that most closely matches the one you are currently using (e.g., **Cisco Prime Infrastructure 1.2**).

c. Click **Prime Infrastructure Patches** to see the list of available patches for that version of the product.

d. Next to each patch that is required, click **Download**, then follow the prompts to download the file.

Step 2 Open a console session and log in as admin to the existing Prime Infrastructure server

Step 3 Copy the downloaded patch file to the default local repository. For example:

```
admin# copy source disk:/defaultRepo
```

Where:

- *source* is the downloaded patch file's location and name (for example: ftp://<YourFTPServer>/pi_1.2.1.12_update.tar.gz).
- *disk* is the disk and path to the local defaultRepo.

Step 4 Install the patch:

```
admin# patch install patchFile defaultRepo
```

Where *patchFile* is the name of the patch file you copied.

Installing the Plug and Play Gateway Patch

The Plug and Play Gateway standalone server patch is available in the pnp-gateway-patch-2.0.0.28.tar.gz file.

The patch upgrade procedure requires an FTP or TFTP server containing the patch file. You can access the server from the Cisco Prime Infrastructure 1.2 Plug and Play Gateway standalone server.

Step 1 Log in to the Plug and Play Gateway standalone server as admin user.

Step 2 Create a repository in the configuration mode and execute the repository command by providing the repository name and other details.

Step 3 Use the patch install command to install the pnp-gateway-patch-2.0.0.28.tar.gz Plug and Play Gateway standalone patch.

Step 4 Execute the pnp setup command to reconfigure the Plug and Play standalone server and start the plug and play processes:

```
pnp-server login: admin
Password:
```

```
pnp-server/admin# configure
Enter configuration commands, one per line. End with CNTL/Z.
pnp-server/admin(config)# repository <repository_name>
pnp-server/admin(config-Repository)# url ftp://<SERVER_HOST_NAME>/<FOLDER_LOCATION>
pnp-server/admin(config-Repository)# user <USER_ID> password <OPTION> <PASSWORD>
pnp-server/admin(config-Repository)# exit
pnp-server/admin(config)# exit
pnp-server/admin#
pnp-server/admin# patch install pnp-gateway-patch-2.0.0.28.tar.gz
pnp-patching-<VERSION>.tar.gz <repository_name>
Save the current ADE-OS running configuration? (yes/no) [yes] ?
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Patch installation...
Patch successfully installed
pnp-server/admin#
pnp-server/admin# pnp setup
```

Migrating to a New System

System migration is the preferred option for most upgrades of production installations. In most cases, you will need to supply new server hardware to complete the migration.

Note that, to use this path, you must be migrating from one of the release levels listed in Upgrading Cisco Prime Infrastructure, page 18, and have installed the required backup and restore patches listed in Table 8 on page 18.

Step 1 Before you begin, remove any existing High Availability configuration from your primary and secondary Prime Infrastructure servers. You can do this using either of the following options:

- Launch Prime Infrastructure, choose **Administration > High Availability > HA Configuration**, and click **Remove**.
- Go to admin console and run the **ncs ha remove** command.

Step 2 If you have not already done so: Set up a remote backup repository for the old host. For details, see Using Remote Backup Repositories in the *Cisco Prime Infrastructure 2.0 Administrator Guide*.

Step 3 Take an application backup of the old host on the remote repository. For details, see Taking Application Backups From the Interface in the *Cisco Prime Infrastructure 2.0 Administrator Guide*

Step 4 Install the new host as explained in Installing Cisco Prime Infrastructure, page 22.

Step 5 Configure the new host to use the same remote backup repository as the old host.

Step 6 Restore the application backup on the remote repository to the new host, as explained in Restoring From Application Backups in the *Cisco Prime Infrastructure 2.0 Administrator Guide*.

Step 7 When the upgrade is complete:

- Instruct users to clear the browser cache on all client machines that accessed an older version of Prime Infrastructure before they try to connect to the upgraded Prime Infrastructure server.
- If you run into problems creating a backup after you have upgraded to version 2.0, see Managing Disk Space Issues on Prime Infrastructure Servers, page 22
- If you were using external AAA (RADIUS or TACACS) before the upgrade, see Renewing Your AAA Settings, page 22.

Performing an Inline Upgrade

Inline upgrade is simpler than system migration, and requires no new hardware.

Note If you are upgrading from Prime Infrastructure 1.x small virtual machine, you should create a new virtual machine with the Express OVA, back up your existing small virtual machine, and then restore it on the new virtual machine. You can delete the old small virtual machine after the new virtual machine is fully operational. Inline upgrade of the small virtual machine is not supported.

Step 1 Before you begin, remove any existing High Availability configuration from your primary and secondary Prime Infrastructure servers. You can do this using either of the following options:

- Launch Prime Infrastructure, choose **Administration > High Availability > HA Configuration**, and click **Remove**.
- Go to admin console and run the **ncs ha remove** command.

Step 2 Copy the upgrade file downloaded from cisco.com to the default repository:

```
admin# copy source disk:/defaultRepo
```

Where:

- *source* is the application upgrade file's URL, path and filename (for example: FTP://<YourFTPServer>/PI-Upgrade-2.0.0.0.294.tar.gz).
- *disk* is the disk and path to the local defaultRepo.

Step 3 Stop the Prime Infrastructure server by entering the command **ncs stop**.

Step 4 Run the application upgrade:

```
admin# application upgrade PI-Upgrade-2.0.0.0.294.tar.gz defaultRepo
```

This step can take 30 minutes or more to complete, depending on the size of the application database.

Step 5 When the upgrade is complete:

- Verify that the application is running by entering the command **ncs status** command.
- Instruct users to clear the browser cache on all client machines that accessed an older version of Prime Infrastructure before they try to connect to the upgraded Prime Infrastructure server.
- If you run into problems creating a backup after you have upgraded to version 2.0, see Managing Disk Space Issues on Prime Infrastructure Servers, page 22
- If you were using external AAA (RADIUS or TACACS) before the upgrade, see Renewing Your AAA Settings, page 22.

Managing Disk Space Issues on Prime Infrastructure Servers

If you are experiencing issues with disk space *during* an upgrade, we suggest you either:

- Use the VMware **Edit Settings** feature to increase the amount of disk space allocated to the OVA.
- Use the upgrade method explained in Migrating to a New System, page 20 to move your installation to a server with adequate disk space.

If you are unable to create a backup *after* upgrading your existing system, follow the steps below to free disk space and create a successful backup. If you are still unable to create a backup after using the `ncs cleanup` command, set up and use a remote FTP repository for your backups, as explained in Using Remote Backup Repositories in the *Cisco Prime Infrastructure 2.0 Administrator Guide.*

Step 1 Open a console session and log in to the server as admin. Enter the password when prompted.

Step 2 At the command line, enter the following command to compact the application database:

```
admin# ncs cleanup
```

Step 3 When prompted, answer `Yes` to the deep cleanup option. When the operation is complete, you should be able to perform another backup.

Renewing Your AAA Settings

If you were using external RADIUS or TACACS user authentication before upgrading, you must transfer the expanded Prime Infrastructure 2.0 user task list to your AAA server. After you upgrade Prime Infrastructure, you must re-add any permissions on the TACACS+ or RADIUS server and update the roles in your TACACS server with the tasks from the Prime Infrastructure server. For information, see (Setting the AAA Mode in the *Cisco Prime Infrastructure 2.0 Administrator Guide.*

If you changed the IP address of the Prime Infrastructure server during the upgrade process, you will need to log in to Prime Infrastructure as user “root” and follow the instructions given in Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes before other users will be able to log in.

7 Installing Cisco Prime Infrastructure

If you are currently running any previous version of Cisco Prime Network Control System (NCS), NCS (WAN), or Prime Assurance Manager, you must upgrade instead of installing. See Upgrading Cisco Prime Infrastructure, page 18.

Before You Begin

Before installing Prime Infrastructure in a virtual machine, you must ensure that:

- Set up devices and data sources in your network to work with Prime Infrastructure (see Pre-Installation Tasks, page 8).
- VMware ESX/ESXi is installed and configured on the machine you plan to use as the Prime Infrastructure server host. See the VMware documentation for information on setting up and configuring your host machine.
- The installed VMware ESX/ESXi host is reachable.
- The VMware vSphere client is installed on a Windows host (or laptop). See the VMware documentation on how to install the VMware vSphere client. After the virtual host is available on the network, you can browse to its IP address to display a web-based interface from which you can install the VMware vSphere client.

  The VMware vSphere Client is Windows-based, so you must download and install the client using a Windows PC.
- The Prime Infrastructure OVA is saved to the same machine where your vSphere client is installed. Depending on your arrangement with Cisco, you may download the OVA file from Cisco.com or use your Cisco-supplied installation media.

Deploying the OVA from the VMware vSphere Client

Make sure that all of the system requirements are met before you deploy the OVA. Review the sections System Requirements, page 8 and Before You Begin, page 22.

Step 1 Launch your VMware vSphere client.

Step 2 Choose **File > Deploy OVF Template**.

The Deploy OVF Template window appears.

Step 3 Click the **Deploy from file** radio button.

Step 4 Click **Browse** to access the location where you have saved the OVA file.

Step 5 Click **Next**.

The OVF template details are displayed in the OVF Template Details window.

Step 6 Verify the details about the OVA file, including the product name, version, and the size, then click **Next**.

The Name and Location window appears.

Step 7 Specify a name and location for the template that you are deploying. The name must be unique within the inventory folder, and can contain up to 80 characters.

Step 8 Click **Next**.

The Ready to Complete window appears. It displays the details of the OVA file, the name of the virtual appliance, size, host, and storage details.

Step 9 After you verify the options, click **Finish** to start the deployment.

This may take a few minutes to complete. Check the progress bar in the Deploying Virtual Application window to monitor the task status.

After the deployment task has successfully completed, a confirmation window appears.

Step 10 Click **Close**.

The virtual appliance that you deployed is listed under the host, in the left pane of the vSphere client.

Installing the Server

After you deploy the Prime Infrastructure OVA, you must configure the virtual appliance to install and start Prime Infrastructure.

Step 1 In the VMware vSphere client, right-click the deployed virtual appliance and choose **Power > Power On**.

Step 2 Click the **Console** tab. At the localhost login prompt, enter **setup**.

Step 3 The console prompts you for the following parameters:

- hostname—The host name of the virtual appliance.
- IP Address—The IP address of the virtual appliance.
- IP default netmask—The default subnet mask for the IP address.
- IP default gateway—The IP address of the default gateway.
- Default DNS domain—The default domain name.
- Primary nameserver—The IP address of the primary name server.
- Secondary name servers—The IP address if the secondary name server, if available. You can add up to three secondary name servers.
- Primary NTP server—The IP address or host name of the primary Network Time Protocol server you want to use. (`time.nist.gov` is the default).
- Secondary NTP servers—The IP address of the secondary NTP server.

- System Time Zone—The time zone code you want to use.
- Clock time—The clock time based on the server's time zone.
- Username—The name of the first administrative user (known as "admin"). This is the administrator account used to log in to the server via SSH or Telnet. You can accept the default, which is `admin`.
- Password—Enter the admin user password and then confirm it. The default is `admin`.

Step 4 When you are done entering these values, the installer application tests the network configuration parameters you entered. If the tests are successful, it begins installing Prime Infrastructure.

Step 5 When the application installation is complete, you will be prompted for the following post-installation parameters:

- High Availability Role Selection—Enter `yes` at the prompt if you want this installed server to serve as the fallback secondary server in a high-availability implementation. You will be prompted to provide a High Availability registration key. If you enter `no` at the prompt, the server will act as the primary server (standalone) and the installation will process with the following prompts:
- Root Password—Enter the password to be used for the default `root` administrator, and then confirm it. This is the root account used to log in to the Prime Infrastructure user interface for the first time and set up other user accounts.
- FTP password—Enter the FTP password and confirm it.

Step 6 When the installation is complete, the virtual appliance reboots and you are presented with a login prompt.

Step 7 Log in to the virtual appliance using the "admin" username and password you specified in step 3.

Logging into the Prime Infrastructure User Interface

Follow these steps to log into the Prime Infrastructure user interface through a web browser:

Step 1 Launch one of the Supported Browsers (see System Requirements, page 8) on a different computer from the one on which you installed and started Prime Infrastructure.

Step 2 In the browser's address line, enter **https:**//*ipaddress*, where *ipaddress* is the IP address of the server on which you installed Prime Infrastructure. The Prime Infrastructure user interface displays the Login window.

Note When you access Prime Infrastructure for the first time, some browsers will display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the Prime Infrastructure server. After you complete this procedure, the browser will accept the Prime Infrastructure server as a trusted site in all future login attempts.

Step 3 Enter the *root* administrator username and password, as specified when Installing the Server, page 23.

If any licensing problems occur, a message appears in an alert box. If you have an evaluation license, the number of days until the license expires is shown. You are also alerted to any expired licenses. You have the option to go directly to the **Administration > Licenses** page to address these problems.

Step 4 Click **Login** to log into Prime Infrastructure. The user interface is now active and available for use. The home page appears.

To ensure system security, select **Administration > Users, Roles & AAA > Change Password** to change the password for the *root* administrator.

To exit the user interface, close the browser page or click **Logout** in the upper right corner of the page. Exiting a Prime Infrastructure user interface session does not shut down Prime Infrastructure on the server.

If a system administrator stops the Prime Infrastructure server during your Prime Infrastructure session, your session ends, and the browser displays this message: "The page cannot be displayed." Your session does not reassociate to Prime Infrastructure when the server restarts. You must start a new Prime Infrastructure session.

8 Getting Started

After you install Prime Infrastructure, you must perform additional tasks to begin managing your network. These tasks are all listed in the "Getting Started" chapter of the *Cisco Prime Infrastructure 2.0 User Guide*. After you complete these tasks, you are ready to start monitoring and configuring your network.

9 Installing the Plug and Play Gateway on Standalone Servers

To install and start the Prime Infrastructure Plug and Play Gateway, you should deploy the OVA and configure the virtual appliance.

Note The Plug and Play Server is also available as a integrated server with the Prime Infrastructure in Release 2.0. The Plug and Play Gateway automatically starts along with the Prime Infrastructure and uses the credentials and certificates of the Prime Infrastructure. This section provides the procedure only to set up the Plug and Play Gateway on Standalone Servers that can be used in scenarios like DMZ.

Prime Infrastructure Plug and Play Gateway Server Requirements

The server requirements for the Cisco Prime Infrastructure Plug and Play Gateway OVA are as follows:

- VMware ESXi Server version 4.1.0 or 5.0 is required. Version 5.0 is preferred. Prime Infrastructure 2.0 has not been tested with VMware ESXi Server versions later than 5.0.
- RAM— 4GB
- Disk Space—100 GB (Recommended to use SAN)
- Processors—4 virtual CPUs with 2.93 GHz or faster

Deploying the Prime Infrastructure Plug and Play Gateway OVA

Make sure that all of the system requirements are met before you deploy the OVA. Review the Prime Infrastructure Plug and Play Gateway Server Requirements, page 25 and Before You Begin, page 22 sections.

Step 1 Launch your VMware vSphere client.

Step 2 Choose **File > Deploy OVF Template**.

The Deploy OVF Template window appears.

Step 3 Click the **Deploy from file** radio button.

Step 4 Click **Browse** to access the location where you have saved the OVA file.

Step 5 Click **Next**.

The OVF template details are displayed in the OVF Template Details window.

Step 6 Verify the details about the OVA file, including the product name, version, and the size, then click **Next**.

The Name and Location window appears.

Step 7 Specify a name and location for the template that you are deploying. The name must be unique within the inventory folder, and can contain up to 80 characters.

Step 8 Click **Next**.

The Ready to Complete window appears. It displays the details of the OVA file, the name of the virtual appliance, size, host, and storage details.

Step 9 After you verify the options, click **Finish** to start the deployment.

This may take a few minutes to complete. Check the progress bar in the Deploying Virtual Application window to monitor the task status.

After the deployment task has successfully completed, a confirmation window appears.

Step 10 Click **Close**.

The virtual appliance that you deployed is listed under the host, in the left pane of the vSphere client.

Installing the Cisco Prime Infrastructure Plug and Play Gateway as a Standalone

After you deploy the Cisco Prime Infrastructure Plug and Play Gateway OVA, you must configure the virtual appliance to install and start the Cisco Prime Infrastructure Plug and Play Gateway.

Step 1 In the VMware vSphere client, right-click the deployed virtual appliance and choose **Power > Power On**.

Step 2 Repeat Step 2 and Step 3 in Installing the Server, page 23.

Step 3 After you enter the values, the installer tests the network configuration parameters. If the tests are successful, the installer begins the Cisco Prime Infrastructure Plug and Play Gateway installation.

Step 4 When the installation is complete, the virtual appliance reboots and displays a login prompt.

Step 5 Log in to the virtual appliance by using the administrative username and password.

Generating a CA-Signed Certificate for the Plug and Play Gateway

By default, the Plug and Play Gateway can be set up to generate a Certification Authority-signed certificates. These certificates can be used to create a trustpoint on the device for Secure Sockets Layer (SSL) communication. We recommend that you use the certificates signed by a single certification authority (CA) for both the Plug and Play Gateway and the device.

Note You should generate the certificate only if you require SSL communication (with a CA-signed certificate) to take place between the Plug and Play Gateway and the device.

To generate a CA-signed certificate, follow these steps:

Step 1 Log in to the Cisco Networking Service-supported K9 device and check the version of the software image using the **show version** command. The image that is loaded on the CNS-supported K9 device should be a crypto image.

Step 2 Generate the RSA keys and the CA request using the following command:

```
Generate RSA keys and certificate signing request:
$cd /root
$openssl genrsa -out server.key 1024 // generate an RSA Keypair and a Certificate Signing Request:
$chown root:root server.key
$chmod 400 server.key
$openssl req -new -key server.key -out server.csr

You can enter a period (.) in case you do not want to enter any information. But remember to enter CE
server name as
(Ex: myCEserver.example.com) when asked for Common Name (e.g., YOUR name) []:
```

The server.key and the server.csr files are now in the root directory.

Step 3 Use the .csr file, get the CA certificate from the CA authority.

Step 4 Copy the CA Certificate to the Plug and Play Gateway and use the certificate path to run the Plug and Play setup. For more information on the Plug and Play setup, see the "Setting Up the Prime Infrastructure Plug and Play Gateway" section on page 29.

Activating the CA Certificate on an Endpoint Device

To activate the server certificate on the CNS supported K9 Device, follow these steps:

Step 1 Log in to the CNS supported K9 device and check the clock timings. The endpoint device and the Plug and Play gateway server should have the same timestamp.

```
Router#show clock
02:04:40.065 PST Fri Feb 20 2009

         The certificate begins to be valid starting at 19:30 GMT,
         which is 3:30pm Eastern Time, which is 12:30 Pacific Time.
Hence make sure the clock on router is set correctly.

Router#clock set 01:08:10 20 FEBRUARY 2009
Router#show clock
.01:08:14.082 PST Fri Feb 20 2009
```

Step 2 Check if a certificate is already installed for the required trustpoint. If yes, use this command in the config terminal to revoke the old certificate:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no crypto ca trustpoint example.com
% Removing an enrolled trustpoint will destroy all certificates
 received from the related Certificate Authority.

Are you sure you want to do this? [yes/no]: yes
% Be sure to ask the CA administrator to revoke your certificates.

No enrollment sessions are currently active.
```

Step 3 Run the following commands to define the trustpoint:

```
Router(config)#ip host hostname x.x.x.x
Router(config)#ip host hostname.example.com x.x.x.x
Router(config)#ip domain-lookup
Router(config)#crypto ca trustpoint myCEServer.example.com
Router(ca-trustpoint)#enrollment mode ra
Router(ca-trustpoint)#enrollment terminal
Router(ca-trustpoint)#usage ssl-client
Router(ca-trustpoint)#
Router(ca-trustpoint)#exit
```

Step 4 Authenticate the trustpoint:

```
Router(config)#crypto ca authenticate hostname.example.com
                   Enter the base 64 encoded CA certificate.
                   End with a blank line or the word "quit" on a line by itself

                   Copy the entire content of server.crt here and press enter as below.

Router(config)#crypto ca authenticate myCEServer.example.com

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDFTCCAf2gAwIBAgIKMt87mwABAAABrjANBgkqhkiG9w0BAQUFADAuMRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtURVNULVNTTC1DQTAeFw0wOTAx
MTYxMDU0NDJaFw0xMDAxMTYxMTA0NDJaMDAxDjAMBgNVBAoTBUNpc2NvMR4wHAYD
VQQDExVpbWd3LXRlc3QxMC5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAPAdsaSPKMpGOny05TDuZG3t9Dwlc1VGk2ZfPpp7oX1eQNK4ub3Lr3o5
fb83nmwzzb6hXgDvO3ElX+Xjh+j4LZDDWb30db5jxJvYVz9MyrnChBD7kyLuUaOc
uxLNxPUwnWTzd28n+Wg5uSptH8b/ofxx5WBessCY20448hjTROq5AgMBAAGjgbYw
gbMwHQYDVR0OBBYEFClHMwLRjIfWNvv3FrMLNO/ILJz5MB8GA1UdIwQYMBaAFI7J
Ti5oRslwv2B3MmERGbPKKUsSMFwGA1UdIARVMFMwUQYKKwYBBAEJFQEBADBDMEEG
```

```
CCsGAQUFBwIBFjVodHRwOi8vd3d3LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvcG9s
aWNpZXMvaW5kZXguaHRtbDATBgNVHSUEDDAKBggrBgEFBQcDATANBgkqhkiG9w0B
AQUFAAOCAQEAXP9iMHWVGRucbda++UUR8PFSzaSChmQyWti5+oWe+WCUBU/HtonM
XACZBxwA4HTT7eqhPfs4HhNUUHT/l/ChZLksaWJNTO7Wa2X80vvJJUoWHVZod1Pm
vUJFgvZCBVBj54wvFaH+ijADzJ3ASVPOMxxdKdJzpYspNE4W0s0ghyIQxXF1Ht/B
n+DBipuG4hx5dK9px5f/nzCYNh5zxPnriaFe7WYiWUxg47WWT1nBMiVED8Z48WwB
gSX2K9+87Jg+lJ8EpQ1Avkf2X7vWsCW1vx9YicLw+RFS6o+4Za+NrwSmF/Y0pGJg
rCJlwLn2n0ZI64atJFa/FdAujr9W9KWrmw==
-----END CERTIFICATE-----quit

Trustpoint 'myCEServer.example.com' is a subordinate CA and holds a non self signed cert
Trustpoint 'myCEServer.example.com' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
       Fingerprint MD5: C7C7BFB5 CD3DDB95 987B0899 0385282E
      Fingerprint SHA1: 82721218 56C6C4FE 855C8B43 AA653F63 786D63BF

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Step 5 Perform the following CNS configuration on the CNS supported K9 device:

```
Router#sh run | i cns
         cns trusted-server all-agents myCEServer
         cns trusted-server all-agents myCEServer.example.com
         cns id string Router
         cns id string Router event
         cns id string Router image
         cns event myCEServer.example.com encrypt 11012 keepalive 60 3
         cns config partial myCEServer.example.com encrypt 443
cns image server https://imgw-test35:443/cns/HttpMsgDispatcher status
https://imgw-test35:443/cns/HttpMsgDispatcher

         cns inventory
         cns exec encrypt 443
```

Step 6 Check if the connection has been established between the CNS supported K9 device and Prime Infrastructure:

```
Router#sh cns event conn
The currently configured primary event gateway:
        hostname is imgw-test10.example.com.
        port number is 11012.
        encryption is enabled.
Event-Id is Router
Keepalive setting:
        keepalive timeout is 60.
        keepalive retry count is 3.
Connection status:
        Connection Established.
The currently configured backup event gateway:
        none.

The currently connected event gateway:
        hostname is imgw-test10.example.com.
        port number is 11012.
        encryption is enabled.
Router#
```

The SSL connection between the CNS supported K9 device and the Prime Infrastructure server must be successfully established.

Setting Up the Prime Infrastructure Plug and Play Gateway

To set up the Cisco Prime Plug and Play Gateway OVA, follow these steps.

Step 1 Log in to the Cisco Prime Plug and Play Gateway server by using the administrative username and password.

Step 2 In the command prompt, enter the **pnp setup** command and press **Enter**.

Step 3 The console prompts for the following parameters:

- IP Address —The IP address to be used by the Plug and Play gateway server.
- SSL Server Certificate — The self/CA signed server certificate for Plug and Play Gateway.
- CNS Event — The CNS event configuration that will be deployed on the device for dynamic location.

Step 4 The console displays the following:

```
bgl-pnp-dev1-ovf/admin# pnp setup

        ######################################################################
        Enter Plug and Play Gateway Setup (setup log /var/KickStart/install/setup.log)
        For detail information about the parameters in this setup,
        refer to Plug and Play Gateway Admin Guide.
        ######################################################################

Enter Prime Infrastructure IP Address: [10.104.105.168]
Enable self certificate for server bgl-pnp-dev1-ovf (y/n) [y]
Self Signed Certificate already available do you want to recreate (y/n)? [n]

        Automatic download of SSL Certificate is possible if
        Prime Infrastructure Server is up and running.

Automatically download the certificate for server 10.104.105.168 (y/n) [y] n
Enter absolute pathname of Prime Infrastructure server certificate file:
[/var/KickStart/install/ncs_server_certificate.crt]

        The maximum number of Event Gateways allowed is '10' for both plain text
        and ssl combined. The Event Gateway ports 11011 and 11012 are reserved for port
        automatic allocation.These ports are not counted while taking the maximum number of ports.

        Each Event Gateway can serves up to a maximum of 1000 devices.

Enter number of Event Gateways that will be started with crypto operation: [5] 10
All the ports are configured for crypto operation. No plain text port is available. Is it the right
configuration y/n: [y]

        The CNS Event command configures how the managed devices should
        connect to this particular Plug and Play Gateway. The command entered in the following
        line should match what's configured on the devices WITHOUT the port
        number and keyword 'encrypt' if cryptographic is enabled.

        For example, if the following CLI is configured on devices
        "cns event bgl-pnp-dev1-ovf encrypt 11012 keepalive 120 2 reconnect 10",
        then `encrypt 11012` should be removed and the below line should be entered :
        "cns event bgl-pnp-dev1-ovf keepalive 120 2 reconnect 10"

        Another example, if this is a backup Plug and Play Gateway and the following CLI is
        configured on devices
        "cns event bgl-pnp-dev1-ovf 11011 source Vlan1 backup", then `11011`
        should be removed and the below line should be entered :
        "cns event bgl-pnp-dev1-ovf source Vlan1 backup"

        Unable to enter a correct CLI could cause the managed devices not
        be able to connect to this Plug and Play Gateway. For details, please refer to
        Installation and Configuration Guide.

Enter CNS Event command: [cns event bgl-pnp-dev1-ovf keepalive 120 2 reconnect 10]
```

```
Commit changes (y/n): y
```

Note For advance setup, use the **pnp setup advanced** command. For details, see the Command Reference Guide for Cisco Prime Infrastructure 2.0.

```
bgl-pnp-dev1-ovf/admin# pnp setup advanced

        ######################################################################
        Enter Plug and Play Gateway Setup (setup log /var/KickStart/install/setup.log)
        For detail information about the parameters in this setup,
        refer to Plug and Play Gateway Admin Guide.
        ######################################################################

Enter IP Address of Plug and Play Gateway server [10.104.105.167]
 **** Setup abort!!! Exiting ***
```

Step 5 To check the status of the Prime Infrastructure Plug and Play gateway server, log in to the gateway server and execute the **pnp status** command, or enter the following URL on the browser https://<IP address or hostname>/cns/ResourceInit?name=port. The gateway server status will be displayed.

```
bgl-pnp-dev1-ovf/admin# pnp status


SERVICE                        |  MODE                 |  STATUS        |  ADDITIONAL INFO
-------------------------------------------------------------------------------------------------
System                         |                       |  UP            |
-------------------------------------------------------------------------------------------------
Event Messaging Bus            |  PLAIN TEXT           |  UP            |  pid: 21161
CNS Gateway Dispatcher         |  PLAIN TEXT           |  UP            |  pid: 21520, port: 11011
CNS Gateway                    |  PLAIN TEXT           |  UP            |  pid: 21549, port: 11013
CNS Gateway                    |  PLAIN TEXT           |  UP            |  pid: 21583, port: 11015
CNS Gateway                    |  PLAIN TEXT           |  UP            |  pid: 21617, port: 11017
CNS Gateway                    |  PLAIN TEXT           |  UP            |  pid: 21656, port: 11019
CNS Gateway                    |  PLAIN TEXT           |  UP            |  pid: 21691, port: 11021
CNS Gateway Dispatcher         |  SSL                  |  UP            |  pid: 21755, port: 11012
CNS Gateway                    |  SSL                  |  UP            |  pid: 21987, port: 11014
CNS Gateway                    |  SSL                  |  UP            |  pid: 22113, port: 11016
CNS Gateway                    |  SSL                  |  UP            |  pid: 22194, port: 11018
CNS Gateway                    |  SSL                  |  UP            |  pid: 22228, port: 11020
CNS Gateway                    |  SSL                  |  UP            |  pid: 22287, port: 11022
HTTPD                          |                       |  UP            |
Image Web Service              |  SSL                  |  UP            |
Config Web Service             |  SSL                  |  UP            |
Resource Web Service           |  SSL                  |  UP            |
Image Web Service              |  PLAIN TEXT           |  UP            |
Config Web Service             |  PLAIN TEXT           |  UP            |
Resource Web Service           |  PLAIN TEXT           |  UP            |
Prime Infrastructure Broker    |  SSL                  |  UP            |  port: 61617, connection: 1


bgl-pnp-dev1-ovf/admin#
```

10 Removing the Prime Infrastructure Virtual Appliance

Removing Prime Infrastructure using the following method will permanently delete all data on the server, including server settings and local backups. You will be unable to restore your data unless you have a remote backup.

Step 1 In the VMware vSphere client, right-click the Prime Infrastructure virtual appliance.

Step 2 Power off the virtual appliance.

Step 3 Click **Delete from Disk** to remove the Prime Infrastructure virtual appliance.

11 Navigation and Documentation Reference

This section provides information about navigational paths to access Prime Infrastructure features, and the details of the sections where the features are covered in Prime Infrastructure documentation.

Table 9 Navigation and Documentation Reference

Task	Navigation in Cisco Prime Infrastructure	Section in Cisco Prime Infrastructure User Guide
Discovering your network	**Operate > Discovery**	Getting Started
Setting up port monitoring	**Design > Port Grouping**	Designing the Network
Setting up virtual domains	**Administration > Virtual Domains**	Getting Started
Using monitoring dashboards	**Operate > Monitoring Dashboards**	Operating the Network
Using templates for configuring and monitoring	**Design > Feature Design** or **Design > Monitor Configuration**	Designing the Network
Using templates for wireless configuration	**Design > Wireless Configuration**	Creating Wireless Controller Templates
Viewing alarms	**Operate > Alarms & Events**	Monitoring Alarms
Finding and comparing device configurations	**Operate > Configuration Archive**	Working with Device Configurations
Maintaining device configurations	**Operate > Configuration Archive**	Maintaining Device Configuration Inventory
Managing Users	**Administration > Users, Roles & AAA**	Controlling User Access
Setting up access switches after they have been added to Prime Infrastructure	**Workflows > Initial Device Setup**	Getting Help Setting Up and Configuring Devices
Preconfiguring devices that will be added to your network in the future	**Workflows > Plug and Play Setup**	Getting Help Setting Up and Configuring Devices

12 Reinstalling Cisco Prime Infrastructure on a Physical Appliance

You must have root privileges to install Prime Infrastructure on a physical appliance. Make sure you have performed a recent backup before reinstalling Prime Infrastructure. After reinstalling, you can restore your data using the backup.

To reinstall Prime Infrastructure on a physical appliance, follow these steps:

Step 1 Insert the provided Prime Infrastructure software Image DVD. The system boots up and the following console appears:

```
ISOLINUX 3.11 2005-09-02  Copyright (C) 1994-2005 H. Peter Anvin

                  Welcome to Cisco Prime Infrastructure

To boot from hard disk, press <Enter>.

Available boot options:

      [1] Prime Infrastructure Installation (Keyboard/Monitor)
      [2] Prime Infrastructure Installation (Serial Console)
      [3] Recover administrator password. (Keyboard/Monitor)
      [4] Recover administrator password. (Serial Console)
      <Enter> Boot existing OS from Hard Disk.

Enter boot option and press <return>.

boot:
```

Step 2 Select option 1 to reinstall Prime Infrastructure software image. The system reboots and the configure appliance screen appears.

Step 3 Enter the initial setup parameters and the system reboots again. Remove the DVD and follow the steps to start the Prime Infrastructure server.

13 Related Documentation

The Cisco Prime Infrastructure 2.0 Documentation Overview lists all documentation is available for Prime Infrastructure:

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

14 Obtaining Documentation and Submitting a Service Request

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

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

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