QUICK START GUIDE

Cisco Prime Infrastructure 1.4 Quick Start Guide

Revised: July 2013, OL-28937-02

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 describes how to install Cisco Prime Infrastructure 1.4.

This guide is targeted to 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 1.2 User Guide*.

2 Product Overview

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. 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, 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.

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 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 easy 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 an 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 • Support for standard NetFlow fields with ability to update/add new ones based on heuristics • 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 • Option to extend predefined collection plans by including more metrics coming in as part of NetFlow records • 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 7.0 and later versions	For detailed information on the supported devices types and software versions, see http://www.cisco.com/en/US/products/ps12239/products_device_support_tables_list.html
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 1.2 User Guide*.

4 About Cisco Prime Infrastructure Licensing

You purchase licenses to access the Prime Infrastructure features required to manage your network. Each license also controls the number of devices or device interfaces that you can manage using those features.

You need a base license and the corresponding feature licenses (such as the assurance or the lifecycle license) to get full access to the respective Prime Infrastructure features to manage a set number of devices or interfaces.

If you have installed Prime Infrastructure for the first time you may access the lifecycle and assurance features using the built-in evaluation license that is available by default. The default evaluation license is valid for 60 days for 100 devices and 150 interfaces. You can send a request to ask-prime-infrastructure@cisco.com if:

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

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

You purchase the following licenses based on the features that you are required to access:

- 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
  - Troubleshooting

  You need to 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, and 10000 devices and can be combined.
- Assurance license—The Assurance license is based on the number of NetFlow monitored interfaces. 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

  You order a single base license, and then purchase assurance licenses as necessary. Assurance licenses are available in bundle sizes of 50, 100, 500, 1000, and 5000 interfaces and can be combined.
- Special PAM-15 license—The Special PAM-15 license is a stand-alone license for commercial use. This license allows you to access a maximum of 15 managed devices and NetFlow-monitored interfaces, in any combination. If you need to add more devices or interfaces, you must purchase additional lifecycle or assurance licenses with part numbers that support 50 or more interfaces.

For more information:

- Prime Infrastructure features, see the *Cisco Prime Infrastructure 1.2 User Guide* at http://www.cisco.com/en/US/products/ps12239/products_user_guide_list.html.
- Ordering Prime Infrastructure licenses, see the *Prime Infrastructure Ordering Guide* at http://www.cisco.com/go/primeinfrastructure.

Understanding License Files Delivered with Prime Infrastructure

The following tables explain which license files are provided with Prime Infrastructure based on the PIDs that you order. Prime Infrastructure 1.1 and 1.2 are product bundles that provide license files for multiple products.

Note Prime Infrastructure 1.4 is only available for existing Prime Infrastructure 1,1, 1.2, or 1.3 customers with a valid service contract.

The Prime Infrastructure 1.2 (bundle) includes:

- Prime Infrastructure 1.2 (product) – replaces Cisco Prime NCS 1.1 and NCS (WAN) 1.1
- Prime LMS 4.2

The Prime Infrastructure 1.1 (bundle) includes:

- Prime NCS 1.1
- Prime NCS (WAN) 1.1
- Prime LMS 4.2

Table 2 Prime Infrastructure 1.2 Part Numbers and License Files

Ordered Part Number	License Type	Included Part Numbers	Used with Product	Notes
R-PI12-BASE-K9*	Base	-	PI 1.2 , 1.3, and 1.4	Base license required for each Prime Infrastructure instance
L-PI12-LF-X	Lifecycle	L-PI12-LF-X-LIC*	PI 1.2, 1.3, and 1.4	Requires a base license
	LMS	L-PILMS42-X*	LMS 4.2	-
L-PI12-AS-X*	Assurance	-	PI 1.2, 1.3, and 1.4	Requires a base license
L-PI12-CM-X	Compliance	L-PI12-CM-X-LIC*	Not Used	Prime Infrastructure 1.2 does not have compliance features that require a license
	Compliance	L-LMS42-CM-25*	LMS 4.2	Requires LMS 4.2.2 or higher
L-PI12-GW	Gateway	-	PI 1.2, 1.3, and 1.4	Right to Use, no license file
Minor Release Upgrade Options for LMS 4.x Users				
R-PI12-M-K9	Base	R-PI12-BASE-K9*	PI 1.2, 1.3, and 1.4	-
L-PI12-X-M	Lifecycle	L-PI12-LF-X-LIC*	PI 1.2, 1.3, and 1.4	-
	LMS	L-PILMS42-X-M*	LMS 4.2	-
Major Release Upgrade Options for LMS 2.x/3.x Users				
R-PI12-UP-K9	Base	R-PI12-BASE-K9*	PI 1.2, 1.3, and 1.4	-
L-PI12-X-UP	Lifecycle	L-PI12-LF-X-LIC*	PI 1.2, 1.3, and 1.4	-
	LMS	L-PILMS42-X-U*	LMS 4.2	-
Migration Options for WCS Users				
R-W-PI12-M-K9	Base	R-PI12-BASE-K9*	PI 1.2, 1.3, and 1.4	New PI 1.2 license files are provided. No need to migrate WCS licenses.
L-W-PI12-X-M	Lifecycle	L-PI12-LF-50-LIC*	PI 1.2, 1.3, and 1.4	New PI 1.2 license files are provided. No need to migrate WCS licenses.
	LMS	L-PILMS42-50-M*	LMS 4.2	-
Minor Release Upgrade Options for NCS Users				

Table 2 Prime Infrastructure 1.2 Part Numbers and License Files (continued)

Ordered Part Number	License Type	Included Part Numbers	Used with Product	Notes
R-N-PI12-M-K9				Use your existing NCS base license for PI 1.2
L-N-PI12-X-M	LMS	L-PILMS42-X-M*	LMS 4.2	Using your existing NCS licenses for PI 1.2
Spare PIDs ordered through the Product Upgrade Tool				
R-PI12-BASE-K9=*	Base	-	PI 1.2, 1.3, and 1.4	-
L-PI12-X-M=	Lifecycle	L-PI12-LF-X-LIC*	PI 1.2, 1.3, and 1.4	-
	LMS	L-PILMS42-X-M*	LMS 4.2	-
L-N-PI12-X-M=	LMS	L-PILMS42-X-M*	LMS 4.2	Use your existing NCS licenses for PI 1.2

* PID that provides a PAK for claim of license file.

Table 3 Prime Infrastructure 1.1 Part Numbers and License Files

Ordered Part Number	License Type	Included Part Numbers	Used with Product	Notes
R-PI-1.1-X-K9	Base	L-PINCS11-X*	NCS 1.0, NCS 1.1, PI 1.2, PI 1.3	Base license required for each product instance
	Base	L-PINCSW11-X*	NCS (WAN) 1.1	Base license required for each product instance
	LMS	L-PILMS42-X*	LMS 4.2	-
L-PI-1.1-X-ADD	Add-On	L-PINCS11-50-A*	NCS 1.0, NCS 1.1, PI 1.2, PI 1.3	-
	Add-On	L-PINCSW11-50-A*	NCS (WAN) 1.1	-
	LMS	L-PILMS42-50-A*	LMS 4.2	-
L-PI-1.1-CM-X*	Compliance	-	LMS 4.2	Only LMS 4.2.2 has compliance features which require a license
Minor Release Upgrade Options for LMS 4.x Users				
R-PI-1.1-MR-K9	Base	L-PINCS11-25-B*	NCS 1.0, NCS 1.1, PI 1.2, PI 1.3	25 device bonus license
	Base	L-PINCSW11-25-B*	NCS (WAN) 1.1	25 device bonus license
R-PI1.1-X-MR-K9	Add-On	L-PINCS11-50-M*	NCS 1.0, NCS 1.1, PI 1.2, PI 1.3	
	Add-On	L-PINCSW11-50-M*	NCS (WAN) 1.1	-
	LMS	L-PILMS42-50-M*	LMS 4.2	-
Major Release Upgrade Options for LMS 2.x/3.x Users				
R-PI1.1-X-UP-K9	Base	L-PINCS11-X-U*	NCS 1.0, NCS 1.1, PI 1.2, PI 1.3	-
	Base	L-PINCSW11-X-U*	NCS (WAN) 1.1	-
	LMS	L-PILMS42-X-U*	LMS 4.2	-
Migration Options for WCS Users				

Table 3 Prime Infrastructure 1.1 Part Numbers and License Files (continued)

Ordered Part Number	License Type	Included Part Numbers	Used with Product	Notes
R-WCS-PI11-M-K9	Base	L-PINCS11-25-B*	NCS 1.0, NCS 1.1, PI 1.2, PI 1.3, PI 1.4	25 device bonus license
	Base	L-PINCSW11-25-B*	NCS (WAN) 1.1	25 device bonus license
R-W-PI11-X-M-K9	Add-On	L-PINCS11-X-M*	NCS 1.0, NCS 1.1, PI 1.2, PI 1.3, PI 1.4	-
	Add-On	L-PINCSW11-X-M*	NCS (WAN) 1.1	-
	LMS	L-PILMS42-X-M*	LMS 4.2	-
Minor Release Upgrade Options for NCS Users				
R-NCS-PI11-MR-K9	Base	L-PINCSW11-25-B*	NCS (WAN) 1.1	25 device bonus license. Use your existing NCS base license for NCS and PI.
R-N-PI11-X-MR-K9	Add-On	L-PINCSW11-X-M*	NCS (WAN) 1.1	Use your existing NCS licenses for NCS and PI
	LMS	L-PILMS42-X-M*	LMS 4.2	-
Spare PIDs ordered through the Product Upgrade Tool				
R-PI11-X-MR-K9=	Base	L-PINCS11-25-B*	NCS 1.0, NCS 1.1, PI 1.2, PI 1.3, PI 1.4	25 device bonus license
	Base	L-PINCSW11-25-B*	NCS (WAN) 1.1	25 device bonus license
	Add-On	L-PINCS11-X-M*	NCS 1.0, NCS 1.1, PI 1.2, PI 1.3, PI 1.4	-
	Add-On	L-PINCSW11-X-M*	NCS (WAN) 1.1	-
	LMS	L-PILMS42-X-M*	LMS	-
R-NPI11-X-MR-K9=	Base	PINCSW11-25-B*	NCS (WAN) 1.1	25 device bonus license. Use your existing NCS licenses for NCS and PI.
	Add-On	L-PINCSW11-X-M*	NCS (WAN) 1.1	Use your existing NCS licenses for NCS and PI.
		L-PILMS42-X-M*	LMS 4.2	-

Note It is important that you use the correct license file with the correct product (for example, do not attempt to use an LMS license file with Prime Infrastructure 1.2). For non-upgrade purchases, you receive an equal number of licenses for each product in the bundle. There is never a need to convert a license intended for one product to another product (for example, convert an LMS license file to Prime Infrastructure 1.2). In the case of upgrades that you receive all the necessary license files. In some cases that you may not need a new license file for a given product, because your existing license files continue to work. For example, all licenses obtained with Cisco Prime NCS 1.0 continue to work with Prime NCS 1.1 and Prime Infrastructure 1.2, 1.3, and 1.4.

However, due to a bug (CSCue51282) you will not be able to add newly purchased Prime Infrastructure lifecycle or assurance licenses until you first apply a Prime Infrastructure 1.2 base license. You can order the Prime Infrastructure 1.2 base license at no charge, using either the regular ordering process or the product upgrade tool, if you have a valid service contract. When going through the regular ordering process, order the top-level part number R-PI12-K9 with the base option R-PI12-BASE-K9. When using the product upgrade tool, order R-PI12-BASE-K9=.

Cisco Prime NCS and Prime Infrastructure license files are node 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 find the UDI or VUDI in the Prime Infrastructure web interface by choosing Administration > Licenses.

In some cases you might need to request a license re-host; for example, if you reinstall the product on a new system or virtual machine or you perform a migration upgrade. To re-host licenses, email a request to licensing@cisco.com and include your UDI or VUDI details and existing license details.

Understanding Cisco Prime Infrastructure Device Licensing Entitlement

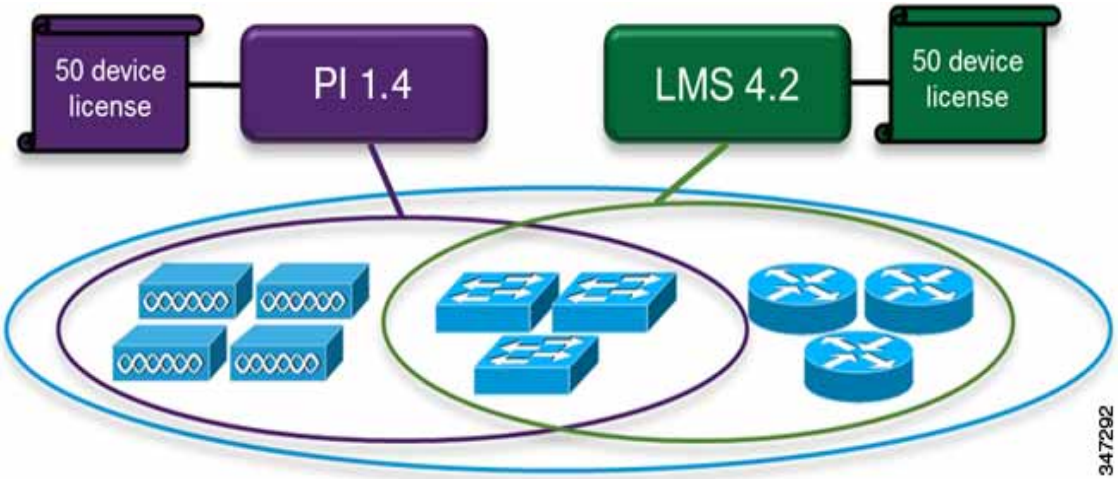
You are entitled to use any combination of the products included with Cisco Prime Infrastructure 1.4 to manage up to the number of devices for which you have purchased licenses. Each product receives a full device count license; but still the entitlement is as described, even though this could potentially be exceeded given that there is no common license pool being used. Only a single device license is consumed even if you choose to manage a given device with more than one of the included products.

The following figure shows a hypothetical example, where Prime Infrastructure has been licensed for 50 devices. Two products are being used:

- Prime Infrastructure 1.4 is managing four APs and three switches.
- LMS 4.2 is managing three routers, plus the three switches managed by Prime Infrastructure 1.4.

In this example, ten device licenses of the entitlement are being used, and 40 are not used.

Figure 1 Sample Device Licensing Entitlement



5 Pre-Installation Tasks

Before installing Prime Infrastructure, complete the tasks in the following sections.

System Requirements

Server Requirements (for VMware ESXi environment)

VMware ESXi Server software is required on the server. Version 5.0 or 5.1 is required for the Large and Extra Large OVAs. Version 4.1 will work with Small and Medium OVAs, but 5.0 or 5.1 is preferred.

Prime Infrastructure can be installed as a pre-sized virtual appliance (OVA) on your own server. The minimum server requirements for each of the Prime Infrastructure OVA options are as follows:

- Small OVA (requires ESXi 4.1 or 5.0 or 5.1):
  - RAM—8 GB
  - Disk Space—200 GB
  - Processors—4 virtual CPUs
- Medium OVA (requires ESXi 4.1 or 5.0 or 5.1):
  - RAM—12 GB
  - Disk space—300 GB
  - Processors—4 virtual CPUs
- Large OVA (requires VMware ESXi 5.0 or 5.1):
  - RAM—16 GB
  - Disk Space—400 GB
  - Processors—16 virtual CPUs
- Extra Large OVA (requires VMware ESXi 5.0 or 5.1):
  - RAM—24 GB
  - Disk Space—1.2 TB
  - Processors—16 virtual CPUs

For hard disks of all sizes, I/O throughput must be greater than 200 MB per second.

For virtual CPUs, you can configure any combination of sockets and cores, the product of which must equal the number of virtual CPUs required. For example, if 16 virtual CPUs are required, you can configure 4 sockets with 4 cores, or 2 sockets with 8 cores, etc.

Prime Infrastructure is also available as a hardware appliance, which comes pre-installed with the Large OVA and has the following specifications:

- RAM—16 GB
- Disk Space—900 GB
- Processors—16 virtual CPUs

For maximum management capacities for each option, see Scaling Prime Infrastructure, page 12.

Web Client Requirements

Hardware—A Mac or Windows laptop or desktop compatible with one of the supported browsers:

- Google Chrome 25.0, 26.0, or 27.0
- Microsoft Internet Explorer 8.0 or 9.0 with Chrome plug-in. Native Internet Explorer is not supported.
- Mozilla ESR 17.x, 17 and later

Display resolution—We recommend that you set the screen resolution to 1024 x 768 or higher.

Adobe Flash Player—For Prime Infrastructure features to work properly, you must install Adobe Flash Player 10.2.2 on the client machine. 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 11). You will want to ensure that you have selected an option appropriate for the size and complexity of your network.

Table 4 gives the maximum number of devices, clients, events, and Netflow data flows that Prime Infrastructure can manage for each option. Capacities for the pre-installed hardware appliance match the Large option.

Table 4 Scaling: Prime Infrastructure Server Capacities (Includes Assurance)

	Small	Medium	Large	Extra Large
Devices	250 total. The mix of devices may include up to: • Wired Devices: 100 • Controllers: 2 • Autonomous APs: 100 • Unified APs: 100 • NAMs: 0	500 total. The mix of devices may include up to: • Wired Devices: 300 • Controllers: 5 • Autonomous APs: 300 • Unified APs: 300 • NAMs: 0	10,000 total. The mix of devices may include up to: • Wired Devices: 6,000 • Controllers: 500 • Autonomous APs: 3,000 • Unified APs: 5,000 • NAMs: 500	18,000 total. The mix of devices may include up to: • Wired Devices: 13,000 • Controllers: 1,000 • Autonomous APs: 3,000 • Unified APs: 15,000 • NAMs: 1,000
Clients	Wired: 1,000 Wireless: 1,000 Roaming: 250	Wired: 6,000 Wireless: 4,000 Roaming: 1,000	Wired: 50,000 Wireless: 75,000 Roaming: 25,000	Wired: 50,000 Wireless: 200,000 Roaming: 40,000
Events[1]	100 per second[2]	100 per second[2]	300 per second[2]	1,000 per second[2]
Netflows	0	0	16,000 flows per second	80,000 flows per second

1. Events are syslogs or SNMP traps received from managed network devices.
2. Sustained rate. Burst rate is 5 times the sustained rate, assuming each burst lasts for 10 seconds and occurs once an hour.

Ports Used

The following ports are used by Prime Infrastructure and Assurance. These ports must be open in firewalls.

Table 5 Ports to be Used

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
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)
514	UDP	Devices to server	Syslog messages
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/Tomcast JSP engine
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, and so on.)
16113	TCP	Controller to Location Server, LS to Controller	Cisco Network Mobility Services Protocol messaging
20514[1]	UDP	Endpoints to server	Syslog receiver
61617[2]	TCP	Server to endpoints	Establish SSL Java Message Service connections

1. Used by Prime Infrastructure with Assurance only.
2. Used by the Prime Infrastructure Plug and Play Gateway only.

Setting Up Devices for Prime Infrastructure

Before installing, you must enable devices to provide Prime Infrastructure with 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 Prime Infrastructure 1.3 Supported Devices table.

You must also configure your devices to support SNMP traps and syslogs, and the Network Time Protocol (NTP), as described 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 that you want to manage using Prime Infrastructure.
- Configure these same devices to send SNMP notifications to the Prime Infrastructure server.

Use the following Cisco 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 that 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 Cisco IOS global configuration command on each SNMP device:

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

where:

- *PIHost* is 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.

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 specify the NTP server during server installation (see the "Installing the Server" section on page 20). 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 will need to complete pre-installation tasks so that Assurance can monitor your network interfaces and services. These tasks are in addition to those covered in the "Setting Up Devices for Prime Infrastructure" section on page 14.

Supported Assurance Data Sources

Prime Infrastructure with Assurance needs to collect data from your network devices using the exported data sources shown in Table 6. For each source, the table shows the devices that support this form of export, and the minimum version of Cisco IOS or other software that must be running on the device to export the data.

Use this table 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 may also need to make changes to ensure that Prime Infrastructure can collect this data, as explained in the "Configuring SNMP" section on page 14.

Note Table 6 contains just a subset of the devices that Prime Infrastructure supports. For a complete list, see the Prime Infrastructure 1.3 Supported Devices table.

Table 6 Prime Infrastructure Assurance: Supported Data Sources, Devices and Software Version

Device Data Sources	Supported Devices	Minimum Software Version
Medianet NetFlow	Cisco Catalyst 3750 Series Switches, Cisco Catalyst 3560 Series Switch	Cisco IOS Release 12.2(58)SE
	Cisco Catalyst 6500 and Catalyst 6500-E Series Switches	Cisco IOS Release 15.0(1)SY
	Cisco 880, 890, 1900, 2900 and 3900 Series Integrated Services Routers	Cisco IOS Release 15.1(3)T
NetFlow (NF) and Flexible NetFlow (FNF)	Nearly all Cisco devices	Cisco IOS Release 11.1 (for NF only) or Cisco IOS Release 12.2(31)SB2 (for FNF)
Network Analysis Module (NAM)	Any NAM-compatible product, including: • Cisco Catalyst 6500 Series Network Analysis Module (NAM-1x/NAM-2x)[1] • Cisco 7600 Series Network Analysis Module (NAM-1x/NAM-2x) • Cisco NAM 2300 Series Appliances • Cisco NAM 2200 Series Appliances • Cisco Branch Routers Series Network Analysis Module (NME-NAM) • Cisco SM-SRE Network Analysis Module	All software versions are supported
Performance Agent (PA)	Cisco 880, 890, 1900, 2900, and 3900 Integrated Services Routers (PA is not supported on "E" models and 3925)	Cisco IOS Release 15.1(4)M
Simple Network Management Protocol (SNMP)	All	N/A

1. The NAM-3 module running 6.x code is not supported in Prime Infrastructure 1.x. To get this support, upgrade to Prime Infrastructure 2.1 or later.

Configuring Assurance Data Sources

Before installing, you should enable your supported devices to provide Prime Infrastructure with fault, application and performance data, and ensure that time and date information are consistent across your network as described in the following topics.

Enabling Medianet NetFlow

To ensure that 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 one in the following example 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
  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
```

where:

- *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 that you want to monitor.
- Export the NetFlow data to the Prime Infrastructure server and port.

Use the following commands 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 Cisco 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 Prime Infrastructure as part of NetFlow export datagrams.

For more information on NetFlow configuration, see the following documentation:

- Cisco IOS Release 15.1 M&T Configuration Guides
- *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 “Places in the Network Where NAMs Are Deployed” section.

If your NAMs are deployed properly, then no other pre-installation work is required. When you conduct discovery using Cisco Prime Assurance Manager 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 Prime Infrastructure will result in data duplication.

Enabling Performance Agent

To ensure that Prime Infrastructure can collect application performance data, use the Cisco 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 Cisco 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, use the following commands:

```
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 Installing Prime Infrastructure

If you are currently running any previous version of Prime Network Control System (NCS) or Prime Assurance Manager, you must upgrade, not install (see the "Upgrading Cisco Prime Infrastructure" section on page 22). The following instructions are only for new installations or if you are migrating into a new Prime Infrastructure system.

Before You Begin

Before installing Prime Infrastructure in a virtual machine, you must do the following:

- Set up devices and data sources in your network to work with Prime Infrastructure (see the "Pre-Installation Tasks" section on page 11).

- Ensure that the 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.
- Ensure that the installed VMware ESX/ESXi host is reachable.
- Ensure that 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.

Note The VMware vSphere Client is Windows-based, so you must download and install the client using a Windows PC.

- Ensure that 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

Make sure that all of the system requirements are met before you deploy the OVA. Review the "System Requirements" section on page 11 and the "Before You Begin" section on page 18.

Note If you want to increase the size of the OVA (for example, move from a small OVA to a medium OVA), you must make a backup of your system and then restore on a new larger system. You must follow the upgrade process (see the "Upgrading Cisco Prime Infrastructure" section on page 22). Also, you can only increase the size of the OVA.

For the best performance:

- We recommend that VMware resources (such as CPU and memory) are reserved for the Prime Infrastructure virtual machine.
- Choose thick provisioning for disks when allocating disks for the virtual machine.
- Ensure that the disks have sufficient read/write performance, use disks with IOPS greater than 200.

Step 1 Launch your VMware vSphere client.

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

The Deploy OVF Template window appears.

Step 3 Select 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 might 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 the *setup* command.

Step 3 The console prompts you for the following parameters:

- hostname—The hostname 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—Enter *y* at the prompt and then enter the IP address of each additional name server. Press **Enter** on a blank line to continue.
- Primary NTP server—The IP address or hostname of the primary Network Time Protocol server you want to use. (*time.nist.gov* is the default).
- Secondary NTP servers—Enter *y* at the prompt and then enter the IP address or hostname of each additional NTP server. Press **Enter** on a blank line to continue.
- System Time Zone—The UTC time zone code you want to use.
- 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 server as the fallback secondary server in a high-availability implementation.
- Root Password—Enter the password to be used for the default root administrator, and then confirm it. This is the administrator 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 that you specified in Step 3.

Logging in to the Prime Infrastructure User Interface

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

Step 1 Launch one of the Supported Browsers (see the "System Requirements" section on page 11) 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 you install the server (see the "Installing the Server" section on page 20).

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 in to Prime Infrastructure. The user interface is now active and available for use. The home page appears.

To ensure system security, choose **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.

7 Upgrading Cisco Prime Infrastructure

Important Notes

- We recommend that you upgrade to Prime Infrastructure 1.4 only if you are deploying AireOS Wireless LAN Controller Software Release 7.5.
- Once you upgrade to Prime Infrastructure 1.4, you may not be able to upgrade to some new versions of Prime Infrastructure at the time of their release. However, a migration path will be made available to the latest available Prime Infrastructure at a later date.
- We highly recommend that you take a backup of your data before upgrade and save it for the future.
- If you are running the previous releases of Prime Infrastructure such as 1.1.0.58, 1.1.1.24, 1.2.1.12 and not planning to upgrade to Prime Infrastructure 1.4, it is recommended to upgrade to Prime Infrastructure 1.3.0.20 and apply the upgrade patch (Update 1 for Cisco Prime Infrastructure 1.3.0.20) that is available at: http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.3.1/release/notes/cpi_rn_13_update1.html
- You cannot migrate from Cisco WCS 7.x to Prime Infrastructure 1.4. If you want to do this, you need to follow instructions to migrate to 1.1.1.24 and then upgrade to Prime Infrastructure 1.4. For more information, see the following URL: http://www.cisco.com/en/US/docs/wireless/ncs/1.1/release/notes/NCS_RN1.1.1.html

Recommended Upgrade Paths

- You can upgrade the following products to Cisco Prime Infrastructure 1.4:
  - Cisco Prime Network Control System 1.1.0 (1.1.0.58)
  - Cisco Prime Network Control System 1.1.1 (1.1.1.24)
  - Cisco Prime Infrastructure 1.2.1.12
  - Cisco Prime Infrastructure 1.3.0.20
  - Update 1 for Cisco Prime Infrastructure 1.3.0.20
- If you are running the previous releases of Prime Infrastructure such as 1.1.0.58, 1.1.1.24, 1.2.1.12 and not planning to upgrade to Prime Infrastructure 1.4, it is recommended to upgrade to Prime Infrastructure 1.3.0.20 and apply the upgrade patch (Update 1 for Cisco Prime Infrastructure 1.3.0.20) that is available at: http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.3.1/release/notes/cpi_rn_13_update1.html
- You cannot migrate from Cisco WCS 7.x to Prime Infrastructure 1.4. If you want to do this, you need to follow instructions to migrate to 1.1.1.24 and then upgrade to Prime Infrastructure 1.4. For more information, see the following URL: http://www.cisco.com/en/US/docs/wireless/ncs/1.1/release/notes/NCS_RN1.1.1.html
- Once you upgrade to Prime Infrastructure 1.4, you may not be able to upgrade to some new versions of Prime Infrastructure at the time of their release. However, a migration path will be made available for the latest available Prime Infrastructure at a later date.

Before You Upgrade

Before you perform an upgrade, you must remove the high availability configuration from the primary and secondary Prime Infrastructure servers. You can remove the high availability configuration using either of the following options:

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

If you are upgrading to Prime Infrastructure in a high availability environment, see the "Upgrading Prime Infrastructure in a High Availability Environment" section of the *Cisco Prime Infrastructure Configuration Guide, Release 1.4*.

Note Upgrading Cisco Prime Network Control System 1.1.2.12 or 1.1.3.2 to Cisco Prime Infrastructure 1.4 is not supported directly. If you plan to upgrade from Cisco Prime Network Control System 1.1.2.12 or 1.1.3.2 to Cisco Prime Infrastructure 1.4, contact Cisco TAC for upgrade instructions and assistance. Also, read the following software advisory for more information on how to upgrade. http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.3/software/advisory/Software_Advisory_CPI_1_1_2_and_1_1_3.pdf.

Upgrade Methods

You can upgrade using either of the following methods:

- **Migrate to a New System (recommended)**—Allows you to back up the data from your existing system, install Cisco Prime Infrastructure 1.4 as a new system, and restore the existing system's data to the new system. You can then decommission the old system.

  Note This option is preferred if you want to migrate to a larger OVA, cannot disturb your production system, or have a large network. For details, see the "Migrating to a New Prime Infrastructure 1.4 System" section on page 25.

- **Inline Upgrade**—Upgrades your existing system to Version 1.4 All existing data is retained and you will be using the same size OVA at the end. The existing product will not be operational until the upgrade is complete. This option is for users who do not have another system to work with. For details, see the "Performing an Inline Upgrade to Prime Infrastructure 1.4" section on page 26.

Note Both options require you to install a patch to the existing system before performing the upgrade. For details, see the "Installing the Point Patch" section on page 23.

Installing the Point Patch

If you are upgrading from one of the products listed in Table 7, you must apply a patch to your existing system before you start any upgrade to Prime Infrastructure.

Different point patch files are provided for each version of Prime Infrastructure predecessor products. Download only the patch file that matches the product and version of your existing system, as shown in Table 7.

The point patches are located at the following location:

http://software.cisco.com/download/release.html?mdfid=284396249&flowid=34522&softwareid=284272933&release=1.2.1&relind=AVAILABLE&rellifecycle=&reltype=all

Table 7 Point Patch Files

If your existing system is...	Download this point patch file	Description
Cisco Prime Network Control System 1.1.0.58	ncs_patch-1.1.0.58-upgrade-12.tar.gz	This patch MUST be applied prior to upgrading to Prime Infrastructure 1.4.
Cisco Prime Network Control System 1.1.1.24	ncs_1_1_1_24-Update.13.4.tar.gz	This patch MUST be applied on top of your existing Prime Infrastructure 1.1.1.24 before upgrading or restoring to Prime Infrastructure 1.4. This patch addresses critical defects in backup and restore.

Table 7 Point Patch Files

If your existing system is...	Download this point patch file	Description
Prime Infrastructure 1.2.0.103 and 1.2.1.12 Patch	PI_1_2_1_12u-Update.1.tar.gz	This patch MUST be applied on top of your existing Prime Infrastructure 1.2.1.12 (migrated from 1.2.0.103), before upgrading or restoring to Prime Infrastructure 1.4. This patch addresses critical defects in backup and restore.
Prime Infrastructure 1.2.1.12	PI_1_2_1_12-Update.1.0.tar.gz	This patch MUST be applied over top of your existing Prime Infrastructure 1.2.1.12 before upgrading or restoring to Prime Infrastructure 1.4. This patch addresses critical defects in backup and restore.
Prime Infrastructure 1.3.0.20	PI_1_3_0_20-Update.1.12.tar.gz	This patch MUST be applied over top of your existing Prime Infrastructure 1.3.0.20 before upgrading or restoring to Prime Infrastructure 1.4.

To install the point patch to your existing system before upgrading, follow these steps:

Step 1 Download the appropriate point patch for your system (see Table 7) to a local FTP server in your environment.

Step 2 Open a console session and log in to the existing server as admin. Enter the password when prompted.

Note If you want to know more about creating a remote repository, see the Setting Up Remote Repositories section of the Prime Infrastructure User Guide: http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.2/user/guide/ManageData.html

Step 3 Copy the patch file to the default local repository:

```
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). You can obtain the source file by using any of the following methods:
  - cdrom—Local CD-ROM drive (read only)
  - disk—Local hard disk storage
  - ftp—URL using a FTP server.
  - http—URL using a HTTP server (read only)
  - https—URL using a HTTPS server (read only)
  - nfs—URL using a NFS server
  - sftp—URL using a SFTP server
  - tftp—URL using a TFTP server
- *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 that you copied.

Migrating to a New Prime Infrastructure 1.4 System

To migrate to a new Prime Infrastructure system:

1. Back Up the Data from the Existing System, page 25
2. Install a New Prime Infrastructure System and Restore the Data from the Backup, page 25

Note To reinstall Prime Infrastructure on a new system or virtual machine, you must e-mail a request to licensing@cisco.com to rehost your license on a new machine. Include your VUDI details and existing license details including the number of licenses in your request.

Back Up the Data from the Existing System

Step 1 Ensure that you have installed the appropriate point patch for your existing system, as explained in the "Installing the Point Patch" section on page 23.

Step 2 Run a backup (using the UI) on the existing system (see the *Cisco Prime Infrastructure Configuration Guide*, Scheduling Automatic Backups). If the system is not running, you can run a backup using the CLI. Use the following command:

```
admin# backup filename repository reponame application NCS
```

Where *filename* is the name you want to assign to the backup file. The resulting backup filename will be in this format: filename_date_time.tar.gpg

Where *reponame* can be located on the local disk or on a remote location.

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

Step 3 Open a console session and log in to the existing server as admin. Enter the password when prompted.

Step 4 If the backup is saved to the local disk repository, copy the file to an external FTP location:

```
copy disk:/reponame/backupfilename ftp://ftpserver/dirpath
```

Install a New Prime Infrastructure System and Restore the Data from the Backup

Step 1 Install Prime Infrastructure 1.4 on a fresh server, as explained in the "Installing Prime Infrastructure" section on page 18.

Note The fresh server must use an OVA that is equal to or larger than the OVA used on the old server.

Step 2 Start a console session and log in as admin to the new Prime Infrastructure 1.4 server.

Step 3 On the new Prime Infrastructure 1.4 server, configure the repository which points to the backup file.

Step 4 Stop the Prime Infrastructure 1.4 server. Enter the **ncs stop** command.

Step 5 Restore the old server backup to the new Prime Infrastructure 1.4 server:

```
admin# restore filename_date_time.tar.gpg repository <reponame> application NCS
```

Where *filename_date_time.tar.gpg* is the name of the backup file.

Where <*reponame*> can be located on the local disk or on a remote location.

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

Step 6 Start the Prime Infrastructure 1.4 server. Enter the **ncs start** command.

Note If you were using external AAA (RADIUS or TACACS) before the upgrade, see the "Renewing Your AAA Settings" section on page 27.

Performing an Inline Upgrade to Prime Infrastructure 1.4

Follow these steps to perform an inline upgrade:

Step 1 Ensure that you have installed the appropriate point patch for your existing system, as explained in the "Installing the Point Patch" section on page 23.

Step 2 Open a console session and log in to the existing server as admin. Enter the password when prompted.

Step 3 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-bundle-1.4.0.x.tar.gz`).
- *disk* is the disk and path to the local defaultRepo.

Step 4 Stop the Prime Infrastructure server. Enter the **ncs stop** command.

Step 5 Run the application upgrade:

```
admin# application upgrade PI-upgrade-bundle-1.4.0.x.tar.gz defaultRepo
```

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

Note Verify that the application is running. Enter the **ncs status** command.

Note If you were using external AAA (RADIUS or TACACS) before the upgrade, see the "Renewing Your AAA Settings" section on page 27.

Managing Disk Space Issues on Prime Infrastructure 1.4 Servers

If you are unable to create a backup after upgrading your existing system, follow these steps to free disk space and create a successful backup:

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 (see the "Back Up the Data from the Existing System" section on page 25).

Creating an SFTP User

You can use Prime Infrastructure server as an SFTP server for which you need to create an SFTP user.

To create an SFTP user, follow these steps:

Step 1 Enable the root patch.

Step 2 Log in to Prime Infrastructure as *root*.

Step 3 Go to the /opt/CSCOlumos/bin directory**.**

Step 4 Run the following command.

```
./sftpconfig.sh
```

This command sets the SSH daemon configurations.

Step 5 Enter the password.

Step 6 If the Naming Service is not configured in Prime Infrastructure, SFTP slows down during user authentication. In this case, it is recommended to disable DNS.

Note The script prompts for a confirmation for disabling the DNS, and later disables the UseDNS option for SSH daemon. This requires the restart of SSH daemon. The script prompts you to confirm.

Step 7 After creating an SFTP user whose username is sftpuser, verify that the external SFTP client can log on using the SFTP user with its credentials

Note After creating an SFTP user, you can disable the root patch. The default port of the SFTP server running on the Prime Infrastructure is 22.

The home directory of the sftpuser is /localdisk/sftp.

The SFTP feature is supported on WLC 7.4.100.0 and later.

Renewing Your AAA Settings

If you were using external RADIUS or TACACS user authentication before upgrading, you must transfer the expanded Prime Infrastructure 1.4 user task list to your AAA server. For information, see the "Setting the AAA Mode" section in the *Cisco Prime Infrastructure 1.2 User Guide*).

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 1.2 User Guide. After you complete these tasks, you are ready to start monitoring and configuring your network.

9 Installation Tasks for the Prime Infrastructure Plug and Play Gateway

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

Prime Infrastructure PnP Gateway Server Requirements

The server requirements for the Prime Infrastructure PnP Gateway OVA are as follows:

- VMware ESXi Server version 4.1.0 or 5.0 is required. Version 5.0 is preferred.
- RAM— 4 GB
- Disk Space—100 GB
- Processors—4 virtual CPUs with 2.93 GHz or faster

Deploying the Prime Infrastructure PnP Gateway OVA

Make sure that all of the system requirements are met before you deploy the OVA. Review the "Prime Infrastructure PnP Gateway Server Requirements" section on page 28 and the "Before You Begin" section on page 18.

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 Prime Infrastructure PnP Gateway

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

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

Step 2 Repeat Step 2 through Step 3 from the "Installing the Server" section on page 20.

Step 3 After you enter the values, the installer tests the network configuration parameters. If the tests are successful, the installer begins the 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.

Setting Up the Prime Infrastructure Plug and Play Gateway

To set up the Prime PnP Gateway OVA, follow these steps:

Note Make sure that all of the system requirements are met before you set up the Prime Infrastructure PnP Gateway OVA. You can review the "Prime Infrastructure PnP Gateway Server Requirements" section on page 28.

Note You should generate the Secure Socket Layer (SSL) key and certificate for the Prime Infrastructure PnP gateway, and then copy the certificate to the Prime Infrastructure PnP gateway VM. For more information about getting a Prime Infrastructure certificate, see Getting the Prime Infrastructure Certificate, page 31 section. Also, you need to obtain the Prime Infrastructure server certificate. Use the **copy** command to copy the certificates from an external location to the disk:/. The "disk:/" refers to the /localdisk directory on the linux file system.

Step 1 Log in to the Prime PnP 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 PnP gateway server.
- Hostname—This fully qualified hostname should be used as the IP host configuration in the device.
- SSL Key File—The private key generated for the PnP gateway server (see the "Generating a Server Certificate" section on page 30).
- SSL Server Certificate—The self/CA signed server certificate for PnP gateway, (see the "Generating a Server Certificate" section on page 30).
- Prime Infrastructure SSL Certificate—The self/CA signed server certificate for Prime Infrastructure.
- HTTPS/SSL Encryption—The secure HTTPS/SSL encryption is enabled by default.
- Port Number—The default port number is 443.
- Authentication—By default the authentication is disabled.
- CNS Event—The CNS event configuration that will be deployed on the device for dynamic port allocation.
- IP addresses—Use the default value.
- Event Port Parameter—Use the default value.
- Prime Infrastructure hostname—Specify the IP address of the Prime Infrastructure server.
- Prime Infrastructure Event Port Parameter—Use the default value.
- Log—Use the default value.
- Data directory—Use the default value.

Step 4 The console displays the following:

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

Enter IP Address of PnP Gateway server [192.168.1.31]
Enter the fully qualified host name of PnP Gateway server [abc.def.com]
Enter absolute pathname of PnP Gateway server key file: []/localdisk/server.key
Enter absolute pathname of PnP Gateway server certificate file: []/localdisk/server.crt
Enter absolute pathname of Prime Infrastructure server certificate file: []/localdisk/ncsserver.crt
Enable secure HTTPS/SSL encryption to secure PnP Gateway Web GUI (y/n) [y]
Enter port number for https web access: [443]

        Enabling clear text operation
```

```
        between PnP Gateway and device(s) increases security risk.

Enable clear text operation between device CNS Agent and PnP Gateway (y/n) [y]
Enter Tomcat internal port number: [8009]
Enter Tomcat shutdown port number: [8005]

Authentication settings:
========================
        IOS Devices are normally authenticated before being allowed to
        connect to the Event Gateway/Config Server. Disabling
        authentication will increase security risk.

Enable authentication (y/n)? [n]
Enter number of Event Gateways that will be started with crypto operation: [5]
Enter port number for http web access: [80]
Enter number of Event Gateways that will be started with plaintext operation: [5]

        The CNS Event command configures how the managed devices should
        connect to this particular PnP 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 PnP 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 PnP 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]

        Enter IP address for CNS Gateway to listen to.
        Enter 1 to have CNSGateway listens to all IP addresses.
IP addresses:[1]
Enter PnP Gateway Event Port Parameter: [62616]
Enter Prime Infrastructure hostname: []192.168.1.32
Enter Prime Infrastructure Event Port Parameter: [61617]
Enter base directory for PnP Gateway log : [/var/log]

        Data directory contains Template and Image files

Enter data directory for PnP Gateway : [/var/KickStart]


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

Step 5 To check the status of the Prime Infrastructure PnP gateway server, log in to Prime Infrastructure PnP 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 Prime Infrastructure PnP gateway server status will be displayed.

Generating a Server Certificate

To generate a server certificate, follow these steps:

Step 1 Use the openssl toolkit to generate an RSA Private Key and CSR (Certificate Signing Request). The RSA Private Key is a 1024 bit key which is stored in a PEM format. The following example shows how to generate the RSA key.

```
openssl genrsa -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.................................++++++
e is 65537 (0x10001)
```

Step 2 After generating the RSA key, generate the CSR. The following example shows how to generate the CSR.

```
openssl req -new -key server.key -out server.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:SanJose
Organization Name (eg, company) [My Company Ltd]:Cisco Systems
Organizational Unit Name (eg, section) []:Org
Common Name (eg, your name or your server's hostname) []:<pnp gateway server fully qualified hostname>
Email Address []:
```

Note Make sure the generated certificate is not shared and that it is protected.

Step 3 The CSR file can be used to generate a signed server certificate from a certificate authority (CA) or you can generate a self-signed certificate.

Step 4 To generate a self-signed certificate, use the following command:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
Signature ok
subject=/C=US/ST=California/L=SanJose/O=Cisco Systems/OU=Org/CN=<pnp gateway server fully qualified
hostname>
Getting Private key
```

Getting the Prime Infrastructure Certificate

To get the Prime Infrastructure certificate, follow these steps:

Step 1 Log into Prime Infrastructure server that have open SSL installed.

Note Ensure to run Prime Infrastructure before this is executed

Step 2 Use the following command to get the certificate:

```
openssl s_client -connect "<PI SERVER ADRRESS>:61617" 2>&1 | sed -ne '/-BEGIN CERTIFICATE-/,/-END
CERTIFICATE-/p' > <CERTIFICATE_FILE_NAME>
```

Step 3 Copy the certificate file name to the Prime Infrastructure Plug and Play gateway.

10 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 8 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 site profiles	• **Operate > Site Profiles & Maps** • **Operate > Device Workcenter**	Getting Started
Setting up port monitoring	**Operate > Port Grouping**	Getting Started
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 > *Templates***	Operating the Network
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

11 Removing Prime Infrastructure

Note Removing Prime Infrastructure using this 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.

To remove Prime Infrastructure on the local server, follow these steps:

Step 1 Right-click the Prime Infrastructure virtual appliance from the VMware vSphere client.

Step 2 Choose **Remove from Disk**.

12 Related Documentation

You can access the additional Cisco Prime Infrastructure documentation at:

http://www.cisco.com/en/US/products/ps12239/tsd_products_support_series_home.html

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

13 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.
