Cisco Prime Infrastructure FIPS 3.2 Quick Start Guide

Revised: March 29, 2018

1 Overview

This section provides basic information about the product and this Guide.

Related Topics

- About This Guide
- Product Overview
- About Cisco Prime Infrastructure Licensing

About This Guide

This guide describes how to install Cisco Prime Infrastructure 3.2 FIPS as an OVA on VMware, Cisco Prime Infrastructure as an ISO on Hyper-V Virtual Machine.Prime Infrastructure is also available as a hardware appliance. For information on how to install the appliance, see the *Cisco Prime Infrastructure 3.2 Appliance Hardware Installation Guide*.This guide also describes about the Upgrade & Migration from the supported previous release Cisco Prime Infrastructure versions to Cisco Prime Infrastructure 3.2 FIPS.

For information about configuring and managing this product, see the *Cisco Prime Infrastructure FIPS 3.2 Administrator Guide* and the *Cisco Prime Infrastructure FIPS 3.2 User Guide*.

Product Overview

Prime Infrastructure provides a single integrated solution for comprehensive lifecycle management of the wired or 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.

For:

- An overview of Prime Infrastructure features and benefits, see the latest Cisco Prime Infrastructure Data Sheets.
- Information about frequently used Prime Infrastructure features, see the *Cisco Prime Infrastructure FIPS 3.2 User Guide*.
- Information about features intended for administrators, see the *Cisco Prime Infrastructure FIPS 3.2 Administrator Guide.*

About Cisco Prime Infrastructure Licensing

Prime Infrastructure licenses control the features that you can use and the number of devices you can manage using those features. For more information about:

- Cisco Prime Infrastructure license types and how to order them, see the *Cisco Prime Infrastructure 3.2 Ordering and Licensing Guide*.
- How to apply purchased licenses, see the *Cisco Prime Infrastructure FIPS 3.2 Administrator Guide.*

2 Before You Install

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

Related Topics

- Understanding System Requirements

- Scaling Prime Infrastructure

Understanding System Requirements

Prime Infrastructure comes in two main forms:

- **Virtual**: The Prime Infrastructure virtual appliance is packaged as an Open Virtualization Archive (OVA) file, which must be installed on a user-supplied, qualified server running VMware ESXi. This form allows you to run on the server hardware of your choice. You can also install the virtual appliance in any of four configurations, each optimized for a different size of enterprise network. For hardware requirements and capacities for each of the virtual appliance's size options, see Virtual Appliance Options.
- **Hyper V**: Cisco Prime Infrastructure for Microsoft Hyper-V extends Cisco networking benefits to Microsoft Windows Server Hyper-V deployments. For deploying Cisco Prime Infrastructure on Hyper-V Virtual appliance, see the Cisco Prime Infrastructure 3.2 Installation and Migration Guide for Microsoft Hyper-V.
- **Physical**: The physical appliance is packaged as a rack-mountable server, with Prime Infrastructure pre-installed and configured for you. For physical appliance hardware specifications and capacities, see Physical Appliance Options.

Virtual Appliance Options

During installation, you can choose one of four deployment configuration options. Table 1 summarizes the minimum server requirements for each option.

Table 1 Prime Infrastructure Minimum Server Requirements

Requirement	Express	Express-Plus	Standard	Professional
VMware Version	ESXi 5.5 or 6.0	ESXi 5.5 or 6.0	ESXi 5.5 or 6.0	ESXi 5.5 or 6.0
Virtual CPUs[1]	4	8	16	16
Memory (DRAM)	12 GB	16 GB	16 GB	24 GB
HDD Size	300 GB	600 GB	900 GB	1.2 TB
Throughput (Disk IOPS)	200 MB/s	200 MB/s	200 MB/s	320 MB/s

[1] 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.

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

Physical Appliance Options

Prime Infrastructure is available on the Cisco Unified Computing System (UCS) Appliance. Prime Infrastructure 3.2 FIPS is not supported on the PRIME-NCS-APL-K9 (also known as "Gen 1"). Prime Infrastructure 3.2 FIPS is supported on Cisco Prime Infrastructure Appliance (Gen 2, UCS based). The physical appliance specifications are as follows:

Hardware Specifications	CPU (cores/threads)	10 C/20 T
	Memory	64 GB
	Disk Capacity	4x900 GB
	RAID Level RAID	10
	Disk I/O Speed	320 MBps

System Users	Concurrent GUI clients	100
	Concurrent API clients	5

Prime Infrastructure is also available pre-installed on Cisco-supplied hardware as a physical appliance. See the Cisco Prime Infrastructure 3.2 Appliance Hardware Installation Guide for more information.

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

Improving Performance on Appliances

For better performance on the Prime Infrastructure Appliance (Gen 2, UCS based), make sure you configure the virtual drive Write Policy to Write Back Good BBU. To configure the virtual drive Write Policy, follow these steps:

Step 1 Launch the CIMC web interface (see *Setting Up the Appliance* in the *Cisco Prime Infrastructure Appliance Hardware Installation Guide*).

Step 2 Click the **Storage** tab, click on the SAS Modular Controller name, click the **Virtual Drive** tab, then click **Edit Virtual Drive**.

Step 3 Click **OK** on the dialog box that appears.

Step 4 In the Write Policy field, select **Write Back Good BBU**, then click **Save Changes**.

If you are running ESX on custom hardware that has a RAID controller, we recommend you configure the following RAID settings to optimize Prime Infrastructure performance and redundancy:

- RAID 10
- RAID cache of at least 2 GB
- Use write through mode with battery backup

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 55 or later
  - Microsoft Internet Explorer 11 (No plug-ins are required.)
  - Mozilla Firefox ESR 52
  - Mozilla Firefox 52 or later
- Display resolution—Prime Infrastructure supports 1366 x 768 or higher, but we recommend that you set the screen resolution to 1600 x 900.

FIPS Mode Installation

Prime Infrastructure 3.2 offers a direct installation in FIPS mode. This option is intended for customers who require the products they use to be compliant with FIPS-140-2 standards.

Federal Information Processing Standards (FIPS) are United States government computer security standards. The FIPS-140-2 series specify requirements for cryptography modules. For a more complete description, see http://www.nist.gov/itl/fips.cfm.

To verify whether the Prime Infrastructure system is operating in FIPS mode, use the system CLI command show security-status. For more information, see Check On Server Security Status in the *Cisco Prime Infrastructure FIPS 3.2 Administrator Guide*.

When deciding whether to install in FIPS Mode, be aware that:

- Installing Prime Infrastructure in FIPS Mode disables use of certain capabilities in order to comply with the cryptographic security requirements of FIPS-140-2. For more details, see the Best Practices: Server Security Hardening in the *Cisco Prime Infrastructure FIPS 3.2 Administrator Guide*.
- Both Wireless and Wired management solution functionality in Prime Infrastructure is certified for FIPS compliance.
- Refer section "Features that are not supported by FIPS" for unsupported functionalities in FIPS release.
- In FIPS mode, you cannot enable root shell, and access to the root shell CLI is restricted.
- You cannot restore Prime Infrastructure 3.2 FIPS backup to 3.2 or 3.3 release version. You can restore 3.2 FIPS backup only on Prime Infrastructure 3.2 FIPS server.

Scaling Prime Infrastructure

Prime Infrastructure comes with a variety of server installation options (see Understanding System Requirements). Ensure that you select an option appropriate for the size and complexity of your network.

Table 2 lists the maximum number of devices, clients, events, NetFlow-related data flows, and other scale parameters for each option. For example, the Professional option can manage 200,000 wireless clients and 50,000 wired clients.

Table 2 Supported Scale for Prime Infrastructure Installation Options (includes Assurance)

Parameter (Maximums)	Express	Express-Plus	Standard	Professional	Hardware Appliance (Gen 2)[1]
Maximum number of devices (combination of wired and wireless devices)	500	3000	10,000	14,000	24,000
Unified APs	300	2500	5000	10,000	20,000
Autonomous APs	300	500	1500	2500	3,000
Wired Devices	300	1000	6000	10,000	13,000
NAMs	5	5	500	800	1000
Controllers	5	25	500	800	1,000
Wired Clients	6000	50,000	50,000	50,000	50,000
Wireless Clients	4000	30,000	75,000	150,000	200,000
Cisco Mobility Services Engine (MSE)	1	1	6	10	12
Changing Clients (every 5 minutes)[2]	1000	5000	25,000	30,000	40,000
Events Sustained Rate (events per second; includes syslogs, traps, and system events)	100	100	300	500	1000
Syslog Rate	70	70	210	350	600
Trap Rate	20	20	60	100	300
System Event Rate	10	10	30	50	100
NetFlow Rate (flows per second)[3]	3000	3000	16,000	40,000	80,000
Supported Hourly Host Records	144,000	720,000	2,100,000	6,000,000	12,000,000
Interfaces	12,000	50,000	250,000	250,000	350,000
NAM Data Polling Enabled	5	5	20	30	40
Polling Interfaces (polling of trunk ports)	2400	8000	48,000	100,000	100,000
Number of Sites per Campus	200	500	2500	2500	2500
Groups: User-Defined + Out of the Box + Device Groups + Port Groups	50	100	150	150	150

Table 2 Supported Scale for Prime Infrastructure Installation Options (includes Assurance) (continued)

Parameter (Maximums)	Express	Express-Plus	Standard	Professional	Hardware Appliance (Gen 2)[1]
Location Group	100	100	1000	1000	1000
Virtual Domains	100	500	750	750	750

1. Compliance is supported on the Standard, Professional virtual appliance (OVA) and the Gen 2, UCS-based physical appliance only. It is not supported on: Express, Express Plus, OVAs that have been resized to Standard or Professional. If you are running Prime Infrastructure on an unsupported OVA or physical appliance and want to enable Compliance, you must perform a fresh install of the 3.2 Standard or Professional OVA or Gen2 UCS appliance, then use backup/restore to migrate data from your old server to the new server. See Enable Compliance Services in the Cisco Prime Infrastructure 3.2 FIPS Administrator Guide
2. Changing Clients are wireless users who are roaming across APs or disassociating and associating to APs.
3. The NetFlow rate depends on the number of unique clients in the flows. The supported NetFlow rate is also based on the translated number of hourly host records (or unique combinations of server/client and applications) per day.

Note The supported number of FIPS/IPSEC capable device count is 2500.

Scaling for Service Provider Wi-Fi

Table 3 lists the Service Provider Wi-Fi parameters.

Table 3 Scaling for Service Provider Wi-Fi

Parameter	Maximum Supported
Number of APs	20,000
Number of clients	100,000
Sustain trap rate	300/sec
Burst trap rate	400/sec for 10-minute duration

Scaling for Data Center

Table 4 lists the Data Center parameters.

Table 4 Scaling Data Center

Parameter		Standard	Professional	Hardware Appliance (Gen 2)
Data Center Switches	Cisco Nexus devices	2500	3000	3000
Virtual infrastructure	Cisco UCS B-Series devices, Cisco UCS C-Series devices	2000	2000	2000
	VMware vCenters	7	14	14
	VMware Hosts	472	1219	1219
	VMware Clusters	8	15	15
	Virtual machines	5500	12,000	12,000
	Total	10,587	18,648	18,648

3 Installation Options

Prime Infrastructure provides the following installation options:

- New installation on a virtual machine—See Before You Begin Installation on a Virtual Machine.
- New installation on a physical appliance. Prime Infrastructure comes preinstalled on physical appliances, or you can install an image on an existing appliance. See Setting Up Prime Infrastructure on a Virtual Machine or Physical Appliance.
- Upgrade a previous version of Prime Infrastructure—See Upgrading From Previous Releases of Prime Infrastructure.

Before You Begin Installation on a Virtual Machine

Before installing Prime Infrastructure on a virtual machine, you must:

- Ensure that VMware ESXi is installed and configured on the machine that you plan to use as the Prime Infrastructure server. See the VMware documentation for information on setting up and configuring a VMware host. If you are using VMware ESX 5.5, you must use vSphere Client or ESX5.5U2 (or later) Client to manage the virtual machine. Do not edit the virtual machine settings and do not extend or manually add additional disks to the configuration.
- Check that the installed VMware ESXi host is reachable. 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.
- Ensure that the Prime Infrastructure OVA is saved to the same machine where your VMware 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.

Installing Prime Infrastructure on a Virtual Machine

The following steps explain how to install Prime Infrastructure on a virtual machine. Make sure that all of the system requirements are met before you deploy the OVA. Review the sections Understanding System Requirements and Before You Begin Installation on a Virtual Machine.

Step 1 Launch your VMware vSphere Client and connect to the ESXi host or vCenter server.

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

Step 3 Click **Browse** to access the location where you have saved the OVA file on your local machine, then click **Next**.

Step 4 Verify the details on the OVF template details page, then click **Next**.

Step 5 In the End User License Agreement window, click **Accept**, then click **Next**.

Step 6 In the Name and Location window, specify:

- In the Name field, enter the name of the new virtual machine.
- In the Inventory Location area, select the appropriate folder. (If the vSphere Client is connected directly to an ESXi host, this option does not appear.)

Step 7 Click **Next**.

Step 8 In the Deployment Configuration window, select the desired configuration (for example, Express, Standard, Professional, etc.) and view the resources required for the configuration you selected.

Note We recommend you reserve 100% of CPU and memory resources for optimal performance.

Step 9 Click **Next**.

Step 10 In the Host/Cluster window, select the host or cluster on which you want to deploy the OVF template, then click **Next**. (If the vSphere Client is connected directly to an ESXi host, this option does not appear.)

Step 11 In the Storage window, select the datastore that has the required space requirements described in Understanding System Requirements, then click **Next**.

Step 12 In the Disk Format window, select **Thick Provision Lazy Zeroed** to provision the virtual machine virtual disks, then click **Next**. Do not select Thin Provision because if there is no free disk space when the virtual machine needs it, Prime Infrastructure will fail.

Step 13 In the Network Mapping window, select a network for the virtual machine to use, then click **Next**.

Step 14 In the Ready to Complete window, review your settings, select **Power on After Deployment**, then click Finish.

Depending on your network speed and the IOPS of the server, the deployment can take a few minutes to complete.

Setting Up Prime Infrastructure on a Virtual Machine or Physical Appliance

Prime Infrastructure comes preinstalled on physical appliances, or you can install an image on an existing appliance. Complete the following steps to set up and start Prime Infrastructure on a virtual machine or physical appliance.

Step 1 If you are using a virtual machine and it is not already powered on, in the VMware vSphere Client, right-click the deployed virtual appliance and choose **Power > Power On**.

Step 2 Click the **Console** tab.

After the server boots up, you'll see the localhost login prompt.

Step 3 At the localhost login prompt, enter **setup**.

Step 4 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 addresses or host names of the secondary NTP servers to be used when the primary is not available.
- System Time Zone—The time zone code you want to use. See *Time Zones Supported By Cisco Prime Infrastructure* in the *Cisco Prime Infrastructure FIPS 3.2 User Guide*.
- 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 the console or SSH. You can accept the default, which is admin.
- Password—Enter the admin user password and then confirm it.

Tip Keep your Prime Infrastructure password in a safe place. If you forget the password, see *How to Recover Administrator Passwords on Virtual Appliances* in the *Cisco Prime Infrastructure FIPS 3.2 Administrator Guide*.

Step 5 When you are done entering these values, the installer application tests the network configuration parameters that you entered. If the tests are successful, it begins installing Prime Infrastructure.

Step 6 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 secondary server in a high availability implementation. You will be prompted to provide an authentication key to be used for high availability registration. If you enter **no** at the prompt, the server will act as the primary server (standalone) and the installation will proceed with the following prompts:

- Web Interface Root Password—Enter and confirm the password used for the default root administrator. This is the account used to log in to the Prime Infrastructure web user interface for the first time and set up other user accounts.

Step 7 Select **Yes** to proceed with the installation, or select **No** to re-enter high availability and FIPS mode options.

Step 8 When the installation is complete, the appliance reboots and you are presented with a login prompt.

Step 9 Log in to the virtual machine using the “admin” username and password that you specified in Step 4.

Step 10 Run the **ncs status** command (see *Check Prime Infrastructure Server Status* in the *Cisco Prime Infrastructure FIPS 3.2 Administrator Guide*) to verify that the processes have restarted. You should see the following process statuses:

- All Processes are up and running.
- FIPS (Standalone): FTP, TFTP, and PnP are disabled. Other processes are running.

Features that are not supported by FIPS

Cisco Prime Infrastructure 3.2 FIPS does not support the following features:

- Plug and Play deployment
- APIC-EM integration with Plug and Play
- APIC-EM integration with IWAN
- Operation Center
- Maps - Google Earth
- CMX integration with Prime Infrastructure
- Root Shell access (It is disabled by default and cannot be enabled.)
- TFTP and FTP
- LMS Migration
- Collection of telemetry data
- vCenter integration
- Config Archive (Vlan.dat fetch)
- UCS device
- Packet Capture
- MSE High Availability
- Single Sign-On Authentication (SSO)
- Mobility Service Engine (MSE)

IPSec Tested Devices

Table 5 lists IPSec devices that are tested for Prime Infrastructure 3.2 FIPS Release:

Table 5 IPSec Tested Devices

Cisco Tested Devices with IPSEC configurations	Images Used
Cisco 4321 Integrated Services Router	isr4300-universalk9.03.17.02.S.156-1.S2-std.SPA.bin isr4300-universalk9.03.16.00c.S.155-3.S0c-ext.SPA.bin
Cisco Catalyst 6506-E Switch	s72033-advipservicesk9-mz.151-2.SY6.bin s72033-adventerprisek9-mz.151-2.SY4a.bin

Cisco 800 Series Routers	c800-universalk9-mz.SPA.155-3.M3.bin c800-universalk9-mz.SPA.155-3.M5.bin c800-universalk9-mz.SPA.156-3.M2.bin
Cisco Catalyst 3850 Series Switches	cat3k_caa-universalk9.16.03.03.SPA.bin cat3k_caa-universalk9.16.05.01a CAT3K_CAA-UNIVERSALK9-M.bin
Cisco Catalyst 3650-24PS-S Switch	cat3k_caa-universalk9.16.05.01a.SPA.bin
Cisco Catalyst 3750 Series Switches	c3750e-universalk9-mz.152-4.E4.bin
Cisco Catalyst 3560 Series Switches	c3560e-ipbasek9-mz.150-2.SE9.bin c3560e-ipbasek9-mz.150-2.SE10a.bin
Cisco ASR 1000 Router Series	asr1001x-universalk9.03.16.01a.S.155-3.S1a-ext.SPA.bin
Cisco 5520 Wireless Controller	AIR-CT5520-K9-8-3-140-0.aes **Note** For more information see *Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless Release 8.3.140.0.*
Cisco 8540 Wireless Controller	AIR-CT8540-K9-8-3-140-0.aes
Cisco 8510 Wireless Controller	AIR-CT8500-K9-8-3-140-0.aes
Cisco 5508 Wireless Controller	AIR-CT5500-K9-8-3-140-0.aes
Cisco Catalyst 2960-S Series Switches	c2960s-universalk9-mz.152-2.E2
Cisco Catalyst 2960-X Series Switches	c2960x-universalk9-mz.152-2.E
Cisco ASR 1000 Router Series	asr1000rpx86-universalk9.16.04.01.SPA.bin

Before You Migrate Your Data

You should check the validity of your Prime Infrastructure backup data by setting up an additional Prime Infrastructure server (either a spare Prime Infrastructure appliance or a new Prime Infrastructure virtual machine) and perform the restore operation as explained in *Restore an Application Backup* in the *Cisco Prime Infrastructure FIPS 3.2 Administrator Guide*. If you do not have an additional Prime Infrastructure system to validate the backup, take at least two backups to reduce the risk of losing data.

Note You cannot restore Prime Infrastructure 3.2 FIPS backup to 3.2 or 3.3 release version. You can restore 3.2 FIPS backup only on Prime Infrastructure 3.2 FIPS server.

If the restore operation does not work, or there are problems with the backed up image, try taking another backup from a production system, or try restoring from an earlier Prime Infrastructure backup.

If you cannot create a verified backup before installing this version of Prime Infrastructure, open a support case with Cisco TAC.

Migrating Data From Previous Releases of Prime Infrastructure

You can migrate from the Prime Infrastructure 2.2.0.0.158 version to Prime Infrastructure 3.2 FIPS:

See Before You Migrate Your Data before you start the following steps to restore your data from Prime Infrastructure 2.2.0.0.158 to your newly installed Prime Infrastructure 3.2 FIPS server:

Step 1 Configure the new Prime Infrastructure host to use the same remote backup repository as the old host. For details, see *Use a Remote Backup Repository* in the *Cisco Prime Infrastructure FIPS 3.2 Administrator Guide*.

Step 2 Restore the application backup on the remote repository to the new host, as explained in *Restore an Application Backup* in the *Cisco Prime Infrastructure FIPS 3.2 Administrator Guide*.

Step 3 When the process 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/restored Prime Infrastructure server.
- If you are using Prime Infrastructure to manage Cisco Wireless LAN Controllers, see Resynchronizing WLC Configurations after Migration.
- Synchronize your devices as explained in *Synchronize Devices* in the *Cisco Prime Infrastructure FIPS 3.2 User Guide*.

Step 4 After the new Prime Infrastructure 3.2 FIPS server is operational, decommission your previous server.

Assurance Data after Migration

After restoring Prime Infrastructure 2.2.0.0.158 FIPS support server on a new Prime Infrastructure 3.2 FIPS supported virtual machine or hardware appliance, your Assurance license is automatically applied to the new server.

When you move your data to Prime Infrastructure 3.2 FIPS, the following Assurance data is not migrated:

- Raw NetFlow information
- Custom NetFlow reports
- Packet capture files
- Processed non-aggregated data, such as PFR data and URLs

5-minute, 1-hour, and 1-day aggregated data is migrated from Prime Infrastructure 2.2.0.0.158 FIPS support server.

Resynchronizing WLC Configurations after Migration

After you restore the backup of the previous version on the 2.2.0.0.158 version of Prime Infrastructure, your server's records of Cisco Wireless LAN Controller configurations might be out of sync with the configurations stored on those devices. Resynchronize them using the following steps before continuing.

Step 1 Log in to Prime Infrastructure.

Step 2 Choose **Inventory > Network Devices > Wireless Controller**. Prime Infrastructure displays a list of all the controllers it is managing, including all Cisco WLCs.

Step 3 Select a device, then click **Sync**.

Step 4 Repeat steps 2 and 3 for all your other WLCs.

4 Post-Installation Tasks

Follow the instructions in this section once you have finished installing Prime Infrastructure.

- Logging in to the Prime Infrastructure User Interface
- Getting Started Using Prime Infrastructure

Logging in to the Prime Infrastructure User Interface

We strongly recommend you use signed certificates to ensure secure connections between clients and the Prime Infrastructure server. For information about creating a signed certificate, see I*mport Subject Alternate Names (SAN) CA-Signed Certificates* in the *Cisco Prime Infrastructure FIPS 3.2 Administrator Guide*.

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 Understanding System Requirements) 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.

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 Check the **Login Disclaimer Acknowledgment** check box.

Step 4 Enter the *root* administrator username and password, as specified when Setting Up Prime Infrastructure on a Virtual Machine or Physical Appliance.

Step 5 Click **Login** to log in to Prime Infrastructure. The login button will be grayed out if you do not check the **Login Disclaimer Acknowledgment** check box. A toast notification indicating the client IP address, last successful login time, and number of login attempts failed for the last 24 hours is displayed.

The user interface is now active and available for use. The home page appears. 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 6 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 top-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 user interface session, your session ends, and the browser displays this message: "The page cannot be displayed." Your session does not re-associate to Prime Infrastructure when the server restarts. You must start a new Prime Infrastructure session.

Getting Started Using Prime Infrastructure

After you install Prime Infrastructure, you must perform additional tasks to begin managing your network. If you are an administrator, see the following sections in the *Set Up the Prime Infrastructure Server* in the *Cisco Prime Infrastructure FIPS 3.2 Administrator Guide:*

- Configure Data Sources for Cisco Prime Infrastructure With Assurance, including enable NetFlow and Performance Agent.
- How to Manage Disk Space Issues on Prime Infrastructure servers.
- Renew AAA Settings After Installing a New Prime Infrastructure Version
- Prime Infrastructure Software Updates

For information about installing the Cisco Plug and Play Application, see the *Cisco Plug and Play Application Solutions Guide*.

Users should complete the tasks listed in the G*et Started with Prime Infrastructure chapter* of the *Cisco Prime Infrastructure FIPS 3.2 User Guide*. After you complete these tasks, you are ready to start monitoring and configuring your network.

5 Reference Information

The following sections provide reference information about Prime Infrastructure and its support options.

- Ports Used by Prime Infrastructure and Assurance
- Removing the Prime Infrastructure Virtual Appliance
- Navigation and Documentation Reference
- Related Documentation
- Obtaining Documentation and Submitting a Service Request

Ports Used by Prime Infrastructure and Assurance

Table 6 lists the ports used by Prime Infrastructure and Assurance. These ports must be open in firewalls if you are using these services.

Table 6 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
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.
500	UDP	Devices to server	IPSec communication
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
8082	TCP	Client to server	Health Monitor web interface, Apache/Tomcat JSP engine
8087	TCP	Client to server	Secondary server software update page
9991	UDP	Devices to server	NetFlow data receiver **Note** Used when the Plug and Play Gateway is integrated with the Prime Infrastructure server.
9992	TCP	Lync server to Prime Infrastructure server	Lync data receive
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)

Table 6 Ports Used by Prime Infrastructure and Assurance (continued)

Port	Protocol	Direction	Usage
11011	TCP	Endpoints to server	Plain text dispatcher port for the Plug and Play Gateway **Note** Used when the Plug and Play Gateway is integrated with the Prime Infrastructure server.
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
61617	TCP	Server to endpoints	SSL port for Java Message Service connections **Note** Used by the Prime Infrastructure Plug And Play Gateway only.

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. For other methods of removal, see *How to Remove Prime Infrastructure* in *Cisco Prime Infrastructure FIPS 3.2 Admin Guide*.

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.

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 the *Cisco Prime Infrastructure FIPS 3.2 User Guide*.

Table 7 Navigation and Documentation Reference

Task	Navigation in Cisco Prime Infrastructure	Section in Cisco Prime Infrastructure User Guide
Adding licenses	**Administration** > **Licenses and Software Updates** > **Licenses**	Getting Started
Managing Users	**Administration** > **Users** > **Users, Roles & AAA**	Controlling User Access
Discovering your network	**Inventory** > **Device Management** > **Discovery**	Getting Started
Setting up virtual domains	**Administration** > **Users** > **Virtual Domains**	Getting Started
Using monitoring dashboards	**Dashboard** > **Overview** > **General**	Operating the Network
Using templates for configuring and monitoring	**Configuration** > **Templates** > **Features & Technologies** or **Monitor** > **Monitoring Tools** > **Monitoring Policies**	Designing the Network
Viewing alarms	**Monitor** > **Monitoring Tools** > **Alarms and Events**	Monitoring Alarms

Table 7 Navigation and Documentation Reference (continued)

Task	Navigation in Cisco Prime Infrastructure	Section in Cisco Prime Infrastructure User Guide
Maintaining device configurations	**Inventory > Device Management > Configuration Archive**	Maintaining Device Configuration Inventory
Preconfiguring devices that will be added to your network in the future	**Configuration > Plug and Play > Dashboard**	Getting Help Setting Up and Configuring Devices

Related Documentation

The *Cisco Prime Infrastructure 3.2 Documentation Overview* lists all documentation 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.

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.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.