



Cisco Prime Infrastructure 3.0 Quick Start Guide

- 1 [Overview, page 2](#)
- 2 [Before You Install, page 3](#)
- 3 [Installing Cisco Prime Infrastructure, page 9](#)
- 4 [Post-Installation Tasks, page 13](#)
- 5 [Reference Information, page 15](#)

Revised: 2 March 2016

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 Overview

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

Related Topics

- [About This Guide](#)
- [Product Overview](#)
- [Key Features](#)
- [About Cisco Prime Infrastructure Licensing](#)

About This Guide

This guide describes how to install Cisco Prime Infrastructure 3.0.

For detailed information about configuring and managing this product, see the [Cisco Prime Infrastructure 3.0 Administrator Guide](#) and the [Cisco Prime Infrastructure 3.0 User Guide](#).

This guide explains how to install Prime Infrastructure as an OVA on customer-supplied hardware. Prime Infrastructure is also available as a hardware appliance. For information on how to install the appliance, see the [Cisco Prime Infrastructure 3.0 Appliance Hardware Installation 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.

Key Features

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 3.0 User Guide](#).
- Information about features intended for administrators, see the [Cisco Prime Infrastructure 3.0 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 3.0 Ordering and Licensing Guide](#).
- How to apply purchased licenses, see the [Cisco Prime Infrastructure 3.0 User Guide](#).

2 Before You Install

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

Related Topics

- [Understanding System Requirements](#)
- [Scaling Prime Infrastructure](#)
- [If You Are Upgrading From Previous Releases of 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](#).
- **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 5.1 or 5.5	ESXi 5.1 or 5.5	ESXi 5.1 or 5.5	ESXi 5.1 or 5.5
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.

Prime Infrastructure is also available pre-installed on Cisco-supplied hardware as a physical appliance. See the [Cisco Prime Infrastructure 3.0 Appliance Hardware Installation Guide](#) for more information.

For maximum management capacities for each installation option, see [Scaling Prime Infrastructure](#).

Physical Appliance Options

Prime Infrastructure is available on the Cisco Unified Computing System (UCS) Appliance. Prime Infrastructure 3.0 is not supported on the Cisco Prime Infrastructure Physical Appliance (Gen 1). Prime Infrastructure 3.0 is supported on Cisco Prime Infrastructure Physical Appliance (Gen 2, UCS based). You can upgrade a Prime Infrastructure Physical Appliance (Gen 2, UCS Based) appliance running Prime Infrastructure 2.2.x to Prime Infrastructure 3.0. [Table 2](#) describes the physical appliance options.

Table 2 Prime Infrastructure Physical Appliance Options for the Prime Infrastructure Physical Appliance (Gen 2, UCS based)

Physical Appliance Options	Appliance Image Format	Bare Metal/ISO
	Equivalent 1.x Option	Physical Appliance
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
Devices	Maximum unified APs	20,000
	Maximum autonomous APs	3000
	Maximum WLAN controllers	1000
	Maximum wired (switches, routers)	13,000
	Maximum MSEs	25
	NAMs	1000
	Maximum number of devices	24,000

Table 2 Prime Infrastructure Physical Appliance Options for the Prime Infrastructure Physical Appliance (Gen 2, UCS based)

Clients	Wired clients	50,000
	Wireless clients	200,000
	Changing clients (every 5 min.)	40,000
Monitoring	Events sustained rate (events/sec)	1000
	Netflow rate (flows/sec)	80,000
	Max interfaces	350,000
	Max NAM polling data enabled	40
System	Max number sites/campus	2500
	Max groups ¹	150
	Max virtual domains	1200
System Users	Concurrent GUI clients	50
	Concurrent API clients	5

1. “Maximum groups” is the total number of all user-defined groups, out-of-the-box groups, device groups, and port groups

Improving Performance on Gen2 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**.
-

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 40 or later
 - Microsoft Internet Explorer 10, or 11 (No plug-ins are required.)
 - Mozilla Firefox ESR 31, 38
 - Mozilla Firefox 35 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.

If you are using Google Chrome version 44, you may get an error that says “ERR_INSECURE_RESPONSE”. This is a known Chrome issue, which you can read about at the following URL:

<https://groups.google.com/a/chromium.org/forum/#!topic/chromium-discuss/4ctMmhOTDFg>.

Google is planning to fix this issue in Chrome version 45. See the following URL for status:

<https://code.google.com/p/chromium/issues/detail?id=473390>

To work around this issue, use signed certificates (recommended) or downgrade Chrome to version 43. For information about creating a signed certificate, see [Obtaining and Importing CA-Signed Certificates](#) in the *Cisco Prime Infrastructure 3.0 Administrator Guide*.

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 3](#) 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 3 **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
Virtual Domains	100	500	750	750	750
Concurrent GUI Clients	5	10	25	50	50
Concurrent API (or northbound interface) Clients	2	2	5	5	5
Local Users	100	500	1000	500	1000
Location Groups	50	50	1000	500	1000

1. Compliance is supported on the Professional virtual appliance (OVA) and the Gen 2, UCS-based physical appliance only. It is not supported on: Express, Express Plus, or Standard OVAs; OVAs that have been resized to Professional; Gen 1 physical appliances. 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 3.0 Professional OVA or Gen2 UCS appliance, then use backup/restore to migrate data from your old server to the new server. See [Enabling Compliance Services](#) in the *Cisco Prime Infrastructure 3.0 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.

Scaling for Operations Center

When using Operations Center, we recommend you:

- Use the Standard OVA installation option.
- Ensure that your network is providing the following performance levels between Operations Center and its managed devices:
 - Bandwidth—250 Kbps
 - Latency—up to 5 ms. This is not a hard requirement, but Operations Center will only be as fast as its slowest managed instance. The higher the latency, the slower the overall performance. Use the Network Latency column on the Operations Center Manage & Monitor Servers page to spot managed instances that may be acting as bottlenecks.
- Ensure all instances managed by Operations Center are running Prime Infrastructure 3.0.

[Table 4](#) lists the Operations Center parameters.

Table 4 **Scaling Operations Center**

Operations Center Parameter	Maximum Supported
Number of managed instances	10
Number of managed virtual domains	100
Concurrent GUI clients	100

See [Table 2](#) for physical appliance options and [Table 3](#) for installation option scaling information. For more information, see [Setting Up Operations Center](#) in the *Cisco Prime Infrastructure 3.0 Administrator Guide*.

Scaling for Data Center

[Table 5](#) lists the Data Center parameters.

Table 5 **Scaling Data Center**

Parameter		Standard	Professional	Hardware Appliance (Gen 2)
Wireless networking	Wireless LAN Controller (WLC)	100	200	400
Data Center networking	Wired Devices (Cisco Catalyst 3000 Series devices, Cisco Nexus 5000 Series devices, Cisco Nexus 7000 Series devices, Cisco Integrated Services Routers (ISR), and Cisco ASR devices)	1000	1500	3000

Table 5 *Scaling Data Center (continued)*

Parameter		Standard	Professional	Hardware Appliance (Gen 2)
Virtual infrastructure	Cisco UCS B-Series devices, Cisco UCS C-Series devices	500	1000	2000
	VMware vCenters	5	10	14
	VMware Hosts	250	500	1200
	VMware Clusters	4	8	15
	Virtual machines	2500	6000	12,000
	Total	4395	9218	18,629

If You Are Upgrading From Previous Releases of Prime Infrastructure

You can upgrade the following Prime Infrastructure versions to Prime Infrastructure 3.0:

- Cisco Prime Infrastructure 2.2.3
- Cisco Prime Infrastructure 2.2.2
- Data Center Technology Package 1.0.0 for Cisco Prime Infrastructure 2.2.1
- Wireless Technology Package 1.0.0 for Cisco Prime Infrastructure 2.2.1
- Cisco Prime Infrastructure 2.2.1
- Cisco Prime Infrastructure 2.2

If your product/version is not in this list, to upgrade to 3.0, you must first upgrade to version 2.2.x at a minimum.

You cannot upgrade to Prime Infrastructure 3.0 if you installed version 2.2.x in FIPS mode.

Prime Infrastructure Installation and upgrade files downloaded from Cisco.com are all archive files. Please extract them before using them to install or upgrade.

If you are running multiple versions of Prime Infrastructure from which you want to migrate data, see [If You Are Running Multiple Prime Infrastructure Versions](#).

Remember that backups can only be restored to a new Prime Infrastructure server that is the same size or bigger than your previous server. See [Scaling Prime Infrastructure](#).

Before you upgrade from Prime Operations Center 2.2.x to 3.0, make sure you upgrade any Prime Infrastructure instances that are managed in Prime Operation Center from Prime Infrastructure 2.2.X to Prime Infrastructure 3.0.

To back up your data from a previous supported version of Prime Infrastructure, follow these steps:

-
- Step 1** If you have not already done so: Set up a remote backup repository for the Prime Infrastructure version you are currently running. For details, see [Using Remote Backup Repositories](#) in the [Cisco Prime Infrastructure 3.0 Administrator Guide](#).
- Step 2** Take an application backup of the Prime Infrastructure version you are currently running, and store the backup in the remote repository. For details, see [Taking Application Backups](#) in the [Cisco Prime Infrastructure 3.0 Administrator Guide](#).
- Step 3** Verify the integrity of the backup as explained in [Validating Your Backup](#).
-

If You Are Running Multiple Prime Infrastructure Versions

If you are running multiple previous releases of Prime Infrastructure (for example, you are running version 2.2 and 2.2.1 or 2.2.2), you must select *one* version from which to restore data. You cannot restore data from more than one Prime Infrastructure version. To combine data from multiple Prime Infrastructure versions:

1. Perform the restore operation for one Prime Infrastructure system running a previous Prime Infrastructure version. See [Migrating Data From Previous Releases of Prime Infrastructure](#).
2. Export your device inventory and maps from other Prime Infrastructure systems and import the information into the Prime Infrastructure 3.0 system.

Validating Your Backup

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 [Restoring From Application Backups](#) in the *Cisco Prime Infrastructure 3.0 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.

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.

3 Installing Cisco Prime Infrastructure

Follow the instructions in this section to install Prime Infrastructure.

- [Before You Begin Installation](#)
- [Performing an Inline Upgrade](#)
- [Deploying the OVA from the VMware vSphere Client](#)
- [Installing the Server](#)

Before You Begin Installation

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 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.
- If you download the OVA: Extract the PI-VA-3.0.0.0.78.ova file contained in the PI-VA-3.0.0.0.78.ova.zip archive file downloaded from Cisco.com. Then ensure that the extracted file matches the following checksums:
 - MD5 Checksum: eb20a7542d48d97740a4ad412c82f0cf
 - SHA512 Checksum:
54850a0a35009fad54b707624605cd3715ffe0ea66fc446db4053c399d563c4374fcf8a0122ff4d447e072f27764fc0523f6b140a995d33daacf706a9c3f2134



Note Prime Infrastructure 3.0 does not support FIPS mode installation. You cannot perform an inline upgrade or restore from a backup Prime Infrastructure 2.2.x in FIPS mode to Prime Infrastructure 3.0.

Performing an Inline Upgrade

Inline upgrade is simpler than system migration, and requires no new hardware. The following steps explain how to upgrade from Prime Infrastructure 2.2.x to Prime Infrastructure 3.0.



Note If you are upgrading from a Prime Infrastructure 2.2.x virtual machine, you should create a new virtual machine with the same deployment configuration option you used previously (for example, Express, Express-Plus, Standard, or Professional), back up your existing virtual machine, and then restore it on the new virtual machine. Perform an inline upgrade from Prime Infrastructure 2.2.x, then delete the old virtual machine after the upgraded virtual machine is fully operational.

- Step 1** If you have not already done so: Set up a remote backup repository for the Prime Infrastructure version you are currently running. For details, see [Using Remote Backup Repositories](#) in the *Cisco Prime Infrastructure 3.0 Administrator Guide*.
- Step 2** Take an application backup of the Prime Infrastructure version you are currently running, and store the backup in the remote repository. For details, see [Taking Application Backups](#) in the *Cisco Prime Infrastructure 3.0 Administrator Guide*.
- Step 3** Verify the integrity of the backup as explained in [Validating Your Backup](#).
- Step 4** Remove any existing High Availability configuration from your primary and secondary Prime Infrastructure servers. You can do this using either of the following options:
 - Launch Prime Infrastructure, choose **Administration > High Availability > HA Configuration**, and click **Remove**.
 - Go to admin console and run the **ncs ha remove** command.
- Step 5** Download the PI-Upgrade-3.0.0.0.78.tar.gz archive file from Cisco.com and verify the archive's integrity using the checksum listed for it on Cisco.com.
- Step 6** Extract the upgrade file, PI-Upgrade-3.0.0.0.78.tar.gz, from the downloaded ZIP archive and ensure the extracted file matches the following checksums:
 - MD5 Checksum: 03446c34f1a4ffd5d445c070ee17bfb9
 - SHA512 Checksum:
c366ba3f8740c4fabef1bcdde959710e04cf7b68fdafd44e8ebd085588e9527e1dac6f301125ad221f2ff94ec285d2da
b5985080a2eff71341d60e1fd096917c
- Step 7** Copy the extracted and verified upgrade file to the default repository:


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

Where:

 - *source* is the upgrade file's URL, path and filename (for example:
FTP://<YourFTPServer>/PI-Upgrade-3.0.0.0.78.tar.gz).
 - *disk* is the disk and path to the local defaultRepo.
- Step 8** Stop the Prime Infrastructure server by entering the command **ncs stop**.
- Step 9** Run the application upgrade:


```
admin# application upgrade PI-Upgrade-3.0.0.0.78.tar.gz defaultRepo
```

This step can take 40 minutes or more to complete, depending on the size of the application database.

Step 10 When the upgrade is complete:

- Verify that the application is running by entering the **ncs status** command in the admin console.
 - Instruct users to clear the browser cache on all client machines that accessed an older version of Prime Infrastructure before they try to connect to the upgraded Prime Infrastructure server.
 - If you were using external AAA (RADIUS or TACACS) before the upgrade, see [Renewing AAA Settings](#) in the *Cisco Prime Infrastructure 3.0 Administrator Guide*.
 - If you are using Prime Infrastructure to manage Cisco Wireless LAN Controllers, see [Resynchronizing WLC Configurations](#).
 - Synchronize your devices as explained in [Synchronizing Devices](#) in the *Cisco Prime Infrastructure 3.0 User Guide*.
-

Deploying the OVA from the VMware vSphere Client

Make sure that all of the system requirements are met before you deploy the OVA. Review the sections [Understanding System Requirements](#) and [Before You Begin Installation](#).

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.

Installing the Server

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

-
- Step 1** If the virtual machine 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 of 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 [System Timezones](#) in the *Cisco Prime Infrastructure 3.0 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 [Recovering Administrator Passwords on Virtual Appliances](#) in the *Cisco Prime Infrastructure 3.0 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 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 [Checking Prime Infrastructure Server Status](#) in the *Cisco Prime Infrastructure 3.0 Administrator Guide*) to verify that the processes have restarted. You should see the following process statuses:
- All Processes are up and running.
-

4 Post-Installation Tasks

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

- [Migrating Data From Previous Releases of Prime Infrastructure](#)
- [Logging in to the Prime Infrastructure User Interface](#)
- [Getting Started Using Prime Infrastructure](#)

Migrating Data From Previous Releases of Prime Infrastructure

To restore your data from Prime Infrastructure 2.2.x to your newly installed Prime Infrastructure 3.0 server, follow these steps:

-
- Step 1** Configure the new Prime Infrastructure host to use the same remote backup repository as the old host. For details, see [Using Remote Backup Repositories](#) in the *Cisco Prime Infrastructure 3.0 Administrator Guide*.
- Step 2** Restore the application backup on the remote repository to the new host, as explained in [Restoring From Application Backups](#) in the *Cisco Prime Infrastructure 3.0 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 Prime Infrastructure server.
 - If you are using Prime Infrastructure to manage Cisco Wireless LAN Controllers, see [Resynchronizing WLC Configurations](#).
 - Synchronize your devices as explained in [Synchronizing Devices](#) in the *Cisco Prime Infrastructure 3.0 User Guide*.
- Step 4** After the new Prime Infrastructure 3.0 server is operational, decommission your previous server.
-

Assurance Data after Migration

After restoring Prime Infrastructure 2.2.x on a new Prime Infrastructure 3.0 virtual machine or hardware appliance, your Assurance license is automatically applied to the new server.

When you move your data to Prime Infrastructure 3.0, 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

Aggregated data is migrated depending on from which version of Prime Infrastructure the data is backed up and then restored:

- From Prime Infrastructure 2.2.x to 3.0—5-minute, 1-hour, and 1-day aggregated data is migrated.
- From Prime Infrastructure 3.0 to 3.0—5-minute, 1-hour, and 1-day aggregated data is migrated.

Resynchronizing WLC Configurations

After you restore the backup of the previous version on the 2.2.x 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.
-

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 [Obtaining and Importing CA-Signed Certificates](#) in the *Cisco Prime Infrastructure 3.0 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** Enter the *root* administrator username and password, as specified when [Installing the Server](#).
 - Step 4** Click **Login** to log in to Prime Infrastructure. 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 5** 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 Administrator Setup Tasks in the *Cisco Prime Infrastructure 3.0 Administrator Guide*:

- [Configuring Data Sources for Prime Infrastructure with Assurance](#), including enabling NetFlow and Performance Agent.

- [Managing Disk Space Issues](#) on Prime Infrastructure servers.
- [Renewing AAA Settings](#).
- [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 “Getting Started” chapter of the [Cisco Prime Infrastructure 3.0 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.
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

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

Port	Protocol	Direction	Usage
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 ¹	UDP	Devices to server	NetFlow 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)
11011 ¹	TCP	Endpoints to server	Plain text dispatcher port for the Plug and Play Gateway
11012			SSL dispatcher port for the Plug and Play Gateway
11013			Plain text plug and play port
11014			SSL port for the Plug and Play Gateway
61617 ²	TCP	Server to endpoints	SSL port for Java Message Service connections

1. Used when the Plug and Play Gateway is integrated with the Prime Infrastructure server.

2. 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 [Removing Prime Infrastructure](#) in the *Cisco Prime Infrastructure 3.0 Administrator 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 3.0 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
Maintaining device configurations	Inventory > Device Management > Configuration Archive	Maintaining Device Configuration Inventory
Setting up access switches after they have been added to Prime Infrastructure	Configuration > Plug and Play > Initial Device Setup	Getting Help Setting Up and Configuring Devices
Preconfiguring devices that will be added to your network in the future	Configuration > Plug and Play Setup > Profiles	Getting Help Setting Up and Configuring Devices

Related Documentation

The *Cisco Prime Infrastructure 3.0 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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2012-2015 Cisco Systems, Inc. All rights reserved.