

Cisco Prime Infrastructure 3.9 Quick Start Guide

Overview

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

Related Topics

[About This Guide](#), on page 1

[Product Overview](#), on page 1

[About Cisco Prime Infrastructure Licensing](#), on page 1

About This Guide

This guide describes how to install Cisco Prime Infrastructure 3.9 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 latest [Cisco Prime Infrastructure 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 3.9.

For information about configuring and managing this product, see the [Cisco Prime Infrastructure Administrator Guide](#) and the [Cisco Prime Infrastructure 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 latest [Cisco Prime Infrastructure User Guide](#).
- Information about features intended for administrators, see the latest [Cisco Prime Infrastructure 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 Ordering and Licensing Guide](#).
- How to apply purchased licenses, see the [Cisco Prime Infrastructure Administrator Guide](#).

Before You Install

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

- [Understand System Requirements, on page 2](#)
- [How to Scale Prime Infrastructure, on page 6](#)



Note If your existing Prime Infrastructure is 3.7.x or 3.8.x, and your upgrade path contains 3.4.x or earlier versions, then you cannot in-line upgrade that server to Prime Infrastructure 3.9 due to security vulnerabilities in the underlying Red Hat 6 installation. You will need to take a backup of the Prime Infrastructure 3.7.x or 3.8.x server, deploy a fresh Prime Infrastructure 3.9 server, and restore that backup into the Prime Infrastructure 3.9 server.



Note Cisco ADE (Application Deployment Engine) OS Release 4.1 is supported till EOL of Prime Infrastructure.

Understand 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, on page 2](#).
- **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 latest [Cisco Prime Infrastructure Installation and Migration Guide for Microsoft Hyper-V Virtual Machine](#).
- **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, on page 3](#).

Virtual Appliance Options

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

Table 1: Prime Infrastructure Minimum Server Requirements

Requirement	Express	Express-Plus	Standard	Professional
VMware Version	ESXi 6.0, 6.5, 6.7, or 7.0	ESXi 6.0, 6.5, 6.7, or 7.0	ESXi 6.0, 6.5, 6.7, or 7.0	ESXi 6.0, 6.5, 6.7, or 7.0
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
Minimum CPU Speed	2.29 GHz	2.29 GHz	2.29 GHz	2.29 GHz

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 Prime Infrastructure Physical Appliance and Digital Network Architecture Center (DNAC) Appliance. Prime Infrastructure 3.9 not supported on the PRIME-NCS-APL-K9 (also known as “Gen 1”). Prime Infrastructure 3.9 is supported on PI-UCS-APL-K9 (also known as the Gen 2 appliance), PI-UCSM5-APL-K9 and PI-UCSM5-APL-U-K9 (also known as Gen 3 appliance) and DN1-HW-APL and DN2-HW-APL known as DNAC Appliance). You can upgrade a Prime Infrastructure Physical Appliance running Prime Infrastructure 3.7.x or 3.8.x to Prime Infrastructure 3.9. If the existing setup has 3.1.x, 3.2.x, 3.3.x, 3.4.x or 3.5.x versions, you must first upgrade it to 3.8.x version so as to upgrade to Prime Infrastructure 3.9 version. The physical appliance specifications are as follows:

Specification	Configuration	Gen-2 Appliance	Gen-3 Appliance	DNAC Appliance	DNAC Appliance (DN2-HW-APL)

Hardware Specifications	CPU (cores/threads)	10 C/20 T	20C/40T	44 C/88 T	44 C/88 T
	Memory	64 GB	64 GB	256 GB	256 GB
	Disk Capacity	4x900 GB	HDD - 4 x 1.2 TB SSD - 4 x 900 GB	4X 1.8 TB	6 X 1.9 TB
	RAID Level RAID	10	10	1, 1, 10 (446(bootable), 1787, 3574 in GB)	1, 1, 10 (446(bootable), 1787, 5361 in GB)
	Disk I/O Speed	320 MBps	320 MBps	320 MBps	320 MBps
System Users	Concurrent GUI clients	50	50	50	50
	Concurrent API clients	5	5	5	5



Note Prime Infrastructure uses the 10G port as eth0 for Cisco DNA Center Appliance. You must perform the following steps to use the 1G port.

1. Navigate to **Compute > BIOS**.
2. Select the **Configure BIOS** tab and then the **Advanced** tab.
3. Expand the **LOM and PCIe Slots configuration** link.
4. Select the **Disabled** option from **PCIe Slot:MLOM OptionROM** and **PCIe Slot:MLOM Link Speed** drop-down lists.
5. Perform reboot operation.
6. Install Prime Infrastructure.



Note Gen-3 Appliance is supported from Prime Infrastructure 3.4.1.

While installing Prime Infrastructure on physical appliances, make sure network management IP address should be configured to Gigabit Ethernet 0 interface for all network management traffic (eg. netconf, telemetry, snmp etc).

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

For maximum management capacities for each installation option, see [How to Scale Prime Infrastructure, on page 6](#)

How to Improve the Performance of Appliances

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

Procedure

-
- Step 1** Launch the CIMC web interface (see the section *How to Set Up the Appliance* in the latest [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 Back Good BBU
-

Web Client Requirements

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

- Hardware—A Mac or Windows 7 or Windows 10 laptop or desktop compatible with one of the following tested and supported browsers:
 - Firefox : Version 80.0.1 and above
 - Firefox ESR : 68.0esr and above
 - Google Chrome - Version 85.0.4183.83 (Official Build) (64-bit) and above
 - Internet Explorer - Version 11.1016.18362.0
- Display resolution—Prime Infrastructure supports 1366 x 768 or higher, but we recommend that you set the screen resolution to 1600 x 900.



Note Due to strict certificate check in Firefox browser, when you have two different Prime Infrastructure server with same hostname you will get the below error code:

- Failed : Error code: SEC_ERROR_REUSED_ISSUER_AND_SERIAL

To avoid this you can import CA Signed certificate in PI server through admin CLI. See *Import CA-Signed Host Certificates* from [Ciso Prime Infrastructure 3.8 Admin Guide](#) steps to generate CSR and import CA signed certificate.

How to Scale Prime Infrastructure

Prime Infrastructure comes with a variety of server installation options (see [Understand System Requirements, on page 2](#)). Ensure that you select an option appropriate for the size and complexity of your network.

The following table 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) ²	Hardware Appliance (Gen 3)	DNAC Appliance
Maximum number of devices (combination of wired and wireless devices)	500	3000	10,000	14,000	24,000	24,000	24,000
Unified APs	300	2500	5000	10,000	20,000	20,000	20,000
Autonomous APs	300	500	1500	2500	3,000	3,000	3,000
Wired Devices	300	1000	6000	10,000	13,000	13,000	13,000
NAMs	5	5	500	800	1000	1000	1000
Controlllers	5	25	500	800	1,000	1000	1000
Wired Clients	6000	50,000	50,000	50,000	50,000	50,000	50,000
Wireless Clients	4000	30,000	75,000	150,000	200,000	200,000	200,000
Cisco Mobility Services Engine (MSE)	1	1	6	10	12	12	12
Changing Clients (every 5 minutes) ³	1000	5000	25,000	30,000	40,000	40,000	40,000

Parameter (Maximums)	Express	Express-Plus	Standard	Professional	Hardware Appliance (Gen 2) ²	Hardware Appliance (Gen 3)	DNAC Appliance
Events Sustained Rate (events per second; includes syslogs, traps, and system events)	100	100	300	500	1000	1000	1000
Syslog Rate	70	70	210	350	600	600	600
Trap Rate	20	20	60	100	300	300	300
System Event Rate	10	10	30	50	100	100	100
NetFlow Rate (flows per second) ⁴	3000	3000	16,000	40,000	80,000	80,000	80,000
Supported Hourly Host Records	144,000	720,000	2,100,000	6,000,000	12,000,000	12,000,000	12,000,000
Interfaces	12,000	50,000	250,000	250,000	350,000	350,000	350,000
Compliance Violation Limit ⁵	—	—	20000	80000	80000	80000	80000
NAM Data Polling Enabled	5	5	20	30	40	40	40
Polling Interfaces (polling of trunk ports)	2400	8000	48,000	100,000	100,000	100,000	100,000
Number of Sites/Campus	200	500	2500	2500	2500	2500	2500
Groups: User-Defined + Out of the Box + Device Groups + Port Groups	50	100	150	150	150	150	150
Location Group	100	100	1000	1000	1000	1000	1000
Virtual Domains	100	500	750	750	750	750	750
Concurrent GUI Clients	5	10	25	50	50	50	50
Concurrent API (or northbound interface) Clients	2	2	5	5	5	5	5

² Compliance is supported on the Standard, Professional virtual appliance (OVA) and the Gen 2 appliance, Gen 3 appliance and DNAC 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 3.9

Standard or Professional OVA or Gen2 appliance or Gen 3 Appliance or DNAC 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 3.9 Administrator Guide](#).

- ³ Changing Clients are wireless users who are roaming across APs or disassociating and associating to APs.
- ⁴ 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.
- ⁵ If the Compliance violation for the Professional virtual appliance exceeds 80000, the compliance job will not show any data.



Note When there is a high inflow of data for hosts, it triggers hosts_lt and hosts_mt tables to exceed the default max record count and retention age. Prime Infrastructure performance might get affected, and the services might go down while creating the backup file because of disk space issues. To address this issue, you must reduce the maximum records and age of the retention by 65% of the actual default settings of highly utilized tables, maximum records, and age.



Note Please ensure to select the Unified APs/Wireless client range within the specified limits mentioned in the table. If the AP count/Client count exceeds the given limit, Prime Infrastructure will throw an error "PGA memory used by the instance exceeds PGA_AGGREGATE_LIMIT".



Note Supported Scale for PnP Provisioning:

- Maximum number of devices per profile: 100
- Maximum number of Simultaneous Deployments per APIC-EM limitation : 50 (Threads)



Important We recommend that you maintain an acceptable level of latency between your devices and the Cisco Prime Infrastructure server. A high latency might result in the server being unable to manage your devices, or the background tasks running slowly. A typical example of such a scenario is when you have thousands of APs and multiple Cisco Wireless Controllers managed by Prime Infrastructure across a WAN. In such a situation, we recommend that you install Prime Infrastructure in a local setup to ensure that the device response time is not impacted by queries from Prime Infrastructure.

How to Scale for Service Provider Wi-Fi

The following table lists the Service Provider Wi-Fi parameters.

Table 3: Scaling for Service Provider Wi-Fi

Parameter	Maximum Supported
Number of APs	20,000

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

How to Scale for Operations Center

When using Operations Center, we recommend that 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 3.9.

To help you roll out new versions of Prime Infrastructure at your own pace, Operations Center always supports management of instances of both the current and the very last version of Prime Infrastructure (also known as “N-1 management”). For example: If you upgrade your Operations Center management server to 3.9, you can use that server to continue managing Prime Infrastructure 3.8.x instances, as well as upgraded 3.9 Prime Infrastructure instances.



Note Make sure that you do the following when you are upgrading the Operation Center:

- Remove the managed instances before upgrading the Operation Center.
- Upgrade the Operation Center.
- Re-add the managed instances.

The following table lists the Operations Center scaling parameters.

Table 4: Scaling Operations Center

Operations Center Parameter	Maximum Supported
Number of managed instances	15
Concurrent GUI clients	100

See [Physical Appliance Options, on page 3](#) for physical appliance options and the table under the section [How to Scale Prime Infrastructure, on page 6](#) for installation option scaling information. For more information, see *Set Up Operations Center* in the latest [Cisco Prime Infrastructure Administrator Guide](#).

How to Scale for Data Center

The following table lists the Data Center parameters.

Table 5: Scaling Data Center

Parameter	Devices	Standard	Professional	Hardware Appliance (Gen 2)	Hardware Appliance (Gen 3)	DNAC Appliance
Data Center Switches	Cisco Nexus devices	2500	3000	3000	3000	3000
Virtual infrastructure	Cisco UCS B-Series devices, Cisco UCS C-Series devices	2000	2000	2000	2000	2000
	VMware vCenters	7	14	14	14	14
	VMware Hosts	472	1219	1219	1219	1219
	VMware Clusters	8	15	15	15	15
	Virtual machines	5500	12000	12,000	12,000	12,000
	Total		10587	18648	18,648	18,648

How to Scale for CDB

The following table lists the number of records with the approximate size on disks for CDB parameters.

Table 6: Supported Scale for CDB

CDB/ Install Type	Express	Express-Plus	Standard	Professional	Hardware Appliance (Gen 2)	Hardware Appliance (Gen 3)	DNAC Appliance
CoreConv	123120000 950 MB	123120000 950 MB	123120000 950 MB	123120000 950 MB	6156000000 45 GB	6156000000 45 GB	6156000000 45 GB
ARTClSvr	100440064 750 MB	100440064 750 MB	100440064 750 MB	100440064 750 MB	5022000000 40GB	5022000000 40GB	5022000000 40GB
Custom NetFlow (per CDB created by user)	100440064 500 MB * no. of custom cdb's created	100440064 500 MB * no. of custom cdb's created	100440064 500 MB * no. of custom cdb's created	100440064 500 MB * no. of custom cdb's created	5808098304 5 GB * no. of custom cdb's created	5808098304 5 GB * no. of custom cdb's created	5808098304 5 GB * no. of custom cdb's created
Disk Space used by Other CDBs	3 GB approximately	3 GB approximately	3 GB approximately	6 GB approximately	10GB approximately	10GB approximately	10GB approximately

Installation Options

Prime Infrastructure provides the following installation options:

- New installation on a virtual machine—See [Before You Begin Installation on a Virtual Machine](#), on page 11.
- New installation on a physical appliance. Prime Infrastructure comes preinstalled on physical appliances, or you can install an image on an existing appliance. See [Set Up Prime Infrastructure on a Virtual Machine or Physical Appliance](#), on page 12.
- Upgrade a previous version of Prime Infrastructure—See [How to Upgrade From Previous Releases of Prime Infrastructure](#), on page 14.

Before You Begin Installation on a Virtual Machine

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

- 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 PI-VA-3.9.0.0.219.ova from Cisco.com or use your Cisco-supplied installation media. Verify the integrity of the OVA file using its checksum listed on Cisco.com.

Install 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 [Understand System Requirements](#) and [Before You Begin Installation on a Virtual Machine](#), on page 11.



Note If you are using Esxi 6.5 or later, you can deploy latest ova using Web Client.

Procedure

-
- 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**.
- Note** We will reserve half of the CPU resources and memory based on your OVA selection.
- Note** Ensure the **Publisher** field shows Cisco Systems, Inc.
- 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, Express Plus, Standard, Professional, etc.) and view the resources required for the configuration you selected.
- Note** It is mandatory to 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 [Understand System Requirements, on page 2](#), then click **Next**.
- Step 12** In the Disk Format window, select **Thick Provisioning** 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.

Set 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.

Procedure

-
- 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.

Note If an IPv6 address is not manually configured on the interface, or discovered dynamically, the IPv6 address will be automatically configured.

- 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 the chapter *Time Zones Supported By Cisco Prime Infrastructure* in the [Cisco Prime Infrastructure 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 the section *How to Recover Administrator Passwords on Virtual Appliances* in the latest [Cisco Prime Infrastructure Administrator Guide](#).

Step 5 When you are done entering these values, you will be prompted for the following 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:
- **Advance Security option**— You will be prompted for accessing root shell. Enter **Yes** at the prompt to enable root shell access. Enter **No** to disable root shell access.
- **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 6 Select **Yes** to proceed with the installation, or select **No** to re-enter high availability options.

Step 7 When you are done entering these values, the installer application tests the network configuration parameters you have entered. If the tests are successful, it begins installing Prime Infrastructure.

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 the section *Check Prime Infrastructure Server Status* in the latest [Cisco Prime Infrastructure User Guide](#)) to verify that the processes have restarted. You should see the following process statuses:

- All Processes are up and running.

How to Upgrade From Previous Releases of Prime Infrastructure

You can upgrade the following versions of Prime Infrastructure to 3.9:

- Cisco Prime Infrastructure 3.8.1
- Cisco Prime Infrastructure 3.8 Update 02
- Cisco Prime Infrastructure 3.8
- Cisco Prime Infrastructure 3.7.1 Update 04
- Cisco Prime Infrastructure 3.7.1
- Cisco Prime Infrastructure 3.7 Update 03
- Cisco Prime Infrastructure 3.7

If your existing Prime Infrastructure is 3.7.x or 3.8.x, and your upgrade path contains 3.4.x or earlier versions, then you cannot in-line upgrade that server to Prime Infrastructure 3.9 due to security vulnerabilities in the underlying Red Hat 6 installation. You will need to take a backup of the Prime Infrastructure 3.7.x or 3.8.x server, deploy a fresh Prime Infrastructure 3.9 server, and restore that backup into the Prime Infrastructure 3.9 server.



Note While upgrading from PI 3.7.x or PI 3.8.x to PI 3.9, it is mandatory to install the PI 3.9 Mandatory Oracle Patch (PI_3_9_Oct_Oracle_patch-1.0.8.ubf) after Upgrade. This patch includes Oracle Oct 2020 patch and Catalyst 9800 16.12.x version support. This Patch is not required for Prime Infrastructure 3.9 fresh installation as ISO & OVA images already have this Oracle Patch.

But, If you need support for Catalyst 9800 16.12.x version, you will need to install this UBF irrespective of how you migrated to 3.9 (Fresh Install, B&R and Upgrade).

For instruction to install the Oracle Patch, see *Installing Cisco Prime Infrastructure System Patch 3.9* section in the latest [Prime Infrastructure Administrator Guide](#).



Note Setting the hostname using **hostnamectl** changes the uppercase letters to lowercase. Although Redhat 7 and CentOS 7 provide **hostnamectl** to set the hostname permanently, the real hostname will only be lowercase even if the users specify any uppercase letters.

If you are running multiple versions of Prime Infrastructure from which you want to migrate data, see [Migrate Data From Previous Releases of Prime Infrastructure, on page 17](#).

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 [How to Scale Prime Infrastructure, on page 6](#).

Before you upgrade from Operations Center 3.7.X or 3.8.x to 3.9, make sure you upgrade any Prime Infrastructure instances that are managed in Operations Center from Prime Infrastructure 3.7.X or 3.8.x to Prime Infrastructure 3.9.

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

Procedure

-
- 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 the section *Using Remote Backup Repositories* in the latest [Cisco Prime Infrastructure 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 the section *Perform an Immediate Application Backup Using the CLI* in the latest [Cisco Prime Infrastructure Administrator Guide](#).
- Step 3** Verify the integrity of the backup as explained in [.Before You Migrate Your Data, on page 17](#)
-

What to do next

You can upgrade Prime Infrastructure using either of the following methods:

- Perform an inline upgrade of existing 3.7.x and 3.8.x system—See [How to Perform an Inline Upgrade, on page 15](#).
- Restore data from backup on running system—See [Before You Migrate Your Data, on page 17](#).

How to Perform an Inline Upgrade

Inline upgrade is simpler than system migration, and requires no new hardware. Prime Infrastructure 3.9 supports inline upgrade from Prime Infrastructure 3.7.x, and 3.8.x.

Prime Infrastructure supports only the upgrading of secondary server from 3.7.x and 3.8.x to 3.9. To pair HA with primary server in Prime Infrastructure version 3.9, you must either install a new secondary server from the Prime Infrastructure 3.9 OVA image or upgrade from 3.7.x and 3.8.x to 3.9 using the upgrade bundle file and integrate it with the primary server for high availability. For details, [Install Prime Infrastructure on a Virtual Machine, on page 11](#).

The following steps explain how to upgrade from primary Prime Infrastructure 3.7.x, and 3.8.x to Prime Infrastructure 3.9.

Procedure

-
- Step 1** Set up a remote backup repository for the Prime Infrastructure version you are currently running. For details, see the section *Use a Remote Backup Repository* in the latest [Cisco Prime Infrastructure 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 the section *Perform an Immediate Application Backup Using the CLI* in the latest [Cisco Prime Infrastructure Administrator Guide](#).
- Step 3** Verify the integrity of the backup as explained in [Before You Migrate Your Data](#).

- Step 4** Remove any existing High Availability configuration from your primary Prime Infrastructure server. You can do this using either of the following options:
- Launch Prime Infrastructure, choose **Administration > Settings > High Availability > HA Configuration**, and click **Remove**. Ensure the configuration mode changes to “HA Not Configured.”
 - Ensure the primary server is the active Prime Infrastructure server, go to the admin console on the primary server and run the **ncs ha remove** command.

- Step 5** Move backup files (all files with the tar.gz extension) from the /localdisk directory to another server and ensure that /localdisk has 80% free space. For details, see the sections *copy and delete commands* and *show disks command* in the latest [Command Reference Guide for Cisco Prime Infrastructure](#).

Please ensure that /tmp folder has 80% free space for the upgrade to complete successfully.

- Step 6** Download the upgrade bundle PI-Upgrade-37x_38x_to_3.9.0.0.219.tar.gz from Cisco.com and verify the integrity using its checksum listed on Cisco.com.

- Step 7** Copy the verified upgrade file to the default repository:

Example:

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

Where:

- *source* is the upgrade file’s URL, path and filename (for example: FTP://<YourFTPServer>/PI-Upgrade-37x_38x_to_3.9.0.0.219.tar.gz)
- *disk* is the disk and path to the local defaultRepo.

- Step 8** Ensure the current version of Prime Infrastructure is 3.7.x, and 3.8.x.

- Step 9** Ensure the local repository (defaultRepo) contains no backup files.

- Step 10** Stop the Prime Infrastructure server by entering the command **ncs stop**

- Step 11** It is recommended to run the application upgrade from the console. For a virtual appliance, you can run the application upgrade from the VM console. For a physical appliance, you can run the application upgrade from the KVM, VGA, or serial console. (If you are using the serial console, make sure baud rate is configured to 9600)

Example:

```
admin# application upgrade PI-Upgrade-37x_38x_to_3.9.0.0.219.tar.gz defaultRepo
```

This step can take several hours to complete, depending on the size of the application database.

- Step 12** 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 the section *Renew AAA Settings After Installing a New Prime Infrastructure Version* in the latest [Cisco Prime Infrastructure Administrator Guide](#).

- If you are using Prime Infrastructure to manage Cisco Wireless LAN Controllers, see [Resynchronize WLC Configurations after Migration](#)
- Synchronize your devices as explained in the section *Synchronize Devices* in the latest [Cisco Prime Infrastructure User Guide](#).

Note When you upgrade from Prime Infrastructure version 3.7.x & 3.8.x to 3.9 that uses two NICs, network outage occurs post the upgrade. This can be avoided by performing the following steps:
You must not add 2 NICs before the first power up of deployment. Also, adding 2 NICs at the same time is not recommended.

- Login to VMware vSphere.
- Choose the Virtual Machine where the Dual NIC has to be configured.
- Power off the Virtual Machine.
- Choose edit settings and then add the second NIC.
- Turn on the Virtual Machine.

Note When customer runs Virtual Machine with two network interfaces, after installation of the patch/upgrade, the Prime instance will reboot automatically.
We recommend you to check the network whether the MAC address and network interface match with each other and manually change if there is a mismatch.

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 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.

Migrate Data From Previous Releases of Prime Infrastructure

You can migrate from the following 3.7.x, and 3.8.x Prime Infrastructure versions to Prime Infrastructure 3.9 :

- Cisco Prime Infrastructure 3.8.1
- Cisco Prime Infrastructure 3.8 Update 02
- Cisco Prime Infrastructure 3.8
- Cisco Prime Infrastructure 3.7.1 Update 04

- Cisco Prime Infrastructure 3.7.1
- Cisco Prime Infrastructure 3.7 Update 03
- Cisco Prime Infrastructure 3.7

If you are running multiple previous releases of Prime Infrastructure (for example, you are running version 3.7.x or 3.8.x), 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:

See [Before You Migrate Your Data](#) before you start the following steps to restore your data from Prime Infrastructure 3.7.x, and 3.8.x to your newly installed Prime Infrastructure 3.9 server:

Procedure

- 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 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 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 [Resynchronize WLC Configurations after Migration, on page 19](#).
 - Synchronize your devices as explained in *Synchronize Devices* in the [Cisco Prime Infrastructure User Guide](#).
- Step 4** After the new Prime Infrastructure 3.9 server is operational, decommission your previous server.
-

Assurance Data after Migration

After restoring Prime Infrastructure 3.7.x, and 3.8.x on a new Prime Infrastructure 3.9 virtual machine or hardware appliance, your Assurance license is automatically applied to the new server.

When you move your data to Prime Infrastructure 3.9, the following Assurance data will not get 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 3.7.x, and 3.8.x to 3.9.

Resynchronize WLC Configurations after Migration

After restoring Prime Infrastructure 3.7.x, and 3.8.x backup on a new Prime Infrastructure 3.9, 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.

Procedure

-
- 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.
-

Post-Installation Tasks

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

[Log in to the Prime Infrastructure User Interface, on page 19](#)

[Get Started Using Prime Infrastructure, on page 20](#)

Log 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 *Import CA-Signed Certificates* in the latest [Cisco Prime Infrastructure Administrator Guide](#).

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

Procedure

-
- Step 1** Launch one of the Supported Browsers (see [Understand System Requirements, on page 2](#)) 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 in [Set Up Prime Infrastructure on a Virtual Machine or Physical Appliance, on page 12](#)
 - 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.

Get 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 latest [Cisco Prime Infrastructure 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 chapter *Get Started with Prime Infrastructure chapter* in the latest [Cisco Prime Infrastructure User Guide](#). After you complete these tasks, you are ready to start monitoring and configuring your network.

Reference Information

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

- [Ports Used by Prime Infrastructure and Assurance, on page 20](#)
- [Remove the Prime Infrastructure Virtual Appliance, on page 23](#)
- [Navigation and Documentation Reference, on page 23](#)
- [Related Documentation, on page 24](#)
- [Obtaining Documentation and Submitting a Service Request, on page 24](#)

Ports Used by Prime Infrastructure and Assurance

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

Table 7: 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
80	HTTP	Server to devices	Provisioning of Nexus devices
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 using HTTPS (enabled by default).
443	TCP	Server to cisco.com	To check for software updates between the Prime Infrastructure server and cisco.com.
443	TCP	Prime Infrastructure to Cisco DNA Center server	Device, Groups, Maps, CMX migration to DNA Center.
514	UDP	Devices to server	Syslog server
830	TCP	Prime Infrastructure to Device	To open the NETCONF port for communication
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

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
8078	TCP	Client to Server	Browser access to Prime Infrastructure via HTTPS to the Cisco DNA Center Coexistence Tool
8080	TCP	Devices (Cisco Wireless Controllers version 8.6 or higher) to Server	SSL (HTTPS) port for receiving Wireless Client Health Metrics from WLC devices
8082	TCP	Client to server	Health Monitor web interface, Apache/Tomcat JSP engine
8085	TCP	Client to server	Used by the Health Monitor process to check network bandwidth speed between Primary and Secondary servers, when the user executes readiness test under High Availability
8087	TCP	Client to server	Secondary server software update page
9991	UDP	Devices to server	NetFlow data receiver
9992	TCP	Lync server to Prime Infrastructure server	Lync 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 ⁶	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
20830	TCP	Devices to Coral	Coral accepts TDL based telemetry including AP and client data from devices. (Specific to 17.12 Cisco Catalyst 9800 Wireless Controllers.)
61617 ⁷	TCP	Server to endpoints	SSL port for Java Message Service connections

- ⁶ Used when the Plug and Play Gateway is integrated with the Prime Infrastructure server.
⁷ Used by the Prime Infrastructure Plug And Play Gateway only.

Remove 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 the latest [Cisco Prime Infrastructure Admin Guide](#).

Procedure

-
- 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 chapters where the features are covered in the latest [Cisco Prime Infrastructure User Guide](#) and the [Cisco Prime Infrastructure Administrator Guide](#).

Table 8: Navigation and Documentation Reference

Task	Navigation in Cisco Prime Infrastructure	Chapter in Cisco Prime Infrastructure Guides
Adding licenses	Administration > Licenses and Software Updates > Licenses	Licenses and Software Updates in the Administrator Guide
Managing Users	Administration > Users > Users, Roles & AAA	User Permissions and Device Access in the Administrator Guide
Discovering your network	Inventory > Device Management > Discovery	Add and Organize Devices in the User Guide
Setting up virtual domains	Administration > Users > Virtual Domains	User Permissions and Device Access in the Administrator Guide
Using monitoring dashboards	Dashboard > Overview > General	Get Started With Cisco Prime Infrastructure in the User Guide
Using templates for configuring and monitoring	Configuration > Templates > Features & Technologies or Monitor > Monitoring Tools > Monitoring Policies	Create Templates to Automate Device Configuration Changes in the User Guide
Viewing alarms	Monitor > Monitoring Tools > Alarms and Events	Monitor Alarms and Events in the User Guide

Task	Navigation in Cisco Prime Infrastructure	Chapter in Cisco Prime Infrastructure Guides
Maintaining device configurations	Inventory > Device Management > Configuration Archive	Manage Device Configuration Files in the User Guide
Reconfiguring devices that will be added to your network in the future	Configuration > Plug and Play > Dashboard	Use Plug and Play to Deploy New Devices in the User Guide

Related Documentation

The [Cisco Prime Infrastructure 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 or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

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

