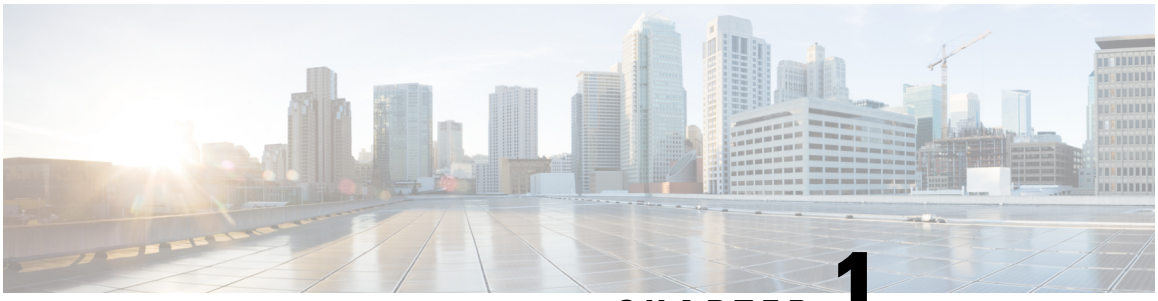
# Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide - 12.x

**First Published:** 2017-12-19

**Last Modified:** 2021-01-08

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS



CHAPTER 1

# Cisco Prime Collaboration Assurance and Analytics Overview

This section explains the following:



## About Cisco Prime Collaboration Assurance and Analytics

This document provides information on Cisco Prime Collaboration Assurance and Analytics 12.1 (includes Service Pack 1, Service Pack 2, and Service Pack 3 releases).

Cisco Prime Collaboration Assurance and Analytics provides real-time monitoring, proactive troubleshooting, and long term trending and analytics in one integrated product.

Cisco Prime Collaboration Assurance provides integrated service assurance management through a single, consolidated view of the Cisco voice, and video collaboration environment. It includes continuous, real-time monitoring and advanced troubleshooting tools for Cisco Unified Communications and Cisco TelePresence systems including the underlying transport infrastructures. It proactively notifies operators of issues and facilitates resolution through proactive fault detection and isolation using diagnostic tools. For video, the solution allows operators to view end-to-end session paths and identify jitter and packet loss, which impacts the session quality.

Cisco Prime Collaboration Assurance is available in Advanced mode.

**Cisco Prime Collaboration Assurance and Analytics Advanced**

Cisco Prime Collaboration Assurance and Analytics Advanced offers full-featured real-time monitoring and diagnostics system for voice, video, and Contact Center network assurance. The Analytics module provides historical reporting of key performance indicators (KPIs) and allows IT network managers to analyze trends for capacity planning, resource optimization, and quality of service.

In the Cisco Prime Collaboration Assurance - Advanced option, you can select either the Enterprise mode deployment or Managed Service Provider (MSP) deployment.

In the Enterprise mode, Cisco Prime Collaboration Assurance Advanced includes Cisco Prime Collaboration Analytics and Cisco Prime Collaboration Contact Center Assurance. If you have purchased the license for Cisco Prime Collaboration Analytics and Cisco Prime Collaboration Contact Center Assurance, you can access the Cisco Prime Collaboration Analytics and Cisco Prime Collaboration Contact Center Assurance dashboards. If you select to install in MSP mode, Cisco Prime Collaboration Analytics is available only in Cisco Prime Collaboration 11.5 and later versions.

For details on Advanced version of Cisco Prime Collaboration Assurance, see the Cisco Prime Collaboration-Standard and Advanced Offerings.

**Cisco Prime Collaboration Analytics**

Cisco Prime Collaboration Analytics helps you identify traffic trends, technology adoption trends, and over- and underutilized resources in your network. You can also track intermittent and recurring network issues and address service quality issues.

For more details on the features available in Cisco Prime Collaboration Analytics 12.x, see the "Prime Collaboration Analytics Dashboards and Reports" chapter in Cisco Prime Collaboration Analytics Guide.

**Cisco Prime Collaboration Contact Center Assurance**

Cisco Prime Collaboration Contact Center Assurance is a monitoring and diagnostics tool that helps you maximize the Cisco Unified Contact Center Enterprise uptime. For more details on the features available in Cisco Prime Collaboration Contact Center Assurance, see the "Overview of Cisco Prime Collaboration Contact Center Assurance" chapter in Cisco Prime Collaboration Contact Center Assurance Guide.

# Cisco Prime Collaboration Assurance and Analytics High Availability

Cisco Prime Collaboration Assurance and Analytics supports High Availability (HA) through the VMware vSphere HA feature. You do not need an extra Cisco Prime Collaboration Assurance and Analytics license to configure HA. For details on how to configure the virtualization layer HA for Cisco Prime Collaboration Assurance and Analytics, see the VMware vSphere HA for Cisco Prime Collaboration white paper.

# Cisco Prime Collaboration Assurance and Analytics Geo-Redundancy

Cisco Prime Collaboration Assurance and Analytics support Geo-Redundancy through the VMware vSphere replication. You do not need an extra Cisco Prime Collaboration Assurance and Analytics license to configure Geo-Redundancy. For more information on Geo-Redundancy, see Geo Redundancy for Cisco Prime Collaboration Assurance and Analytics.

# Change History

The following table describes the information that has been added or changed in the Cisco Prime Collaboration Assurance 12.x (includes FCS/SP1/SP2/SP3).

*Table 1: Change History*

| Release Date | First Customer Shipment (FCS)/Service Pack(s) (SP) |
|---|---|
| 08-JAN-2021 | SP4 -Republished<br>Added the note Adobe Flash Player is not applicable for SP4. |
| 08-DEC-2020 | SP4 |
| 15-APR-2019 | SP3 |
| 23-OCT-2018 | SP2 - Republished<br>Modified the values in the column "Minimum vCPU Reservation" in the table "Virtual Machine Requirements for Cisco Prime Collaboration Assurance" along with the Note. |
| 16-OCT-2018 | SP2 |
| 12-SEP-2018 | SP1 - Republished |
| 08-AUG-2018 | SP1 |
| 19-DEC-2017 | FCS |

# What's New in Cisco Prime Collaboration Assurance

## Cisco Prime Collaboration Assurance and Analytics 12.1 Service Pack4

**Note** You can install Cisco Prime Collaboration Assurance 12.1 Service Pack 4 using OVA files for fresh installation. Any new user, who purchases Cisco Prime Collaboration Assurance, must install Cisco Prime Collaboration Assurance 12.1 Service Pack 4 directly.

The following are the new changes introduced in the Cisco Prime Collaboration Assurance and Analytics 12.1 Service Pack 4.

*Table 2: What's New in Cisco Prime Collaboration Assurance 12.1 Service Pack 4 Features*

| Name | Description | Where Documented |
|---|---|---|
| Cisco Prime Collaboration Assurance 12.1 Service Pack 4 new endpoint support. | New endpoint support | Supported Devices for Cisco Prime Collaboration Assurance Service Pack 4 |
| Changes to the UCM SIP Trunk and Endpoint Diagnostics screen | Two new buttons "Stop/Resume" Monitoring are introduced. | Cisco Prime Collaboration Assurance - Advanced and Analytics Guide, 12.1 Service Pack 4 |

| Name | Description | Where Documented |
|---|---|---|
| New correlation alarms | Two new correlation alarms "AnalogEndPointLostContact" and "OtherEndPointLostContact" in “Correlation” User Interface page. | Cisco Prime Collaboration Assurance - Advanced and Analytics Guide, 12.1 Service Pack 4 |
| Flash player migration | Flash Player dependency is removed from various UI pages of Cisco Prime Collaboration Assurance as part of Flash migration feature. | Cisco Prime Collaboration Assurance - Advances and Analytics Guide, 12.1 Service Pack 4 |

**Note** We recommend that you use Microsoft Edge over IE to view all graphs.

## Cisco Prime Collaboration Assurance and Analytics 12.1 Service Pack 3

**Note** You can install Cisco Prime Collaboration Assurance 12.1 Service Pack 3 using OVA files for fresh installation. Any new user, who purchases Cisco Prime Collaboration Assurance, must install Cisco Prime Collaboration Assurance 12.1 Service Pack 3 directly.

The following are a few changes introduced in the Cisco Prime Collaboration Assurance and Analytics 12.1 Service Pack 3.

*Table 3: What's New in Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Features*

| Name | Description | Where Documented |
|---|---|---|
| Cisco Prime Collaboration Assurance support for Collaboration System Release (CSR) 12.5 Compatibility | Update CSR 12.5 related information in compatibility matrix<br>New endpoint support | Supported Devices for Cisco Prime Collaboration Assurance |

| Name | Description | Where Documented |
|---|---|---|
| Platform Changes | Cisco Prime Collaboration Assurance 12.1 Service Pack 3 has been enhanced to use CentOS **7.5**.<br><br>In addition to the existing features (as mentioned in the table on "What's New in Cisco Prime Collaboration Assurance 12.1 Features", following are the changes introduced in Cisco Prime Collaboration Assurance 12.1 Service Pack 3:<br><br>**1.** **Note on CPU reservation changes** in the section on System Requirements - Server and Client Machine Requirements<br><br>**2.** Cisco Prime Collaboration Assurance can also be deployed on **vCenter Application 6.7 or ESXi Server 6.7** (Small, Medium, Large, and VeryLarge, and VeryLarge-db OVA) | |
| Upgrade to Cisco Prime Collaboration Assurance 12.1 Service Pack 3 | Change in the section on 'Upgrade Sequence'. | Readme for Cisco Prime Collaboration Assurance and Analytics 12.1 Service Pack 3. |

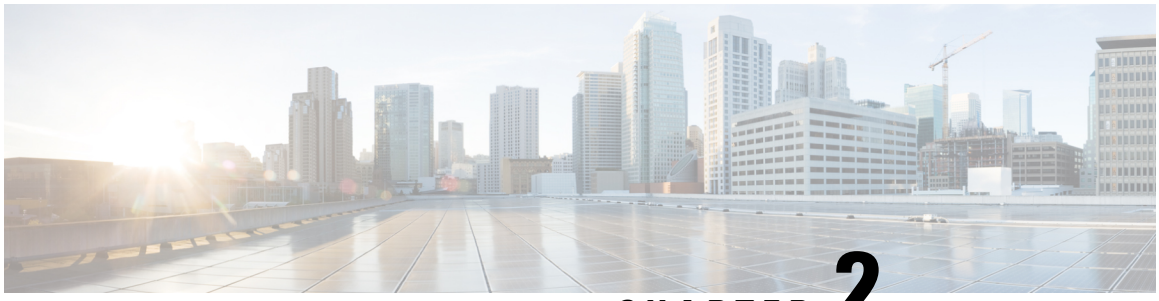
**Cisco Prime Collaboration Assurance and Analytics 12.1 (includes Service Pack 1 and Service Pack 2)**

The following are a few new deployment methods introduced in the Cisco Prime Collaboration Assurance and Analytics 12.1 (includes Service Pack 1 and Service Pack 2).

*Table 4: What's New in Cisco Prime Collaboration Assurance 12.1 Features*

| Name | Description | Where Documented |
|---|---|---|
| General | Features and Enhancements | What's New in Cisco Prime Collaboration Assurance |

| Name | Description | Where Documented |
|---|---|---|
| New Installation | Cisco Prime Collaboration Assurance 12.1 has been enhanced to use the latest Open Source platform like CentOS 7.3 and OpenJDK-7. Following are the new features introduced in Cisco Prime Collaboration Assurance 12.1:<br>**1.** Installation Requirements - last row on User Accounts and Installation Prompts<br>**2.** System Requirements - Server and Client Machine Requirements<br>**3.** User Accounts<br>**4.** Installation Prompts<br>**5.** Deploy Cisco Prime Collaboration Assurance Using vCenter or ESXi (Small, Medium, Large, and VeryLarge, and VeryLarge-db OVA)<br>**a.** Configure the Database Server<br>**b.** Configure the Application Server<br>**6.** OVF Tool<br>**a.** Setting Up the OVF Tool<br>**b.** How to Create a Configuration File<br>**c.** Adding Files from an OVF Package | New Installation |
| Migrate Cisco Prime Collaboration Assurance | Migration to latest open source platform such as CentOS 7.3. The sections updated include:<br>**1.** Overview of Data Migration Assistant<br>**2.** Preinstallation Guidelines<br>**3.** Pre-requisites for Backup and Restore<br>**4.** Preparation for Data Migration Assistant<br>**5.** Perform Data Migration Assistant Backup<br>**6.** Perform Data Migration Assistant Restore<br>**7.** Validate Data Migration Assistant | Migrate Cisco Prime Collaboration Assurance |



CHAPTER 2

# Cisco Prime Collaboration Assurance and Analytics Licensing

Cisco Prime Collaboration Assurance and Analytics is a licensed software product that is secured to the MAC of the virtual machine. The Cisco Prime Collaboration Assurance and Analytics license enables the features and endpoint quantities for the Cisco Prime Collaboration Assurance and Analytics application that you choose to install. You can order license based on the collaboration management options required, and the quantity of the endpoints.

This section explains the following:



## Access to the Software Image, PAK, and License File

The product numbers ordered for Cisco Prime Collaboration are: R-xxx and L-xxx. When you order the product numbers for Cisco Prime Collaboration, an email is sent to your ship-to email address. This email contains the instructions on how you can access the Cisco eDelivery site so that you can download the software images and license Product Authorization Keys (PAKs). The software image is downloaded and installed on the virtual machine. The license PAK ID from the ESD site allows you to access the Cisco Licensing Site to associate the virtual machine MAC address to a license key or keys that are then installed on the virtual machine(s). These license keys activate the Cisco Prime Collaboration software to be used in a production environment. These license keys together also convert a trial installation into a production environment. Only (1) R-xxx type license is required for each Cisco Prime Collaboration installation.

**Note** The PAK is used to log in to the Cisco software site and has a virtual machine MAC address associated to it. The PAK is emailed to you, and a license file is created for you to download. Cisco Prime Collaboration Assurance requires individual license files. After you download the license files, register them with the Cisco Prime Collaboration Assurance servers.

# Cisco Prime Collaboration Assurance Advanced Licensing

Cisco Prime Collaboration Assurance - Advanced licensing is based on the endpoint quantity. The number of endpoints determines the number of licenses that you need to purchase to manage your network. Along with the total number of endpoints, you must also consider the system capacity parameters, such as the number of each supported endpoint types, and CDR limits, to choose the most suitable virtual machine resources for your deployment.

With Assurance Advanced option, you can manage Cisco voice and video Collaboration Systems through a single, consolidated view. It includes continuous, real-time monitoring and advanced troubleshooting tools for Cisco Collaboration applications and endpoints, such as Cisco Unified Communications Manager, Cisco TelePresence Video Communication Server (Cisco VCS), Cisco TelePresence, and so on.

The mode of installation is Evaluation or Advanced. To learn more about Advanced install mode, see Deployment Model - Assurance.

The quantity of the endpoints determines the number of licenses that you need to purchase to manage your network.

Along with the total number of endpoints, you must also consider the system capacity parameters, such as the number of each supported endpoint types, and CDR limits, to choose the most suitable OVA for your deployment.

For more information on system capacity parameters for Cisco Prime Collaboration Assurance Advanced 12.x, see the System Capacity for Cisco Prime Collaboration Assurance.

The Cisco Prime Collaboration Assurance Image (R-PC-xxxx) license is required to activate Cisco Prime Collaboration Assurance in a production network. You must order one license for each server. A new license is required for each major upgrade and is included in the upgrade parts and the Product Upgrade Tool entitlements. For more information on the Product Upgrade Tool, see Version Upgrade Guide.

You can purchase scale licenses based on the endpoints that you want to manage. For more information on the scale licenses and part numbers in Cisco Prime Collaboration Assurance and Analytics 12.x, see Cisco Prime Collaboration Ordering Guide. You must have Cisco partner privilege to access the Ordering Guide.

**Note** All Unified CM registered endpoints in a specific cluster must be managed in Cisco Prime Collaboration Assurance to provide the statistics data to support all monitoring, testing, and reporting features in Cisco Prime Collaboration Assurance and Analytics; for example, statistics from the Unified CM Publisher CDR are required to compute route group utilization, Severely Conceal Seconds Ratio (SCSR)(%), and call failure measurements. When the Unified CM publisher is discovered, all endpoints (including phones) registered with it are discovered.

To add Cisco Prime Collaboration Assurance license file, go to **System Administration** > **License Management**. For more information in Cisco Prime Collaboration 12.x, see the *Add and Delete a License File* section of “Manage Licenses” chapter in the Cisco Prime Collaboration Assurance User Guide - Advanced.

# Cisco Prime Collaboration Contact Center Assurance Licensing

Cisco Prime Collaboration Contact Center Assurance requires the Cisco Prime Collaboration Assurance Advanced license. The Cisco Prime Collaboration Contact Center Assurance licensing is based on the number

of concurrent Unified Contact Center Enterprise (Unified CCE) agents logged in. Apply the Cisco Prime Collaboration Contact Center Assurance license only after adding the Cisco Prime Collaboration Assurance Advanced license.

Cisco Prime Collaboration Contact Center Assurance polls the number of agents logged in to the Unified CCE every 30 minutes. If the number of agents logged in exceeds the permitted number mentioned in the license file, the system displays a popup window with a warning message.

Cisco Prime Collaboration Contact Center Assurance raises one violation per day irrespective of the number of warning popup windows displayed. If there are 10 such violations within the 30-day period, then your license expires within the next 30 days of receiving the tenth violation.

If you add the license file for Cisco Prime Collaboration Assurance Advanced but not for Cisco Prime Collaboration Contact Center Assurance, you can access the features for Cisco Prime Collaboration Contact Center Assurance only until the evaluation expiry or purchase of license.

Upon license expiry, the Unified CCE infrastructure devices are not displayed in the UC Performance dashboard, **Threshold Rules**, and **Correlation Rules** windows. You cannot view the Contact Center Topology page. To continue using these features, purchase the required number of Cisco Prime Collaboration Contact Center concurrent agent licenses. You can view the license details for Cisco Prime Collaboration Contact Center Assurance by navigating to the **System Administration** > **License Management** page.

For details on the features that are enhanced after you add the Cisco Prime Collaboration Contact Center Assurance license 12.x, see the "Overview of Cisco Prime Collaboration Contact Center Assurance" chapter in Cisco Prime Collaboration Contact Center Assurance Guide.

The number of agents that you can manage after you purchase a license remains the same as the Evaluation mode. For more information, see Endpoints and Contact Center Agents Count section.

# Cisco Prime Collaboration Analytics Licensing

Cisco Prime Collaboration Analytics is supported only in the Cisco Prime Collaboration Assurance Advanced deployment. Apply the Cisco Prime Collaboration Analytics license after adding the Cisco Prime Collaboration Assurance Advanced license.

The total number of Cisco Prime Collaboration Analytics scale licenses obtained must be greater than or equal to the total number of scale licenses you have for Cisco Prime Collaboration Assurance Advanced. For example, if you are managing 1000 endpoints in Cisco Prime Collaboration Assurance Advanced, you must have Cisco Prime Collaboration Analytics license for 1000 or more endpoints.

# Endpoints and Contact Center Agents Count

The number of endpoints and agents that are supported in Cisco Prime Collaboration Assurance - Advanced (including Cisco Prime Collaboration Analytics and Contact Center Assurance) depends on the OVA size. The Cisco Prime Collaboration Analytics endpoints count must be greater than or equal to the total number of endpoints you have in Cisco Prime Collaboration Assurance - Advanced.

You can manage the following endpoint and agent quantities in the Cisco Prime Collaboration Assurance - Advanced and Cisco Prime Collaboration Contact Center Assurance. These numbers are applicable for Evaluation and Licensed modes.

| OVA Deployment Model | Total Number of Endpoints | IP Phones/Software Clients/DX Series[1] | Collaboration Room Endpoints/EX Series | Immersive TelePresence | Concurrent Contact Center Agent |
|---|---|---|---|---|---|
| Small (Enterprise and MSP) | Up to 3000 | Up to 3000 | Up to 250 | Up to 50 | Up to 450 |
| Medium (Enterprise and MSP) | Up to 20,000 | Up to 20,000 | Up to 2500 | Up to 500 | Up to 4000 |
| Large (Enterprise and MSP) | Up to 80,000 | Up to 80,000 | Up to 3000 | Up to 500 | Up to 12000 |
| Enterprise Very Large | Up to 150,000 | Up to 150,000 | Up to 5000 | Up to 1000 | Up to 12000 |
| MSP Very Large | Up to 150,000 | Up to 150,000 | Up to 5000 | Up to 1000 | Up to 12000 |

[1] Cisco Prime Collaboration Assurance can only be deployed with Cisco endpoints – combination of soft endpoints and hard endpoints.

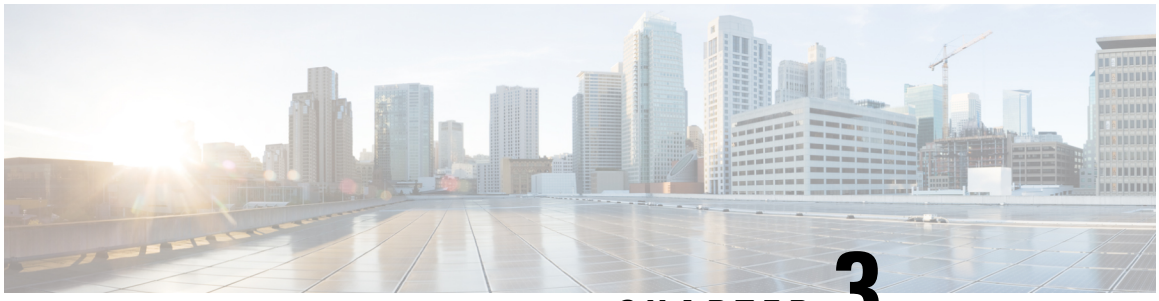
For more information, see the following documents

- System Capacity for Cisco Prime Collaboration
- Endpoint types Collaboration Endpoints.

.

PART I

# New Installation



CHAPTER 3

# Installation Requirements

This section explains the following:



# Installation Requirements

***Table 5: Installation Requirements***

| Requirements | Description |
|---|---|
| Number of Servers | Cisco Prime Collaboration Assurance application must be installed on virtual machines. To learn about the installation modes and the required number of servers, see Number of Servers. |
| Virtualization Requirements | The Cisco Prime Collaboration Assurance images are in the OVA file format. To learn more about the VMware environment required, see VMware Requirements. |
| System Requirements | System requirements vary based on the number of endpoints that you want to manage. See System Requirements - Server and Client Machine Requirements, on page 15.<br><br>For details on the maximum system capacity, such as, number of access ports, number of device pools, number of voice interfaces in Cisco Prime Collaboration Assurance Guide, see System Capacity for Cisco Prime Collaboration Assurance. |

| Requirements | Description |
|---|---|
| Ports Requirements | Cisco Prime Collaboration uses several protocols to communicate with other processes and devices.<br>Ensure that the required ports are available for Cisco Prime Collaboration to communicate. For more details, see Required Ports for Cisco Prime Collaboration Assurance . |
| Device configurations<br>( CiscoTelePresence Management Suite (TMS), Cisco Unified Communications Manager (CUCM), Cisco TelePresence Video Communication Server(VCS), Video endpoints, Multipoint Control Unit (MCU), and so on) | The voice and video endpoints and infrastructure devices require certain configurations for the Cisco Prime Collaboration server to communicate. For more details, see Setting up Devices for Cisco Prime Collaboration Assurance. |
| Download Images | Cisco Prime Collaboration images are provided on the eDelivery site and on the Cisco.com support software download site. You must have an order for an eDelivery or SWSS contract. |
| User Accounts and Installation Prompts | During installation, you must perform the following:<br>• Specify various passwords at different instances for Cisco Prime Collaboration Assurance. See User Accounts.<br>• Specify the Virtual machine details. See Installation Prompts. |

# Number of Servers

To install Cisco Prime Collaboration Assurance - Advanced (without Cisco Prime Collaboration Analytics), you need only one virtual machine. If you want to enable Cisco Prime Collaboration Analytics during the Cisco Prime Collaboration Assurance Advanced installation, the number of virtual machines that are required to install Cisco Prime Collaboration Assurance depends on the number of endpoints that you want to manage in Cisco Prime Collaboration Analytics:

- If you have fewer than or equal to 80,000 endpoints (small, medium, and large deployment models), you need one virtual machine where you can install both the database and application. To learn about configuring Cisco Prime Collaboration Assurance for small, medium, and large deployment models, see Deploy Small, Medium, and Large Cisco Prime Collaboration Assurance OVA Using vCenter.
- If you have more than 80,000 endpoints (very large deployment model), you need two virtual machines to install the database and application separately on each machine. To learn about configuring Cisco Prime Collaboration Assurance for very large deployment model, see Deploy Very Large Cisco Prime Collaboration Assurance OVA Using vCenter.

  Before installing the Cisco Prime Collaboration Assurance, ensure that you know the IP addresses for each of the virtual machines.

# VMware Requirements

Ensure that your VMware environment meets the following requirements:

- OVA is downloaded and saved to the same machine on which the vSphere Client is installed.
- VMware ESXi is installed and configured on the ESXi host. For more information on setting up and configuring your host machine, see the VMware documentation.

  The VMware vSphere Client is Windows-based. Therefore, download and install the client from a Windows system.

  Once you install the vSphere Client, you can run it and log in to the virtual host, using the hostname or IP address of the virtual host, the root log in ID, and the password that you configured. You can add the host to a vCenter if you want to manage it through vCenter. For more information, see the VMware documentation.
- VMware ESXi server hostname is configured in the DNS server.
- VMware ESXi server is synchronized with the NTP server.

**Note** Make sure you have admin privileges to configure vCenter, UCS, and ESXi in Cisco Prime Collaboration Assurance.

# System Requirements - Server and Client Machine Requirements

Cisco Prime Collaboration Assurance 12.x runs on any VMware-certified hardware.

**For Cisco Prime Collaboration Release 12.1 SP3 and later**

Cisco Prime Collaboration Assurance runs on any VMware-certified hardware with ESXi Server and vCenter Application versions 6.0, 6.5, 6.7, or 7.0 is installed. Small, Medium, Large and Very Large deployment models require ESXi Server and vCenter Application versions 6.0, 6.5, 6.7, or 7.0.

**For Cisco Prime Collaboration Release 12.1 SP2 and earlier**

Cisco Prime Collaboration Assurance runs on any VMware-certified hardware with ESXi Server and vCenter Application versions 5.5, 6.0, or 6.5 is installed. Small, Medium, Large and Very Large deployment models require ESXi Server and vCenter Application versions 5.0, 6.0, or 6.5.

**Note**

- We recommend that you install and run Cisco Prime Collaboration Assurance on Cisco Unified Computing System (UCS), which is VMware-certified.
- Cisco Prime Collaboration Assurance 12.x runs on CentOS. This operating system is included with the Cisco Prime Collaboration Assurance application and is installed when the Cisco Prime Collaboration Assurance OVA is deployed.

# Virtual Machine Requirements for Cisco Prime Collaboration Assurance

The table lists the virtual machine requirements for the Cisco Prime Collaboration Assurance application, based on the number of endpoints that are managed in Cisco Prime Collaboration Assurance. The virtual machine requirements mentioned in this table are also applicable for Cisco Prime Collaboration Analytics and Cisco Prime Collaboration Contact Center Assurance. For details on the endpoint quantities supported in each OVA deployment model, see Endpoints and Contact Center Agents Count section.

| Managed Endpoints | Number of exclusive vCPUs | Minimum vCPU Reservation | RAM | Memory Reservation | NIC | IOPS | Disk Space |
|---|---|---|---|---|---|---|---|
| **Enterprise: Small and Medium** | | | | | | | |
| Up to 3000 endpoints (Small-Assurance only) | 4 | 10 GHz | 14 GB | 14 GB | 1 GB | 100 | 250 GB |
| Up to 3000 endpoints (Small-Assurance & Analytics) | 4 | 10 GHz | 14 GB | 14 GB | 1 GB | 200 | 250 GB |
| Up to 20,000 endpoints (Medium-Assurance only) | 6 | 15 GHz | 22 GB | 22 GB | 1 GB | 200 | 300 GB |
| Up to 20,000 endpoints (Medium-Assurance & Analytics) | 6 | 15 GHz | 22 GB | 22 GB | 1 GB | 400 | 300 GB |
| **Enterprise and MSP**<br>*Large* - Up to 80,000 endpoints | | | | | | | |
| Up to 80,000 endpoints (Large-Assurance only) | 14 | 35 GHz | 34 GB | 34 GB | 1 GB | 800 | 500 GB |
| Up to 80,000 endpoints (Large-Assurance & Analytics) | 14 | 35 GHz | 34 GB | 34 GB | 1 GB | 1300 | 500 GB |
| **Enterprise and MSP**<br>*Very Large* - Up to 150,000 endpoints | | | | | | | |

| Managed Endpoints | Number of exclusive vCPUs | Minimum vCPU Reservation | RAM | Memory Reservation | NIC | IOPS | Disk Space |
|---|---|---|---|---|---|---|---|
| Cisco Prime Collaboration Assurance only | 22 | 55 GHz | 40 GB | 40 GB | 1 GB | 1000 | 750 GB |
| Cisco Prime Collaboration Assurance and Cisco Prime Collaboration Analytics (Application Server) | 22 | 55 GHz | 40 GB | 40 GB | 1 GB | 1000 | 750 GB |
| Cisco Prime Collaboration Assurance and Cisco Prime Collaboration Analytics (Database Server) | 8 | 20 GHz | 16 GB | 16 GB | 1 GB | 1000 | 750 GB |

**Note**

- The Input/Output Operations/Sec (IOPS) measurements were taken using **VMware IO Analyzer** tool, available at: I/O Analyzer .
- The Input/Output Operations/Sec (IOPS) is tested when the services are running.
- vCPU speed depends on the Cisco UCS server or the virtualized hardware.
- We do not support oversubscribing server parameters (not using a 1:1 ratio of physical to virtual resources), such as, vCPU and memory. Cisco Prime Collaboration Assurance needs exclusive use of these resources.
- For CPU, any model with physical core speed 2.5 GHz or higher (normal not Turbo) is required. If the requirement is not met after installation, a warning banner is displayed at the top of the user interface until the resource requirement is met.
- For possible, processor recommendations, visit Virtualization for Cisco Prime Collaboration Assurance (PCA) and refer to appropriate UCS Tested Reference Configurations or UCS or 3rd-party Specs-based on Intel Xeon choices.

**Recommendations to Improve IOPS:**

- RAID Configuration: RAID 10 provides better write performance and provides redundancy.
- Data store configuration: Dedicated data store for all OVA types.
- Use SSDs or 15K RPM SAS disks for 80K and 150K deployments.
- Use Fibre Channel-SAN storage with dedicated LUN with IOPS mentioned in the preceding table.

# Client Machine Requirements for Cisco Prime Collaboration Assurance

This table lists the client machine requirements for Cisco Prime Collaboration Assurance application.

| Attributes | Values |
|---|---|
| Display resolution | 1440 x 900 |
| Supported Browser | **For Cisco Prime Collaboration Release 12.1 SP3 and later**<br>The following browsers are supported:<br>• Windows Internet Explorer 10 and 11<br>• Google Chrome 73 or later<br>• Mozilla Firefox - upto 52 ESR<br>**For Cisco Prime Collaboration Release 12.1, 12.1 Service Pack 1, and 12.1 Service Pack 2**<br>The following browsers are supported:<br>• Mozilla Firefox 38 ESR and 45 ESR<br>• Windows Internet Explorer 10 and 11<br>• Google Chrome 53 or later<br>Cisco Prime Collaboration Assurance provides a self-signed certificate (HTTPS). To allow access to the Cisco Prime Collaboration Assurance client, ensure that security is set to either medium or low in the browsers and do the following:<br>• Ensure that you enable cookies in the browser.<br>• Ensure that you install the operating system and the browser in English version, and set locale as English (United States) [en-US] for Cisco Prime Collaboration Assurance.<br>**Note** Ensure that you select only English (United States) [en-US] under Languages and remove the other locale options from the browsers settings.<br>• Ensure that you disable the popup blocker if you have installed it as Cisco Prime Collaboration Assurance uses popup dialog boxes at several instances. |

| Attributes | Values |
|---|---|
| Adobe Flash Player | Install Adobe Flash Player on the client machine for Cisco Prime Collaboration Assurance features to work properly. We recommend that you download and install Adobe Flash Player version 13.x or later from the Adobe website.<br>**Note** For Cisco Prime Collaboration Assurance 12.1 Service Pack 4 and later, Adobe Flash Player is not required. |
| Environment | Clients must be able to access Cisco Prime Collaboration Assurance:<br>• Across a firewall - for information on how to configure client access, see Firewall documentation.<br>• Across a VPN - the VPN tunnel must connect the client and a VPN router or similar device. For more information on required ports, see Required Ports for Cisco Prime Collaboration Assurance . |
| Network Connectivity | If you have deployed Cisco Prime Collaboration Assurance in a large or very large deployment, we recommend that you have a minimum of 30-Mbps network connectivity. The network connectivity is with reference to the speed of the internet connection. |

# Mandatory Service Pack(s) or Engineering Special(s)

The following table lists the various upgrade path(s) that are mandatory for Cisco Prime Collaboration Assurance 12.1 Service Pack(s) or Engineering Special(s).

***Table 6: Mandatory Upgrade Path(s)***

| Service Pack(s) / Engineering Special(s) | Original Release Date | Comments / Mandatory Service Pack(s) or Engineering Special(s) and their Status |
|---|---|---|
| SP4 | 08-DEC-2020 | Cisco Prime Collaboration Assurance 12.1 Service Pack 4 must be installed on Cisco Prime Collaboration Assurance 12.1 Service Pack 3 (with or without Engineering Specials).<br>For more information, see the chapter on 'Introduction' in Readme for Cisco Prime Collaboration Assurance and Analytics 12.1 Service Pack 4.<br>**Status**: Mandatory |

| Service Pack(s) / Engineering Special(s) | Original Release Date | Comments / Mandatory Service Pack(s) or Engineering Special(s) and their Status |
|---|---|---|
| ES4 | 17-FEB-2020 | Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Engineering Special 4 is a cumulative of Cisco Prime Collaboration Assurance Service Pack 3 along with Engineering Special 1, Engineering Special 2, Engineering Special 3, and Engineering Special 4. Install either Cisco Prime Collaboration Assurance 12.1 Service Pack 3 or Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Engineering Special 3 or Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Engineering Special 2 or Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Engineering Special 1 before applying the Cisco Prime Collaboration Assurance Service Pack 3 Engineering Special 4.<br><br>**Status**: Current |
| ES3 | 27-NOV-2019 | Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Engineering Special 3 is a cumulative of Cisco Prime Collaboration Assurance Service Pack 3 along with Engineering Special 1, Engineering Special 2, and Engineering Special 3. Install either Cisco Prime Collaboration Assurance 12.1 Service Pack 3 or Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Engineering Special 2 or Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Engineering Special 1 before applying the Cisco Prime Collaboration Assurance Service Pack 3 Engineering Special 3.<br><br>**Status**: Current |
| ES2 | 21-AUG-2019 | Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Engineering Special 2 is a cumulative of Cisco Prime Collaboration Assurance Service Pack 3 along with Engineering Special 1 and Engineering Special 2. Install either Cisco Prime Collaboration Assurance 12.1 Service Pack 3 or Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Engineering Special 1 must be installed before applying the Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Engineering Special 2.<br><br>**Status**: Obsolete |
| ES1 | 29-MAY-2019 | Cisco Prime Collaboration Assurance 12.1 Service Pack 3 must be installed before applying the Cisco Prime Collaboration Assurance 12.1 Service Pack 3 Engineering Special 1.<br><br>**Status**: Obsolete |

| Service Pack(s) / Engineering Special(s) | Original Release Date | Comments / Mandatory Service Pack(s) or Engineering Special(s) and their Status |
|---|---|---|
| SP3 | 15-APR-2019 | Cisco Prime Collaboration Assurance 12.1 Service Pack 3 must be installed on Cisco Prime Collaboration Assurance 12.1 Service Pack 2.<br>For more information, see the chapter on 'Introduction' in Readme for Cisco Prime Collaboration Assurance and Analytics 12.1 Service Pack 3.<br>**Status**: Mandatory |
| ES2 | 08-MAR-2019 | Cisco Prime Collaboration Assurance 12.1 Service Pack 2 Engineering Special 2 is a cumulative of Cisco Prime Collaboration Assurance Service Pack 2 along with Engineering Special 1 and Engineering Special 2. Install either Cisco Prime Collaboration Assurance 12.1 Service Pack 2 or Cisco Prime Collaboration Assurance 12.1 Service Pack 2 Engineering Special 1 before applying the Cisco Prime Collaboration Assurance Service Pack 2 Engineering Special 2.<br>**Status**: Obsolete |
| ES1 | 22-NOV-2018 | Cisco Prime Collaboration Assurance 12.1 Service Pack 2 must be installed before applying the Cisco Prime Collaboration Assurance 12.1 Service Pack 2 Engineering Special 1.<br>**Status**: Obsolete |
| SP2 | 15-OCT-2018 | Cisco Prime Collaboration Assurance 12.1 Service Pack 2 must be installed on Cisco Prime Collaboration Assurance 12.1 Service Pack 1.<br>**Status**: Mandatory |
| SP1 | 09-AUG-2018 | **Path(s):**<br>**1.** 12.1 → SP1 (Fresh Installation)<br>Apply Cisco Prime Collaboration Assurance 12.1 SP1 directly on a freshly installed server.<br>Or<br>12.1 with ES (ES1/ES2/ES3/ES4) upgrade to SP1.<br>**2.** **Migration**: 11.6 → Install 12.1→ Apply 12.1 SP1 → Perform DMA<br>SP1 includes all the defect fixes from ES1 to ES4.<br>**Status**: Mandatory |
| ES4 | 16-JUL-2018 | **Status**: Obsolete |

| Service Pack(s) / Engineering Special(s) | Original Release Date | Comments / Mandatory Service Pack(s) or Engineering Special(s) and their Status |
|---|---|---|
| ES3 | 28-MAY-2018 | **Status**: Obsolete |
| ES2 | 28-MAY-2018 | **Status**: Obsolete |
| ES1 | 08-FEB-2018 | **Status**: Obsolete |
| 12.1 | 19-DEC-2017 | New Features and Enhancements:<br>For more information, see Cisco Prime Collaboration Assurance - Advanced and Analytics End-User Guide or Online Help for 12.1 on Cisco.com.<br>**Status**: Mandatory |

# Deployment Model - Assurance

You can install Cisco Prime Collaboration Assurance in Advanced mode. .

You can download the Cisco Prime Collaboration Assurance OVA deployment file based on the VM resources required to handle the number of endpoints that you want to manage. For more information on the different types of OVA deployment models and the endpoint quantities supported in each deployment model, see Endpoints and Contact Center Agents Count.

### Cisco Prime Collaboration Assurance and Analytics - Advanced

Cisco Prime Collaboration Assurance Advanced provides all the features that enable integrated assurance management of applications and the underlying transport infrastructure. The Advanced mode of Cisco Prime Collaboration supports multiple clusters.

For more details on features available in Advanced mode 12.x, see the *Cisco Prime Collaboration Advanced Features* section of “Overview of Cisco Prime Collaboration Assurance” chapter in Cisco Prime Collaboration Assurance Guide - Advanced.

If you choose to install Cisco Prime Collaboration Assurance in the Advanced mode, you can select either:

- Enterprise mode deployment - Cisco Prime Collaboration Assurance Advanced OVA includes both Cisco Prime Collaboration Analytics and Cisco Prime Collaboration Contact Center Assurance. Each feature is licensed separately.
- Managed Service Provider (MSP) deployment - Cisco Prime Collaboration Assurance Advanced includes only Cisco Prime Collaboration Contact Center Assurance.

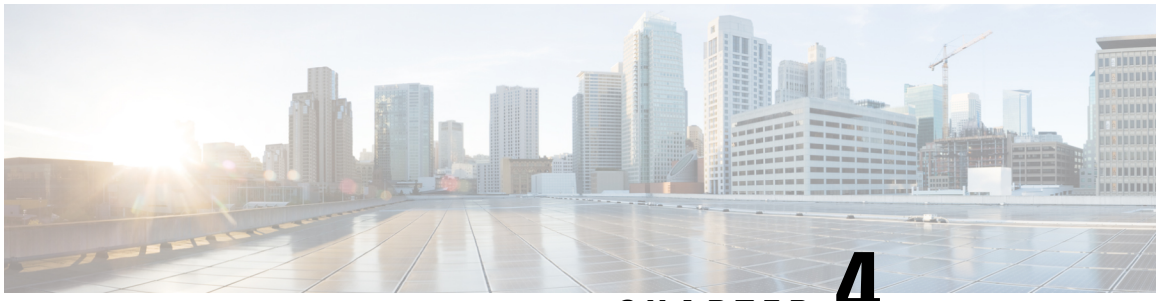
  In Cisco Prime Collaboration Assurance and Analytics 11.1 and earlier versions, Analytics is disabled for MSP - multi-customer enabled installations. Analytics support for MSP installations is being planned for a future release.

There are no separate Cisco Prime Collaboration Assurance - Advanced OVAs for Enterprise and MSP deployments for Small, Medium, and Large deployment models. However, for Very large deployment model, there are separate OVAs for Enterprise and MSP. By default, the Cisco Prime Collaboration Analytics and Cisco Prime Collaboration Contact Center Assurance are installed as part of the Cisco Prime Collaboration

Assurance - Advanced Enterprise installation. For more details, see the System Requirements - Server and Client Machine Requirements.

The MSP mode or Enterprise mode deployment selection is available only when you choose to install Cisco Prime Collaboration Assurance in the Advanced mode.

**Note** In Cisco Prime Collaboration Assurance and Analytics 11.1 and earlier versions, in the MSP mode deployment, Cisco Prime Collaboration Analytics is not installed as part of Cisco Prime Collaboration Assurance Advanced.



CHAPTER 4

# Install Cisco Prime Collaboration Assurance

This section explains the following:



# Download Cisco Prime Collaboration Assurance

Cisco Prime Collaboration Assurance images are provided on the eDelivery site when the product is purchased, and on the Cisco.com support software download site for patches and service packs. For those with a service subscription, such as Cisco Unified Communications Software Subscription (UCSS)/ Cisco Prime Product Assured Software Subscription (PASS) that are recently replaced by Cisco Software Support Service (SWSS), download your major upgrades from the Product Upgrade Tool (PUT). For more information on Product Upgrade Tool, see Version Upgrade Guide.

**Important** Download the OVA file on a machine where the vSphere Client is installed. To ensure that the downloaded OVA file is not corrupt, verify if the Message Digest 5 (MD5) checksum of the OVA file matches with the value in the download site. To view the MD5 checksum of the OVA file available in Cisco.com support software download site, hover your mouse pointer on the filename.

To install only Cisco Prime Collaboration Assurance, download the Cisco Prime Collaboration Assurance OVA file based on the number of endpoints that you want to manage.

You can configure the Cisco Prime Collaboration Assurance and Analytics application for the following types of deployment models:

- Cisco Prime Collaboration Assurance and Analytics OVA for a small deployment - For up to 3000 endpoints (which can include up to 100 Cisco TelePresence systems only).
- Cisco Prime Collaboration Assurance and Analytics OVA for a medium deployment - For up to 20,000 endpoints (which can include up to 1,000 Cisco TelePresence systems only).
- Cisco Prime Collaboration Assurance and Analytics OVA for a large deployment - For up to 80,000 endpoints (which can include up to 6,000 Cisco TelePresence systems only).

- Cisco Prime Collaboration Assurance and Analytics OVA for a MSP very large deployment - For up to 150,000 endpoints (which can include up to 6,000 Cisco TelePresence systems only).
- Cisco Prime Collaboration Assurance and Analytics OVA for an Enterprise very large deployment - For up to 150,000 endpoints (which can include up to 6,000 Cisco TelePresence systems only).

You must have a valid Cisco.com user account to download the files.

# User Accounts

For Cisco Prime Collaboration Assurance, specify various passwords at different instances.

- globaladmin - Superuser who can access the Cisco Prime Collaboration Assurance User Interface.
- globaladmin password - Password that you enter when you configure your virtual appliance for a standalone application, see Deploy Cisco Prime Collaboration Assurance Using vCenter or ESXi. You are also required to specify this password when you log in to the User Interface, see the **Password Rules for globaladmin/root** section. After installing Cisco Prime Collaboration Assurance for the first time, it prompts you to reset the password (change the default password).

### Password Rules for the globaladmin/root

Follow these guidelines when you are making up passwords for a globaladmin/root:

- Must contain at least one lowercase letter, uppercase letter, number, and special character (exclamation(!), at(@), hash(#), dollar($), asterisk(*), comma(,), period(.))
- Cannot repeat a character in the password more than three times.
- Cannot contain non-ASCII characters such as minus(-), percent(%), plus(+), ampersand(&), or a space.
- Cannot be Cisco or ocsic or any variant by changing the capitalization of letters, or by substituting 1, exclamation(!), Or pipe(|) for i, zero(0) for o, dollar($) for s.
- Cannot be the same as the username, or the username reversed.
- **For Cisco Prime Collaboration Release 12.1 SP2 and earlier**

  Must be between 8 and 80 characters.

  **For Cisco Prime Collaboration Release 12.1 SP3**

  Must be between 8 and 127 characters (user configurable).
- **For Cisco Prime Collaboration Release 12.1 SP4 and later**
  - Minimum length of password is 4 characters.
  - Maximum length of password is 127 characters.
- Cannot end with colon(:), asterisk(*), comma(,), semicolon(;), equal(=), or hash(#).

# Installation Prompts

We recommend that you know the values for the following parameters before configuring the virtual appliance:

| Field | Description |
|---|---|
| Server Hostname | Specify hostname for Cisco Prime Collaboration Assurance. Can contain hyphen(-) and Alphanumeric characters. Special characters are not allowed. This field is mandatory. |
| Network IP Address | Specify IP Address for this Virtual Machine. This field is mandatory. |
| IP Default Netmask | Specify the Default IP Netmask for this Virtual Machine. This field is mandatory. |
| IP Default Gateway | Specify the Default IP Gateway for this Virtual Machine. This field is mandatory. |
| **Note** 1. This is applicable for the following fields in vCenter 6: IP Address, IP Default Netmask, and IP Default Gateway.<br>**Issue**: By default, IP qualifiers has 4 octets. Due to the limitation in VMware, at times, only 3 octets are visible.<br>**Solution**: Press **Tab** after entering the third octet to enter the value for the fourth octet. The entered value for the fourth octet will not be visible. To view the complete field, press **Next**. The **Deployment Settings** window appears from where you can preview the entered values.<br>2. This is applicable for all the fields in vCenter 6.5.<br>**Issue**: Unable to proceed with the installation if the default values are removed.<br>**Solution**: Retain the default values (which are populated as part of the deployment) of all the fields. You can modify the values but do not remove the default values. | |
| Default DNS Domain | Specify the Default DNS Domain for this Virtual Machine. This field is mandatory. |
| Primary NameServer | You can specify up to 2 NameServers (Comma separated), Secondary NameServer (Optional). |
| NTP Servers | You can specify up to 3 NTP Servers (Comma separated), Secondary/Tertiary NTP Servers (Optional). |
| System Timezone | The configured time zone is UTC by default.<br>**Note** Ensure to add the Timezone details accurately as mentioned in the Supported Time zones for Cisco Prime Collaboration list. Inaccuracy will impact the installation process causing inconsistency and might not bring up Cisco Prime Collaboration Serviceability/Cisco Prime Collaboration Assurance User Interface after installation. |

| Field | Description |
|---|---|
| IPv6 configuration | You can configure IPv6 through Cisco Prime Collaboration Assurance Serviceability User Interface. For more information, see Cisco Prime Collaboration Assurance Serviceability User Guide. |
| Application Mode | You have an option to select any one of the following:<br>ENT - 0; MSP - 1 |
| Remote IP | Specify remote server IP in 2VM VeryLarge Setup. |
| UCOD Mode | You have an option to select any one of the following:<br>No Installation - 0; Master - 1; Responder - 2; Both (Master and Responder) - 3 |
| Enable Analytics | This property is applicable during VeryLarge setup. You have an option to select any one of the following:<br>Enable - 1; Disable - 0 |

# Deploy Cisco Prime Collaboration Assurance Using vCenter or ESXi

**Prerequisites**

Ensure that the requirements listed in System Requirements - Server and Client Machine Requirements have been met.

If you choose to enable Cisco Prime Collaboration Analytics in very large OVA deployment of Cisco Prime Collaboration Assurance, you require two virtual machines - database and application. Reserve two IP addresses in advance for the database and application server, since the IP address of application server is required while installing database server and database server IP address is required while installing the application server.

You must install database server before installing application server.

**Note**

1. OVA's are different for Deploy Cisco Prime Collaboration Assurance Using vCenter and Deploy and Configure Cisco Prime Collaboration Assurance Through ESXi Using Floppy Image.
2. We recommend not to start or stop services in the Cisco Prime Collaboration Analytics database server during the deployment.
3. This is applicable for both vCenter and ESXi. During cloning (the original Cisco Prime Collaboration Assurance Virtual Machine (VM) from one host to another host), customization of parameters (includes network parameters, Time Zone, Primary Name Servers and so on) are not supported in Cisco Prime Collaboration Assurance but can be modified from Cisco Prime Collaboration Assurance Serviceability. For more information, see the chapter on “System Parameters” in “Cisco Prime Collaboration Assurance Serviceability User Guide” on Cisco.com.
4. When you are deploying a Very Large server, first deploy DB VM and then deploy Main VM.

You can deploy Cisco Prime Collaboration Assurance in any one of the following methods:

- Deploy Cisco Prime Collaboration Assurance Using vCenter
- Deploy and Configure Cisco Prime Collaboration Assurance Through ESXi Using Floppy Image
- OVF Tool

# Deploy Cisco Prime Collaboration Assurance Using vCenter

You can choose any of the following OVA's for deploying in vCenter:

1. small.ova
2. medium.ova
3. large.ova
4. verylarge.ova
5. verylarge-db.ova

Based on the OVA that you have downloaded, you can deploy Cisco Prime Collaboration Assurance as follows:

- Deploy Small, Medium, and Large Cisco Prime Collaboration Assurance OVA Using vCenter
- Deploy Very Large Cisco Prime Collaboration Assurance OVA Using vCenter

## Deploy Small, Medium, and Large Cisco Prime Collaboration Assurance OVA Using vCenter

**Step 1** Launch VMware vSphere Client or through VMware vSphere Web Client. For more information, see the **VMware vSphere 5.1 Documentation Center**.

**Step 2** Download the Cisco Prime Collaboration Assurance application bundle from Cisco.com and save to a location.

**Step 3** Choose **File** > **Deploy OVF Template**.

**Step 4** Click **Browse** and navigate to the location where you saved the Cisco Prime Collaboration Assurance respective OVA file. Click **Next**.

**Step 5** In the **OVF Template Details** window, verify the details about the OVA file, including the product name, version, and size, and then click **Next**.

**Step 6** Click **Accept** to accept the end-user license agreement. Click **Next**.

**Step 7** In the **Name** window, specify a name for the template that you are deploying. The name must be unique within the inventory folder and can contain up to 80 characters. In the **Inventory Location** window, select the inventory location where you want to deploy the OVA, and click **Next**.

**Step 8** In the **Disk Format** window, select **Thick provisioned format** to store on the virtual disks, and then click **Next**.

In case of multiple networks during Cisco Prime Collaboration Assurance OVA deployment, ensure that the virtual machine network you select belongs to Cisco Prime Collaboration Assurance and is reachable.

**Step 9** In the **Interview Wizard**, enter the required parameters in the respective fields. For detailed information, see the section on Installation Prompts.

**Note** The configured time zone is UTC by default. For a list of supported time zones, see Supported Time zones for Cisco Prime Collaboration.

**Step 10** In the **Application Properties** section, under **Application Mode**, you can select either the **Enterprise mode** or **Managed Service Provider (MSP)** mode of deployment.

**a.** Enter **0** to deploy Cisco Prime Collaboration Assurance in the Enterprise mode.

**b.** Enter **1** to deploy Cisco Prime Collaboration Assurance in the MSP mode.

**Note** Unified Communications Operations Dashboard is not supported in MSP mode.

**Step 11** Verify the options in the **Ready to Complete** window, and then click **Finish** to start the deployment.

**Note** Check the progress bar in the **Deploying Virtual Appliance** window to monitor the task status.

**Step 12** Click **Close**.

The virtual appliance that you deployed appears in the left pane of the vSphere Client, under the host

For more information on Cisco Prime Collaboration 12.x, see the chapter on "Overview of Cisco Prime Collaboration Assurance" in Cisco Prime Collaboration Assurance Guide - Advanced.

**Step 13** Power ON the Virtual Machine to start the Cisco Prime Collaboration Assurance installation process. Open VMConsole of the deployed Virtual Machine to monitor the sequence of installation steps to determine whether it is success or failure. The installation takes a maximum of 30 minutes to complete.

**Note**

- If installation is successful, Root Access and VMConsole Access is disabled by default.
- If installation fails, system will be in the monitoring state for an hour after which Root Access and VMConsole Access will be enabled.

  **Enabling Root Access and VMConsole Access**: Root Access and VMConsole Access is automatically enabled when the Cisco Prime Collaboration Assurance detects configuration errors. Access is enabled to rectify any configuration errors that has caused the installation to fail.

  **Disabling Root Access and VMConsole Access**: Root Access and VMConsole Access is again disabled whenever all the Cisco Prime Collaboration Assurance processes come up successfully or when reboot is issued for the next time.

## Deploy Very Large Cisco Prime Collaboration Assurance OVA Using vCenter

**Step 1** Launch VMware vSphere Client or through VMware vSphere Web Client. For more information, see the steps on Install the vSphere Web Client.

**Step 2** Download the Cisco Prime Collaboration Assurance application bundle from Cisco.com and save to a location.

**Step 3** Choose **File** > **Deploy OVF Template**.

**Step 4** Click **Browse** and navigate to the location where you saved the Cisco Prime Collaboration Assurance OVA file. Click **Next**.

**Step 5** In the **OVF Template Details** window, verify the details about the OVA file, including the product name, version, and size, and then click **Next**.

**Step 6** Click **Accept** to accept the end-user license agreement. Click **Next**.

**Step 7** In the **Name** window, specify a name for the template that you are deploying. The name must be unique within the inventory folder and can contain up to 80 characters. In the **Inventory Location** window, select the inventory location where you want to deploy the OVA, and then click **Next**.

**Step 8** If you choose to enable Cisco Prime Collaboration Analytics in very large OVA deployment of Cisco Prime Collaboration Assurance, you require two virtual machines - database and application. Reserve two IP address in advance for database and application server, since IP address of application server is required while installing database server and database server IP address is required while installing application server.

**Note** The sequence in which the deployment takes place is that the Database Server should be started with all services and then Application Server should be installed.

#### What to do next

For information on the methods to configure the database server and application server, see the steps on "Configure the Database Server" and "Configure the Application Server".

## Configure the Database Server

#### Before you begin

Ensure to deploy DB.OVA to configure the database server.

**Step 1** In the **Host / Cluster** window, select the **Host** or **Cluster** on which you want to run the deployed template, and then click **Next**.

**Step 2** In the **Storage** window, select a destination for the virtual machine files, and then click **Next**.

**Step 3** In the **Disk Format** window, select the **Thick Provision Lazy Zeroed** format to store on the virtual disks, and then click **Next**.

In case of multiple networks during Cisco Prime Collaboration Assurance OVA deployment, ensure that the virtual machine network you select belongs to Cisco Prime Collaboration Assurance and is reachable.

**Step 4** In the **Interview Wizard**, enter the required parameters in the respective fields. For detailed information, see the section on Installation Prompts.

**Step 5** Verify the options in the **Ready to Complete** window, and then click **Finish** to start the deployment.

**Note** Check the progress bar in the **Deploying Virtual Appliance** window to monitor the task status.

**Step 6** Click **Close**. The virtual appliance that you deployed appears in the left pane of the vSphere Client, under the host.

**Step 7** Power ON the Virtual Machine to start the Cisco Prime Collaboration Assurance installation process. Open VMConsole of the deployed Virtual Machine to monitor the sequence of installation steps to determine whether it is success or failure. The installation takes a maximum of 30 minutes to complete.

**Note**

- If installation is successful, Root Access and VMConsole Access is disabled by default.
- If installation fails, system will be in the monitoring state for an hour after which Root Access and VMConsole Access will be enabled.

  **Enabling Root Access and VMConsole Access**: Root Access and VMConsole Access is automatically enabled when the Cisco Prime Collaboration Assurance detects configuration errors. Access is enabled to rectify any configuration errors that has caused the installation to fail.

  **Disabling Root Access and VMConsole Access**: Root Access and VMConsole Access is again disabled whenever all the Cisco Prime Collaboration Assurance processes come up successfully or when reboot is issued for the next time.

### What to do next

For information on the method to configure the application server, see the steps on "Configure the Application Server".

## Configure the Application Server

**Step 1** In the **Disk Format** window, select the **Thick Provision Lazy Zeroed** format to store on the virtual disks, and then click **Next**.

In case of multiple networks during Cisco Prime Collaboration Assurance OVA deployment, ensure that the virtual machine network you select belongs to Cisco Prime Collaboration Assurance and is reachable.

**Step 2** On the **Network Mapping** page, select a network and then click **Next**.

**Step 3** In the **Interview Wizard**, enter the required parameters in the respective fields. For detailed information, see the section on Installation Prompts.

**Note** The configured time zone is UTC by default. For a list of supported time zones, see Supported Time zones for Cisco Prime Collaboration.

**Step 4** If you have selected the **Advanced Prime Collaboration Assurance Evaluation** option, you can select either the **Enterprise mode** or **Managed Service Provider (MSP)** mode of deployment.

**a.** Enter **`0`** to deploy Cisco Prime Collaboration Assurance in the Enterprise mode.

**b.** Enter **`1`** to deploy Cisco Prime Collaboration Assurance in the MSP mode.

**Note** Unified Communications Operations Dashboard is not supported in MSP mode.

**Step 5** Verify the options in the **Ready to Complete** window, and then click **Finish** to start the deployment.

**Note** Check the progress bar in the **Deploying Virtual Appliance** window to monitor the task status.

**Step 6** Click **Close**. The virtual appliance that you deployed appears in the left pane of the vSphere Client under the host.

**Step 7** Power ON the Virtual Machine to start the Cisco Prime Collaboration Assurance installation process. Open VMConsole of the deployed Virtual Machine to monitor the sequence of installation steps to determine whether it is success or failure. The installation takes a maximum of 30 minutes to complete.

**Note**

- If installation is successful, Root Access and VMConsole Access is disabled by default.
- If installation fails, system will be in the monitoring state for an hour after which Root Access and VMConsole Access will be enabled.

  **Enabling Root Access and VMConsole Access**: Root Access and VMConsole Access is automatically enabled when the Cisco Prime Collaboration Assurance detects configuration errors. Access is enabled to rectify any configuration errors that has caused the installation to fail.

  **Disabling Root Access and VMConsole Access**: Root Access and VMConsole Access is again disabled whenever all the Cisco Prime Collaboration Assurance processes come up successfully or when reboot is issued for the next time.

### What to do next

After successful deployment, login to Cisco Prime Collaboration Assurance 12.x. For information, see the section on Log in to Cisco Prime Collaboration Assurance.

# Deploy and Configure Cisco Prime Collaboration Assurance Through ESXi Using Floppy Image

You can choose any of the following OVA's for deploying in HypervisorAgnostic (ESXi) using floppy image:

1. small-hva.ova
2. medium-hva.ova
3. large-hva.ova
4. verylarge-hva.ova
5. verylarge-db-hva.ova

## Preparation of the PCAAnswer Template File

PCAAnswer file is an XML-based file that is responsible for hosting a deployed server. It contains Property Keys and Value pairs where all the Network and Application related values are specified in order to commission the server.

Enter the required parameter values in the respective fields in PCAAnswer.xml template file. For detailed information, refer to the Table on “Property Key and Values for Small-hva, Medium-hva, Large-hva, VeryLarge-hva, and VeryLarge-db-hvavOVA(s)” in the section Create a Floppy Image and the section on Installation Prompts.

**Note**

- You must manually enter the values for each of the keys (based on the profile chosen) in the PCAAnswer.xml template file which is available in the Software Download site.

  **Path**: Downloads Home / Cloud and Systems Management / Collaboration and Unified Communications Management / Prime Collaboration / Prime Collaboration Assurance 12.1 / Prime Collaboration Software Images- 12.1

- Follow Step 1 through Step 7 to create, mount, and unmount a new floppy image.
- The configured time zone is UTC by default. For a list of supported time zones, see Supported Time zones for Cisco Prime Collaboration.
- Unified Communications Operations Dashboard is not supported in MSP mode.

## Create a Floppy Image

The floppy image can be created in any 11.x Cisco Prime Collaboration Assurance server or in any RHEL 5.4 or CentOS 7.2 or CentOS 7.3 or CentOS 7.5 servers. The procedure details the steps to create a floppy image which is required for the installation of HypervisorAgnostic Cisco Prime Collaboration Assurance.

**Step 1** To check for floppy drive (fd - partition [0/1/2/3]).

```
dmesg | grep -i Floppy
```

**Step 2** To create a floppy (.flp) image.

```
dd if=/dev/zero of=<custom defined name.flp> bs=512 count=2880
```

(for example, custom defined name is PCAVirtualFloppy.flp)

**Step 3** To create a directory (/media/floppy).

```
mkdir -p /media/floppy
```

**Step 4** To create partition of type ext4.

```
mke2fs <custom defined name.flp>
```

(For example, custom defined name is PCAVirtualFloppy.flp.)

**Note** Provide the same custom defined name as defined in Step 2.

**Step 5** Mount the floppy image with predefined partition to the directory created in Step 3.

```
mount -o loop <custom defined name.flp> /media/floppy/
```

**Step 6** Download the PCAAnswer.xml template file from CCO site. Fill in the necessary values in the PCAAnswer template file specific to the OVA's used for deployment. Manually, copy the PCAAnswer.xml file to the location:

```
/media/floppy
```

**Note** Copy the PCAAnswer.xml file to **/media/floppy** location with all the necessary values filled.

*Table 7: Property Key and Values for Small-hva, Medium-hva, Large-hva, VeryLarge-hva, and VeryLarge-db-hva OVA(s)*

| Property Key | Example for Possible Values | Values for Respective Profiles<br>Mandatory - Y; Optional - O; Not Applicable - N | | |
|---|---|---|---|---|
| | | Small, Medium, and Large | Very Large | VeryLarge-db |
| com.cisco.nm.cpcm.DNS.1 | cisco.com | Y | Y | Y |
| com.cisco.nm.cpcm.OVA-Mode.1<br>Small - 0; Medium - 1; Large - 2; VeryLarge - 3;<br>VeryLarge-db - 4 | 0 | Y | Y | Y |
| com.cisco.nm.cpcm.applicationMode.1<br>Enterprise - 0; MSP - 1 | 0 | Y | Y | Y |
| com.cisco.nm.cpcm.gateway.1 | 10.78.86.1 | Y | Y | Y |
| com.cisco.nm.cpcm.hostname.1 | PCA-217 | Y | Y | Y |
| com.cisco.nm.cpcm.ip.1 | 10.78.86.217 | Y | Y | Y |
| com.cisco.nm.cpcm.nameserver.1 | 72.163.128.140 | Y | Y | Y |
| com.cisco.nm.cpcm.netmask.1 | 255.255.255.0 | Y | Y | Y |
| com.cisco.nm.cpcm.ntpServer.1 | olab-time | Y | Y | Y |
| com.cisco.nm.cpcm.isAnalyticsEnabled.1 | Enable - 1; Disable - 0 | N | Y | N |
| com.cisco.nm.cpcm.remoteIp.1 | 10.77.93.119 | N | O | Y |
| com.cisco.nm.cpcm.systemTimezone.1 | Asia/Kolkata | Y | Y | Y |
| com.cisco.nm.cpcm.ucodInstallMode.1<br>No Installation - 0; Master - 1; Responder - 2;<br>Both (Master and Responder) - 3<br>For more information, see the “Cisco Prime Collaboration Assurance UCOD” User Guide. | 3 | Y | Y | N |

**Step 7** To unmount the mount point

```
umount /media/floppy
```

**Note** If a floppy image is residing in <xyz> server, copy the virtual floppy drive image (.flp) to the local system from where you can browse and upload to the corresponding ESXi DataStore.

### What to do next

For information on the method to deploy small-hva, medium-hva, large-hva, verylarge-hva, and verylarge-db-hva OVA(s), see the section on "Deploy Small, Medium, and Large Cisco Prime Collaboration Assurance OVA Through ESXi" and "Deploy Very Large Cisco Prime Collaboration Assurance OVA Through ESXi".

## Deploy Small, Medium, and Large Cisco Prime Collaboration Assurance OVA Through ESXi

**Step 1** Deploy the HypervisorAgnostic OVA on the available ESXi.

**Note** Do not Power ON the deployed Virtual Machine.

**Step 2** In the **Host / Cluster** window, select the **Host** or **Cluster** on which you want to run the deployed template, and then click **Next**.

**Step 3** In the **Storage** window, select a destination for the virtual machine files, and then click **Next**.

**Step 4** In the **Disk Format** window, select the **Thick Provision Lazy Zeroed** format to store on the virtual disks, and then click **Next**.

In case of multiple networks during Cisco Prime Collaboration Assurance OVA deployment, ensure that the virtual machine network you select belongs to Cisco Prime Collaboration Assurance and is reachable.

**Step 5** Verify the options in the **Ready to Complete** window, and then click **Finish** to start the deployment.

**Note** Check the progress bar in the **Deploying Virtual Appliance** window to monitor the task status.

**Step 6** Click **Close**. The virtual appliance that you deployed appears in the left pane of the vSphere Client, under the host.

**Step 7** Power ON the Virtual Machine to start the Cisco Prime Collaboration Assurance installation process. Open VMConsole of the deployed Virtual Machine to monitor the sequence of installation steps to determine whether it is success or failure. The installation takes a maximum of 30 minutes to complete.

**Note**

- If installation is successful, Root Access and VMConsole Access is disabled by default.
- If installation fails, system will be in the monitoring state for an hour after which Root Access and VMConsole Access will be enabled.

  **Enabling Root Access and VMConsole Access**: Root Access and VMConsole Access is automatically enabled when the Cisco Prime Collaboration Assurance detects configuration errors. Access is enabled to rectify any configuration errors that has caused the installation to fail.

  **Disabling Root Access and VMConsole Access**: Root Access and VMConsole Access is again disabled whenever all the Cisco Prime Collaboration Assurance processes come up successfully or when reboot is issued for the next time.

### What to do next

For information on the steps to configure deployed floppy image, see the section on Configure the Deployed Floppy Image.

# Deploy Very Large Cisco Prime Collaboration Assurance OVA Through ESXi

**Step 1** Deploy the HypervisorAgnostic OVA on the available ESXi.

**Note** Do not Power ON the deployed Virtual Machine.

**Step 2** In the **Host / Cluster** window, select the **Host** or **Cluster** on which you want to run the deployed template, and then click **Next**.

**Step 3** In the **Storage** window, select a destination for the virtual machine files, and then click **Next**.

**Step 4** In the **Disk Format** window, select the **Thick Provision Lazy Zeroed** format to store on the virtual disks, and then click **Next**.

In case of multiple networks during Cisco Prime Collaboration Assurance OVA deployment, ensure that the virtual machine network you select belongs to Cisco Prime Collaboration Assurance and is reachable.

**Step 5** Verify the options in the **Ready to Complete** window, and then click **Finish** to start the deployment.

**Note** Check the progress bar in the **Deploying Virtual Appliance** window to monitor the task status.

**Step 6** Click **Close**. The virtual appliance that you deployed appears in the left pane of the vSphere Client, under the host.

For information on the steps to configure deployed floppy image, see the section on Configure the Deployed Floppy Image.

If you choose to enable Cisco Prime Collaboration Analytics in very large OVA deployment of Cisco Prime Collaboration Assurance, you require two virtual machines - Database and Application. Reserve two IP address in advance for database and application server, since IP address of application server is required while installing database server and database server IP address is required while installing application server.

**Note**

- Ensure to deploy VeryLarge-db-hva OVA to configure the database server.
- The sequence in which the deployment takes place is that the Database Server should be started with all services and then Application Server should be installed.
- For information on the methods to "Configure the Database Server and Application Server", see the section on Preparation of the PCAAnswer Template File.

**Step 7** You can now proceed with the section "Configure the Deployed Floppy Image".

# Configure the Deployed Floppy Image

**Step 1** Upload Floppy Image to the DataStore.

a) Select the deployed virtual machine to view the summary in the **Summary** tab.
You can view the summary of the deployed virtual machine on the right side of the screen.

b) In the **Summary** tab, under **Storage**, click on the DataStore.
**DataStore Browser** window appears.

c) Right-click on the DataStore and choose **Browse DataStore** to browse and add the floppy image (.flp).

d) Click **Upload files to this datastore** available on the header of the window.

e) Choose **Upload File...**.

f) Select the floppy image (<filename.flp>) from the local system and click **Open**.
The floppy image is uploaded from the local system and listed on the DataStore browser.
g) Close the window.

For information about adding a floppy drive to the HypervisorAgnostic Virtual Machine, see Adding Floppy Drives to a Virtual Machine.

**Note** During mounting the floppy image, ensure to check the **Connect at power on** check box.

**Step 2** Select the deployed Virtual Machine and right-click to choose **Power** > **Power On**.

**Step 3** Click **OK**.

**Note** Installation takes about 30 minutes to complete.

**Step 4** Upon Power ON the Virtual Machine starts the Cisco Prime Collaboration Assurance installation process. Open VMConsole of the deployed Virtual Machine to monitor the sequence of installation steps to determine whether it is success or failure. The installation takes a maximum of 30 minutes to complete.

**Note**
- If installation is successful, Root Access and VMConsole Access is disabled by default.
- If installation fails, system will be in the monitoring state for an hour after which Root Access and VMConsole Access will be enabled.

  **Enabling Root Access and VMConsole Access**: Root Access and VMConsole Access is automatically enabled when the Cisco Prime Collaboration Assurance detects configuration errors. Access is enabled to rectify any configuration errors that has caused the installation to fail.

  **Disabling Root Access and VMConsole Access**: Root Access and VMConsole Access is again disabled whenever all the Cisco Prime Collaboration Assurance processes come up successfully or when reboot is issued for the next time.

### What to do next

After successful deployment, login to Cisco Prime Collaboration Assurance 12.1. For information, see the section on Log in to Cisco Prime Collaboration Assurance.

## Modify the Mounted Floppy Image in the Deployed Virtual Machine

**Step 1** Go to **Edit Settings** of the deployed Virtual Machine.

**Step 2** Select **Floppy Drive** > **Use existing floppy image in DataStore**.

**Step 3** Click **Browse** and choose the floppy image (.flp) from the DataStore.

**Step 4** Check both **Connected** and **Connect at Power on** check box(s).

# OVF Tool

Open Virtualization Format (OVF) is an industry standard to describe metadata about virtual machine images in XML format. OVF Tool is a command-line utility that helps users import and export OVF packages to and from a wide variety of products.

Using OVF to distribute virtual machines has the following benefits:

- Ease of use. When users receive a package in OVF format, they do not have to unzip files, execute binaries, or convert disk formats. Adding a vApp can be as simple as typing a URL and clicking **Install**.
- Metadata inclusion. Additional metadata, such as an end-user license agreement, can be packaged with the OVF and displayed before installation.
- Optimized download from the Internet. Large virtual disks are compressed for fast download and to reduce disk space for large template libraries.

This section provides the following information:

## Setting Up the OVF Tool

You can find the latest information about System Requirements, supported VMware software and platforms, installation, and known issues by reading the latest release notes located at the following web page: Latest Release Notes from VMware.

**Installation Prompts**

Following fields are mandatory:

1. Server Hostname
2. Network IP Address
3. IP Default Netmask
4. IP Default Gateway
5. Default DNS Domain

**To run VMware OVF Tool from the command line**

**Step 1** At the command-line prompt, run the OVF Tool as follows: `ovftool <source locator> <target locator>` where `<source locator>` and `<target locator>` are paths to the source and target for the virtual machine, OVF package, OVA package, or vSphere location.

If you are using an operating system where spaces are not allowed in paths on the command line, and need the full path to run OVF Tool, enclose the path in quotes as shown below:

```
"/Applications/VMware OVF Tool/ovftool" --help
```

**Step 2** If you want to specify additional options, type them before the source and target locators. `ovftool <options> <source locator> <target locator>`

**Step 3** To display all options, type **ovftool -h**

### What to do next

For information on the method to create a configuration file, see the section on "Create a Configuration File".

## Create a Configuration File

```
#OVF_OPTIONS='--overwrite --noSSLVerify --acceptAllEulas -dm=thick'
X:injectOvfEnv
X:enableHiddenProperties
overwrite
noSSLVerify
acceptAllEulas
diskMode=thick
powerOn
name=10.78.86.216_<name>
prop:com.cisco.nm.cpcm.ip.1=X.X.X.X
prop:com.cisco.nm.cpcm.netmask.1=255.255.255.0
prop:com.cisco.nm.cpcm.hostname.1=<hostname>
prop:com.cisco.nm.cpcm.gateway.1=X.X.X.X
prop:com.cisco.nm.cpcm.DNS.1=cisco.com
prop:com.cisco.nm.cpcm.nameserver.1=X.X.X.X
prop:com.cisco.nm.cpcm.ntpServer.1=clock.cisco.com
prop:com.cisco.nm.cpcm.systemTimezone.1=<systemTimeZone>
prop:com.cisco.nm.cpcm.licenseMode.1=2
prop:com.cisco.nm.cpcm.applicationMode.1=1
prop:com.cisco.nm.cpcm.ucodInstallMode.1=1
prop:com.cisco.nm.cpcm.isUpgrade.1=1
prop:com.cisco.nm.cpcm.backupServerIp.1=X.X.X.X
prop:com.cisco.nm.cpcm.backupServerPort.1=<portnumber>
prop:com.cisco.nm.cpcm.backupServerUsername.1=<backupServerUsername>
#prop:com.cisco.nm.cpcm.backupServerPassword.1=<backupServerPassword>
prop:com.cisco.nm.cpcm.backupPath.1=/opt/tempbackups/DMA_Backup
datastore=DS-X.X.X.X
network=VM Network
```

| Parameter | Example |
|---|---|
| ip | 10.78.86.216 |
| hostname | testCentos16 |
| gateway | 10.78.86.1 |
| nameserver | 72.163.128.140 |
| timezone | Asia/Kolkata |
| datastore | 10.78.86.211 |

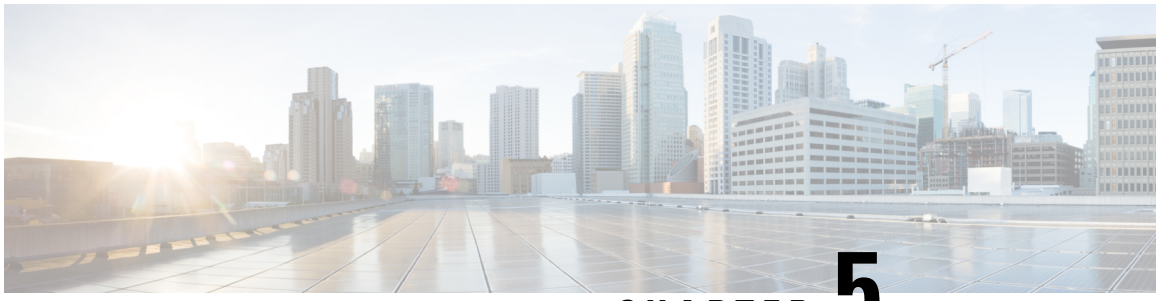
**Note** The above parameters must be saved with extension **.ovftool**.

## Adding Files from an OVF Package

To add files to a vCenter Server from an OVF package, use the following syntax: `ovftool /Location/cpcm-assurance-12.1.0.XXX.ova vi://"Username":"Password"@"Vcenter-IP/FDQN-Name/Datacenter-Name/host/ESXI IP/"`

(For example, ovftool /root/Downloads/cpcm-assurance-12.1.0.995-small.ova vi://"administrator@vsphere.local":"Password!123"@"10.1.1.20-DS/host/10.1.1.20/"

**Note** Any special characters in username and password must be replaced with ASCII characters. For more information, see VMWare Documentation



CHAPTER 5

# Get Started after New Installation

This section explains the following:



# Log in to Cisco Prime Collaboration Assurance

You can invoke Cisco Prime Collaboration Assurance using the client browser.

**Step 1** Open a browser session from your machine.

See the System Requirements - Server and Client Machine Requirements for information about supported browsers.

**Step 2** Enter the `https://<IP_address_of_Prime_Collaboration_application>`

HTTPS has been enabled by default for Cisco Prime Collaboration Assurance. You may use either the IP address or the hostname of the application. If you have configured DNS, we recommend that you use the hostname.

Based on the browser you are using, you see one of the following:

- In Windows Internet Explorer, the **Certificate Error: Navigation Blocked** window.
- In Mozilla Firefox, the **Untrusted Connection** window.

These windows appear because Cisco Prime Collaboration uses a self-signed certificate. Cisco Prime Collaboration Assurance is shipped with self-signed certificate, which is valid for five years.

**Step 3** Remove the SSL certificate warning. For more information on removing SSL Certificate Warning, see Remove the SSL Certificate Warning in Mozilla Firefox, on page 73.

**Step 4** During the first login to Cisco Prime Collaboration Assurance, the URL takes the user to Cisco Prime Collaboration Assurance Serviceability User Interface. Log in as *globaladmin*, with default credentials. The user is prompted to change the default password. Post successful password change, click on the cross launch Click here to open PC Assurance on the Dashboard to navigate between Cisco Prime Collaboration Assurance and Cisco Prime Collaboration Assurance Serviceability.

**Note**

- To launch Cisco Prime Collaboration Assurance Serviceability, the default password is *Cisco123!* . You have to change the default password during the first login after a fresh installation. For detailed steps, see **Cisco Prime Collaboration Assurance Serviceability User Guide**.
- Ensure to configure your web browser to enable/allow pop-up for Cisco Prime Collaboration Assurance IP address before launching Cisco Prime Collaboration Assurance Serviceability. The Allow pop-up window for Cisco Prime Collaboration Assurance must be configured for all the supported web browsers.
- **For Cisco Prime Collaboration Release 12.1 SP4 and later**

  In the case of a very large deployment of 2 VMs, wait for Main (Application) Server installation to complete.

**Step 5** In the login page, log in as globaladmin, using the same credentials that you specified during the configuration. The **Cisco Prime Collaboration** landing page appears along with the Getting Started popup, where you can click the links listed under System Setup and Manage Network to configure the Cisco Prime Collaboration server.

# Troubleshooting

1. **Issue**: Unable to login to Cisco Prime Collaboration server after the browser timeout.

**Recommended Action**: Close the browser or browser tab and open a new browser window to log in again.

**For Cisco Prime Collaboration Release 12.1 SP4 and later**

2. **Issue**: Unable to reset globaladmin password of DB VM.

**Recommended Action**: Wait for Main (Application) Server installation to complete in very large deployment of 2 VMs.

# Get Started with Cisco Prime Collaboration Assurance

After you install the Cisco Prime Collaboration Assurance, perform the tasks listed in the following table:

***Table 8: Get started with Cisco Prime Collaboration Assurance Enterprise Mode***

| Step | Task and Description | Navigation in Cisco Prime Collaboration Assurance Application | Document to be referred |
|---|---|---|---|
| **Add license file** | | | |
| Step 1 | Add a new license file.<br>This step is applicable only if you have purchased Assurance Advanced and/or Analytics license. | **System Administration** > **License Management** | See the *Add and Delete a License File* section of "Manage Licenses" chapter in Cisco Prime Collaboration Assurance Guide - Advanced. |
| **Discover your Network** | | | |

| Step | Task and Description | Navigation in Cisco Prime Collaboration Assurance Application | Document to be referred |
|---|---|---|---|
| Step 1 | Set up the Devices for Auto Discovery.<br><br>Set up the devices in your network first, so that they are ready to get discovered by Cisco Prime Collaboration. | N/A | See Configure Devices for Cisco Prime Collaboration Assurance. |
| Step 2 | Add Device Credentials.<br><br>Add the device credentials to discover devices and collect their inventory details. Always create a different credential profile for each device type. | **Inventory** > **Inventory Management** > **Manage Device Credentials** | See the "Add a Device Credentials Profile" section of "Manage Device Credentials" chapter in Cisco Prime Collaboration Assurance Guide - Advanced. |
| Step 3 | Discover Devices.<br><br>• Discover Cisco Unified Communications Manager (including Cisco Unified IM and Presence) 9.x and later and Cisco Unity Connection 9.x and later applications.<br>• Discover Cisco TelePresence Management Suite<br>• Discover Cisco Expressway<br><br>The Cisco Expressway, Cisco Multipoint Control Unit, Cisco Profile and Codec, default gateway, and switches are discovered along with Cisco TelePresence Management Suite.<br><br>Cisco TelePresence Conductor is not auto discovered through TelePresence Management Suite. The Cisco TelePresence Conductor needs to be discovered separately.<br><br>For more information on supported devices, See Supported Alarms and Events for Cisco Prime Collaboration Assurance . | **Inventory** > **Inventory Management** > **Auto Discovery** > **Device Discovery** | See the "Add Devices—Auto Discovery" section of “Discover Devices” chapter in the Cisco Prime Collaboration Assurance Guide - Advanced. |

| Step | Task and Description | Navigation in Cisco Prime Collaboration Assurance Application | Document to be referred |
|---|---|---|---|
| Step 4 | Verify Inventory<br>**Note** This step is applicable only if you have purchased Assurance Advanced and/or Analytics license.<br>Verify whether all discovered devices are in the Managed state. | **Inventory** > **Inventory Management** > **Manage Credentials** | See the *Manage Inventory* chapter in the Cisco Prime Collaboration Assurance Guide - Advanced. |
| Step 5 | Import Conferences<br>**Note** This step is applicable only if you have purchased Assurance Advanced and/or Analytics license.<br>Import the video collaboration conferences Cisco TelePresence Management Suite Switch to monitor the conferences.<br>To periodically import conferences from Cisco TelePresence Management Suite, define the polling interval based on your business needs, using **Diagnose** > **Conference Diagnostics** > **Import Conference** . | **Diagnose** > **Conference Diagnostics** | See the *Conference Diagnostics Dashboard* section of "Monitor Conferences" chapter in Cisco Prime Collaboration Assurance Guide - Advanced. |
| Step 6 | Verify Conferences<br>**Note** This step is applicable only if you have purchased Assurance Advanced and/or Analytics license.<br>Verify whether all conference details have been imported from Cisco TelePresence Management Suite.<br>Cisco Prime Collaboration collects scheduled conferences data for five days (for the past one day, for the current day, and for three days ahead). | **Diagnose** > **Conference Diagnostics** | See the *Conference Diagnostics Dashboard* section of "Monitor Conferences " chapter in Cisco Prime Collaboration Assurance Guide - Advanced. |

| Step | Task and Description | Navigation in Cisco Prime Collaboration Assurance Application | Document to be referred |
|---|---|---|---|
| Step 7 | Configure Cisco Prime Collaboration as CDR and Syslog destination in Unified Communications Manager.<br><br>Ignore this step if you have enabled auto-configuration of this setting during the Unified CM auto-discovery.<br><br>Perform this step only after the Unified CM clusters are discovered and in a Managed state in Cisco Prime Collaboration. Configure Cisco Prime Collaboration as a CDR and Syslog destination in each of the managed Unified CM clusters. This enables you to monitor the CDR and CMR metrics, and the endpoint registration details. | NA | See Configure Devices for Cisco Prime Collaboration Assurance.<br><br>For information on auto-configuration, see the “Discover Devices” chapter in Cisco Prime Collaboration Assurance Guide - Advanced. |
| Step 8 | Set up the Trunk Traffic Maximum Capacity.<br><br>Perform this step only after the Unified CMs and gateways are discovered and in a Managed state in Cisco Prime Collaboration. You must configure the trunk maximum capacity in Cisco Prime Collaboration. This enables you to determine the busy-hour trunk traffic for each gateway, connected to the Cisco Unified UCM. | **Analytics Administration** > **Trunk Traffic Max Capacity Settings** | See the "Configuring Maximum Capacity for a Trunk or Gateway" of the "Prime Collaboration Analytics Dashboards and Reports" chapter in Cisco Prime Collaboration Analytics Guide . |
| **Set up Alarm Notifications** | | | |
| Step 1 | Set up the SMTP Server.<br><br>Configure the SMTP server so that you can receive alarms by email notifications. | **Alarm & Report Administration** > **E-mail Setup for Alarms & Events** | See the "Configure SMTP Server" section of "Configure System Parameters" chapter in Cisco Prime Collaboration Assurance Guide - Advanced. |

| Step | Task and Description | Navigation in Cisco Prime Collaboration Assurance Application | Document to be referred |
|---|---|---|---|
| Step 2 | Set up Alarm Notifications.<br>Create notification groups based on notification criteria of your choice, for the notifications such as SNMP trap, e-mail, and syslog. | **Alarm & Report Administration** > **Notification Setup** | See the "Add a Device Notification Group" section of "Configure Notifications" chapter in Cisco Prime Collaboration Assurance Guide - Advanced. |
| **Set up the Cisco Prime Collaboration Server** | | | |
| Step 1 | Create Users and Assign Roles .<br>Create users and provide them with role-based access control for multiple levels of authorization . | **System Administration** > **User Management** | See the *Add a User* section of “Manage Users” chapter in Cisco Prime Collaboration Assurance Guide - Advanced. |
| Step 2 | Back up Settings.<br>Perform or schedule periodic data backups. Data can be restored either on the same system or any other system in the event of a system failure. | **System Administration** > **Backup settings** | See the "Schedule Backup using Cisco Prime Collaboration User Interface" section of "Perform Backup and Restore" chapter in the Cisco Prime Collaboration Assurance Guide - Advanced. |
| Step 3 | Create Domains.<br>Create domains to group different devices and assign these domains to users | **System Administration** > **Domain Setup** | See the "Add Domains" section of “Manage Domains” chapter in Cisco Prime Collaboration Assurance Guide - Advanced. |

# Access the System Setup, Manage Network, and License

**User Interface**

The following table lists the menu items that are displayed on the Cisco Prime Collaboration Assurance user interface:

| Cisco Prime Collaboration Assurance - Advanced |
|---|
| **Getting Started** |
| **Netwrok Health Overview** |
| **Monitor** |

| Cisco Prime Collaboration Assurance - Advanced |
|---|
| **Inventory** |
| **Diagnose** |
| **Synthetic Tests** |
| **Reports** |
| **Analytics** |
| **Alarm & Report Administration** |
| **Analytics Administration** |
| **System Administration** |
| **UC Operations Dashboard** |
| **Serviceability** |

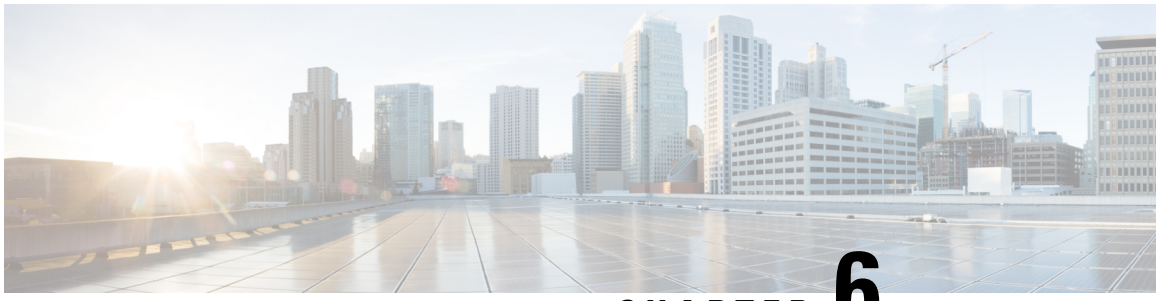
**Note** The conference times out if there is no activity for 15 minutes.

The following is a list of pages that never time out:

- **Network Health Overview**
- **Customer Summary Dashboard (in MSP mode)**
- **Diagnostics Test pages (UC Application Synthetic Test, Audio Phone Features Test, Video Test, and Batch Test)**
- **Endpoint Diagnostics**
- **Performance Dashboards**
- **Conference Diagnostics**
- **All Topology** pages

PART II

# Migrate Cisco Prime Collaboration Assurance



CHAPTER 6

# Migrate Cisco Prime Collaboration Assurance

**This chapter is NOT applicable for 12.1 Service Pack 3 and later releases.**

This section explains the following:



# Overview of Data Migration Assistant

**Note** Migration from Cisco Prime Collaboration Assurance 11.x to Cisco Prime Collaboration Assurance 12.1 Service Pack 3 is not supported.

This chapter provides an overview of Data Migration Assistant (DMA), explains how to install and use it, and provides related information.

DMA assists in migrating Cisco Prime Collaboration Assurance data from supported versions of 11.x to Cisco Prime Collaboration Assurance 12.1.

If you want to migrate from 11.x to 12.1 for both ENT/MSP modes, the following DMA paths are supported:

***Table 9: Supported Versions***

| Mode | 11.5 | 11.5 SP1 | 11.6 |
|---|---|---|---|
| ENT | No | No | Yes |
| MSP | Yes | No | Yes |

**Mandatory Migration Path** for 11.x to 12.1 customers,

```
Install 12.1 FCS -> Apply 12.1 SP1 -> Perform DMA
```

**Note** We recommend you to perform the following before migration.

Apply 12.1 SP1 on 12.1 Fresh installation. For more information on installing 12.1 Service Pack 1, see the "Readme for Cisco Prime Collaboration Assurance and Analytics 12.1 Service Pack 1".

Use the Backup RPM as mentioned in the "Readme for Cisco Prime Collaboration Assurance and Analytics 12.1 Service Pack 1".

12.1 Service Pack 1 Backup RPM can be downloaded from CCO at Software Download.

**Path**: Downloads Home / Cloud and Systems Management / Collaboration and Unified Communications Management / Prime Collaboration / Prime Collaboration Assurance 12.1 / Prime Collaboration Patches- 12.1 Service Pack1

The reason for migration is due to the change in the underline operating system of Cisco Prime Collaboration Assurance.

Data Migration Assistant is performed in the following method:

- Data Migration Assistant Backup - Use Perform Data Migration Assistant Backup to backup your data on 11.x server.
- Data Migration Assistant Restore - Use Perform Data Migration Assistant Restore to restore the backup data on 12.x server.

**Note**

- We recommend you to perform DMA backup either during lean or maintenance period because Cisco Prime Collaboration Assurance Database (DB) restarts twice (once at the beginning and once at the end), as part of a few DMA configuration setup. This restart leads to inconsistent system after backup.
- Currently, the time taken to perform a DMA backup of 50 GB data from 11.x server to 12.1 is around 4 to 5 hours. For a fully loaded setup it takes a minimum of 30 hours.

# Preinstallation Guidelines

Review the following guidelines and perform the appropriate steps before installing DMA:

1. If a PKCS7 or PKCS12 certificate is applied to 11.x and the Cisco Prime Collaboration Assurance is migrated to version 12.1, the certificate will not be restored. You need to regenerate the certificate for the Cisco Prime Collaboration Assurance 12.1.

**Note** From Cisco Prime Collaboration Assurance 11.6 onwards, only PKCS12 certificate is supported.

2. You cannot restore the purchased license of Cisco Prime Collaboration Assurance 11.x to 12.1. You must purchase the license with the same endpoint count for Cisco Prime Collaboration Assurance 12.1. Once

the DMA migration is completed successfully, the Cisco Prime Collaboration Assurance 12.1 server will be in Evaluation mode.

3. DMA backup is not supported in Cisco Prime Collaboration Assurance Release 11.x in “FIPS mode and Standard mode”.
4. DMA restore is not supported in Cisco Prime Collaboration Assurance Release 12.1 in “FIPS mode”.
5. If you have deployed in MSP mode, the Video endpoints with Public IP address(es) become Unreachable after DMA restore.

Following sFTP Servers are supported in the Cisco Prime Collaboration Assurance Data Migration Assistant.

***Table 10: sFTP Servers Supported***

| sFTP Server |
|---|
| Mac OS X |
| Windows SolarWinds |
| Windows FreeFTPd |
| CentOS sFTP Server |
| Linux sFTP Server |

# Pre-requisites for Backup and Restore

### Before you begin

**Pre-requisites for Backup**

1. If you want to perform data migration from 11.0 or 11.1 versions to 12.1 version then first upgrade to the supported upgrade path of either 11.5 or 11.6 versions and then perform data migration to 12.1 version. For more information, see the table on “Supported Versions” in the chapter on “Overview of Data Migration Assistant”.
2. Enable Root Access on 11.x servers before performing Data Migration Assistant (DMA). For steps to enable root access, see Enable Root Access in 11.x Server.
3. If you have created the Phone Status test in Cisco Prime Collaboration Assurance 11.6 server then it is mandatory to run the following commands. This way you can export the existing Phone Status test to a file that can be used to import tests after DMA migration.
   a. Login to the Cisco Prime Collaboration Assurance server as ***root***.
   b. Create a new text file '11.6_PhoneStatusImportFile.txt' with read and write permissions at **/opt/emms/cuom/ImportFiles**.
   c. Run the following command:

```
/opt/postgres/9.2/bin/psql -p 5433 --username=cmuser  cpcm -c "copy (select
extensionnumber, macaddress, ipaddress, saaipaddress from prphone) to '/opt/emms/cuom/
ImportFiles/11.6_PhoneStatusImportFile.txt' delimiter ':';"
```

After running the above commands, you are required to delete all the Phone Status test created in the Cisco Prime Collaboration Assurance 11.6.

4. Delete all the Batch and subsequent Synthetic tests from the Cisco Prime Collaboration Assurance 11.6.
5. Backup is created with hostname in backup path (For example, if the backup path is **/tempbackups** then the backup will be available at: **{ssh username}/tempbackups/{hostname}**).

**Note** The hostname of 11.x and 12.1 should be the same. If the values do not match, then DMA restore fails.

6. The expected time taken for the DMA to complete the backup process varies depending on the profile and data of the backup server.
7. **Disable CDR/CMR configuration on CUCM** Disabling CDR/CMR configuration on CUCM prevents CUCM sending bulk CDR/CMR(s). Perform the following steps:
   a. Go to **CUCM Serviceability** page of all managed CUCM publishers.
   b. Navigate to **Tools** > **CDR Management**.
   c. Select the **PCA IP address/Hostname**.
   d. On the **Billing Application Server Parameters** section, uncheck **Resend on Failure** check box and click **Update**.

**Note** Make sure whether the check box is already unchecked.

8. If Analytics is enabled, the Cisco Prime Collaboration Assurance and Analytics Database (DB) restarts during DMA backup.

**Note** Backup must be taken from 11.x server with the RPM that is provided on CCO site.

**Pre-requisites for Restore**

**Note** The system reboots after successful DMA restore.

1. The expected time taken for the DMA to complete the restore process varies depending on the profile and data of the backup server.
2. The Deleted state devices/endpoints will be purged and after the upgrade these (the devices/endpoints) will not be available.
3. DMA restore on Cisco Prime Collaboration Assurance 12.1 should be performed through Serviceability after taking a DMA backup on 11.x server.
4. The hostname of 11.x and 12.1 should be the same. If the values do not match, then DMA restore fails.

For information on preinstallation guidelines, see the section on Preinstallation Guidelines.

# DMA Backup and Restore Time Period - Approximate Values

The time taken for DMA Backup and Restore varies according to the database size. **Approximate** time taken for different sizes are listed in the table below.

| | Assurance DB Size | Assurance Backup Time | Assurance Restore Time | Analytics DB Size | Analytics Backup Time | Analytics Restore Time | Total Backup Time | Total Restore Time | Total Time Taken for Migration (Excluding Process Startup Time) |
|---|---|---|---|---|---|---|---|---|---|
| Small | 5 GB | 10 minutes | 25 minutes | 60 GB | 50 minutes | 25 minutes | 1 hour | 50 minutes | 1 hour 50 minutes |
| Medium | 15 GB | 25 minutes | 1 hour 5 minutes | 150 GB | 1 hour 15 minutes | 1 hour | 1 hour 40 minutes | 2 hours 5 minutes | 3 hours 45 minutes |
| Large | 25 GB | 35 minutes | 1 hour 45 minutes | 279 GB | 2 hours 40 minutes | 1 hour 40 minutes | 3 hours 15 minutes | 3 hours 5 minutes | 6 hours 20 minutes |
| Very Large | 39 GB | 55 minutes | 2 hours 40 minutes | 383 GB | 3 hours 5 minutes | 2 hours 10 minutes | 4 hours | 4 hours 50 minutes | 8 hours 50 minutes |

# Preparation for Data Migration Assistant

1. For Very Large Deployment, if Analytics is enabled, perform the following:
   a. Enable root for DBVM.
   b. Install the backup RPM in both DBVM and MainVM.
   c. Perform DMA only on the MainVM and when prompted provide password for DBVM on Cisco Prime Collaboration Assurance 12.1.

      If Analytics is disabled or if you do not require Analytics data to be migrated, then DMA has to be performed on the Application server.

2. The hostname of 11.x and 12.1 should be the same and the IP address for both these servers should also be same. If the values do not match, then DMA restore fails.

# Enable Root Access in 11.x Server

Perform the following steps to enable root access in 11.5 and 11.6 servers.

**Step 1** Login as admin from the Cisco Prime Collaboration Assurance VM Console.

```
admin/admin# root_enable
```

**Step 2** Configure the root patch password.

```
admin/admin# root
```

**Step 3** Enter the root password.

```
ade# /opt/emms/emsam/bin/enableRoot.sh
```

**Step 4** Configure the actual root password.

```
ade# passwd
```

### What to do next

Perform DMA (Data Migration Assistant) from Cisco Prime Collaboration Assurance Serviceability.

# Perform Data Migration Assistant Backup

For Pre-requisites, see the section "Pre-requisites for Backup and Restore".

**Step 1** Copy RPM (as shown in the example below) to **/opt**.

For example, CSCOpca-dma-x.x-x.x86_64.rpm.

**Note** For more information, see the respective Read me of Engineering Special or Service Pack release for exact RPM name to be downloaded and used.

The RPM is available on the Cisco Connection Online (CCO) postings.

**Step 2** Run below commands to install RPM.

```
#cd /opt
#rpm -ivh CSCOpca-dma-x.x-x.x86_64.rpm
```

**Note**

- To verify whether the RPM is installed successfully, run the following command:

  ```
  rpm -qa | grep -i CSCOpca-dma
  ```

  The command with an entry is displayed as follows:

  ```
  rpm -qa | grep -i CSCOpca-dma
  Result: CSCOpca-dma-x.x-x
  ```

- If the installation of RPM fails or exists abruptly, run the following command to remove the RPM:

  ```
  rpm -e CSCOpca-dma--x.x-x
  ```

  Or

  ```
  yum remove CSCOpca-dma-x.x-x
  ```

- To verify whether the RPM is uninstalled successfully, run the following command:

  ```
  rpm -qa | grep -i CSCOpca-dma
  ```

The result of the command should not display any entry (**`CSCOpca-dma-x.x-x`**).

**Note** If the error continues to occur, contact the Cisco Technical Assistance Center (TAC) for assistance.

**Step 3** Go to directory **/opt/emms/infra/dma/**.

**Step 4** Run script **./pcandma.sh**.

**Step 5** Enter the values when prompted:

a) **sFTP Server (IP Address)**: Enter sFTP server IP address to store the backup.

Choose any of the sFTP server(s) where DMA backup can be stored and later fetched during DMA restore.

b) **sFTP Port**: Enter sFTP server port number.
c) **User Name**: Enter the username.
d) **Path**: Enter sFTP server backup path.
e) **Password**: Enter the sFTP password.

***Table 11: Field Names with Examples***

| Field Name | Example |
|---|---|
| sFTP Server (IP Address) | 10.78.88.102 |
| sFTP Port | 22 |
| UserName | Enter a name for the Username. For example, **user1** or provide any desired name. |
| Path | Enter the path.<br>The DMA backup is taken in the path relative to the sFTP user home directory.<br>If path is **/backup**, the DMA backup location will be **/user1/backup/{hostname}.** |

**Step 6** Verify for backup in sFTP server at the configured backup location.

If the sFTP UserName is **user1** and the configured backup path is **/backup**, then the backup resides at **/user1/backup/{hostname}**.

Here **{hostname}** is the directory created with the 11.x server's hostname.

**Step 7** Backup file is generated in gpg format for Assurance and Analytics and uploads to sFTP server under the hostname folder under the configured backup location: **/user1/backup/{hostname}**.

For example, if **/backup** is the configured backup location, where the backup is available at **/user1/backup/{hostname}**, where **user1** is the sFTP user home directory and **backup** is Assurance_Backup.tar.gz, Analytics_Backup.tar.gz.

### What to do next

For information on performing Data Migration Assistant Restore, see the section on Perform Data Migration Assistant Restore.

# Troubleshooting

**Issue**: DMA backup fails.

**Conditions**: Following are the conditions:

- sFTP server is not reachable
- Credentials do not match
- Upload of backup file fails and so on

  Relevant messages appear on console.

**Possible Solution**: Following are the logs for reference -

- /var/log/pcandma.log - Provides basic information of the Cisco Prime Collaboration Assurance and Analytics DMA.
- /var/log/dma_debug.log - Provides a complete debug messages of DMA.
- /var/log/assurance_backup_dma.log - Provides detailed information of Assurance backup DMA.
- /var/log/analytics_dma.log - Provides detailed information of Analytics DMA.

# Credential Verification Error Messages for DMA Backup

The credential verification error messages for DMA Backup are tabulated below.

| Error Message | Conditions | Possible Solutions |
|---|---|---|
| Login failed, sFTP server is not reachable. | Invalid sFTP server IP address entered for backup in 11.x server. | Enter an appropriate IPaddress. |
| Unable to connect to the server. Session timed out. | Invalid sFTP port number entered for backup in 11.x server. | Enter an appropriate sFTP Port number. |

| Error Message | Conditions | Possible Solutions |
|---|---|---|
| Login failed, sFTP user name or password is wrong. | Invalid sFTP server credentials entered for backup in 11.x server. | Enter an appropriate sFTP server credentials. |
| Couldn't create directory <location> in sFTP server. | Invalid sFTP server backup path entered for backup in 11.x server. | Enter valid path and try backup again. |
| The data filesystem is <disk usage> % full. The threshold is 85 % . Starting a backup may result in filling up the filesystem. Warning user and aborting backup. Insufficient disk space to perform full backup. | If the disk usage is greater than 85% in backup server. | Check free space and try backup again. |
| Cisco Prime Collaboration Assurance is in FIPS mode. | The DMA backup process terminates, since DMA backup is not supported in FIPS mode. | Turn OFF FIPS mode in PCA to continue DMA backup and start the backup process. |
| Cisco Prime Collaboration Assurance in STANDARD mode. | The DMA backup process terminates, since DMA backup is not supported in STANDARD mode. | - |

# Perform Data Migration Assistant Restore

For Pre-requisites, see the section "Pre-requisites for Backup and Restore".

**Note** When DMA restore is in progress and until DMA is successful, you will not be able to access the following: Cisco Prime Collaboration Assurance User Interface, UCOD application, and all other features of Cisco Prime Collaboration Assurance Serviceability. Once DMA is successful, system reboots and launches the Cisco Prime Collaboration Assurance Serviceability (Login using 11.x password).

**Step 1** Login to Cisco Prime Collaboration Assurance Serviceability.

**Note** For future DMA status logging purpose, enable root access from Cisco Prime Collaboration Assurance Serviceability and take a snapshot of the Virtual Machine. For information, see the chapter on “Root Access” in “Cisco Prime Collaboration Assurance Serviceability” User Guide for Release 12.1.

**Step 2** Choose DMA (Data Migration Assistant) in Cisco Prime Collaboration Assurance Serviceability User Interface.

A confirmation message appears indicating whether you want to perform Data Migration.

- Click **OK** to perform Data Migration. Follow **substeps a** through **substeps e** of Step 3 for a successful data migration.
- Click **Cancel** to close.

  If you click **OK** the application loads the DMA configurations.

**Note** The system reboots after successful DMA restore.

In case of a 2VM setup for a Very Large Deployment, perform the following steps:

**Note** Ensure to enable root access for both DB VM and Main VM before performing Data Migration, to monitor all the activities during the migration. For steps to enable root access, see the chapter on "Root Access" in "Cisco Prime Collaboration Assurance Serviceability" User Guide for Release 12.1.

**a.** Very Large Deployment is a 2VM setup:

1. **DB VM**
   - **a.** In Cisco Prime Collaboration Assurance Serviceability User Interface of DB VM, click **DMA**

     **Note** Read the instructions on the screen carefully before you click OK.

   - **b.** Click **OK**.

     This configures the DB VM server for DMA restore.

2. **Main VM**
   - **a.** In Cisco Prime Collaboration Assurance Serviceability User Interface of Main VM, click **DMA**.

     **Note** Read the instructions on the screen carefully before you click OK.

   - **b.** Click **OK**.

     This configures the Main VM server for DMA restore.

This takes you to the DMA sFTP configuration page of the Cisco Prime Collaboration Assurance Serviceability of the Main VM.

Provide the details of the sFTP server (where the backup is stored) and proceed with DMA configuration.

**Step 3** Perform the following steps:

a) Enter the following values on the **DMA** page.

1. **sFTP Server (IP Address)**: Enter sFTP server IP address where the backup resides.
2. **sFTP Port**: Enter sFTP server port number.
3. **Path**: Enter sFTP server backup path.
4. **User Name**: Enter the username.
5. **Password**: Enter the sFTP password.

| Parameter | Example |
|---|---|
| sFTP Server IP address | 10.78.88.102 |
| sFTP Port number | 22 |
| User Name | Enter a name for the User Name. For example, **user1** or provide any desired name. |

| Parameter | Example |
|---|---|
| sFTP server backup path | Enter the path (relative to the sFTP user home directory). For example, **/backup** if the backup resides in **/user1/backup/{hostname}**.<br>Here **{hostname}** is the directory with the 11.x server's hostname. |

b) Click **Test Connection** to test the sFTP connection.

**Note** In case of test connection failure, possible are the reasons:

- sFTP IP address invalid or not reachable.
- sFTP port number invalid.
- sFTP path invalid.
- sFTP user name or password wrong.

c) Click **Start DMA** to perform DMA restore.

During this process, a progress bar appears indicating the progress of data migration. You can also click on View DMA Status Detail link to view the DMA status detail log indicating DMA Success or Failure status.

A notification appears once DMA is completed.

d) If you have deployed in MSP mode, the Video endpoints with Public IP address(es) become Unreachable after DMA restore.

In such cases, delete the Video endpoints from Inventory Management page and add them with Public and Private IP address(es).

e) Once DMA Restore process completes, the Cisco Prime Collaboration Assurance 12.1 server reboots.

Login to Cisco Prime Collaboration Serviceability and Cisco Prime Collaboration Assurance using the 11.x password. Logging on to Cisco Prime Collaboration Assurance Serviceability provides access to all the menus.

Consider the following methods to validate DMA. For information, see Validate Data Migration Assistant.

f) If DMA fails, you can view the failure log. The login to Cisco Prime Collaboration Assurance Serviceability User Interface mandates DMA to perform again.

### What to do next

**Import Phone Status test After Upgrade**

These steps holds good only after a complete migration of 12.1.

1. Login to Cisco Prime Collaboration Assurance server as *root*.
2. Navigate to **/opt/emms/cuom/ImportFiles** and download **11.6_PhoneStatusImportFile.txt** file to local server.

3. Add respective Read community and Write community strings. For more information, see "/opt/emms/cuom/ImportFiles/PhoneStatusImportFile.txt".
4. Login to Cisco Prime Collaboration Assurance as *globaladmin*.
5. Navigate to **/Synthetic Tests/Phone Status Test** and import the Phone Status test from the file downloaded in Point 2.

**Note** After running the above commands, you are required to delete all the Phone Status test created in the Cisco Prime Collaboration Assurance 11.6 and re-create the Batch Test after the restore is successful.

**Enable CDR/CMR on CUCM** Perform the following steps after DMA Restore.

1. Go to **CUCM Serviceability** page of all managed CUCM publishers.
2. Navigate to **Tools** > **CDR Management**.
3. Select the **PCA IP address/Hostname**.
4. On the **Billing Application Server Parameters** section, check **Resend on Failure** check box and click **Update**.

# Troubleshooting

**Issue**: DMA restore fails.

**Conditions**: Following are the conditions:

- sFTP server is not reachable.
- Credentials do not match.

**Possible Solution**: Following are the logs for reference -

- /var/log/pcandma.log - Provides basic information of the Cisco Prime Collaboration Assurance and Analytics DMA.
- /var/log/dma_debug.log - Provides a complete debug messages of DMA.
- /var/log/assurance_restore_dma.log - Provides detailed information of Assurance restore DMA.
- /var/log/analytics_upgrade.log - Provides detailed information of Analytics upgrade.
- /var/log/dma_status.log - Provides status information of the success or failure of DMA.

# Credential Verification Error Messages for DMA Restore

Following are the conditions and possible solutions for test connection failure.

| Conditions | Possible Solutions |
|---|---|
| Invalid sFTP server IP address entered for restore in 12.1 server. | Enter an appropriate IPaddress. |

| Conditions | Possible Solutions |
|---|---|
| Invalid sFTP port number entered for restore in 12.1 server. | Enter an appropriate sFTP Port number. |
| Invalid sFTP server credentials entered for restore in 12.1 server. | Enter an appropriate sFTP server credentials. |
| Invalid sFTP server restore path entered for restore in 12.1 server. | Enter valid path and try restore again. |

# Validate Data Migration Assistant

Consider the following steps to validate DMA restore.

**Step 1** To verify if DMA is successful, then

**a.** Login as **Root**.

**b.** Check the status in **/var/log/dma_status.log**.

You can view the status information in the log file.

**Step 2** If DMA fails, then

**a.** Click on View DMA Status Detail link to understand the reason for failure and based on the details configure DMA accordingly.

**b.** Reenter the required sFTP configuration values on the DMA page. Click **Test Connection** to test the sFTP connection.

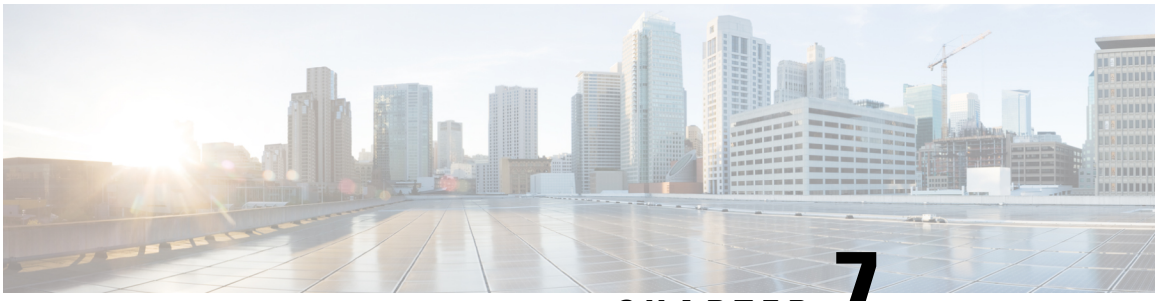
**c.** Click **Start DMA**.

During this process, a progress bar appears indicating the progress of data migration.

**Note**
- If DMA is successful, a success notification popup appears on the right side bottom of the screen.
- If you have missed to view the popup,
  1. Login to Root.
  2. Check for the "Success" or "Failure" status message in **/var/log/dma_status.log** file.

PART III

# Uninstall Cisco Prime Collaboration Assurance



CHAPTER 7

# Uninstall Cisco Prime Collaboration Assurance

This section explains the following:



## Uninstall Cisco Prime Collaboration Assurance

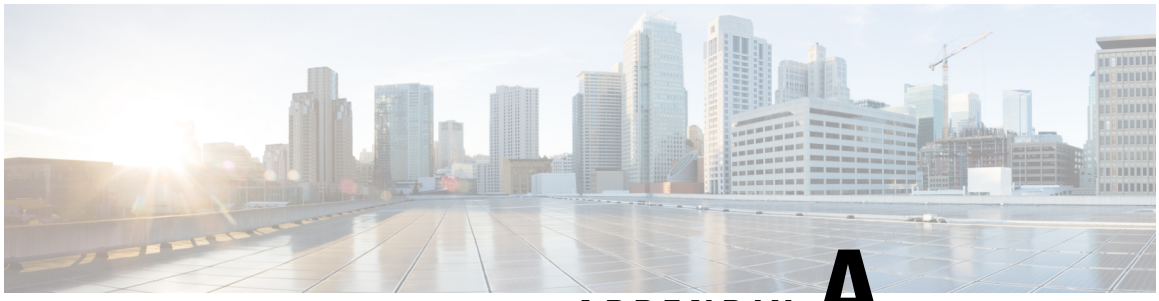
**Note** Before you uninstall, ensure that you delete all the node-to-node tests from the application. If you do not delete these tests, they continue to run on the Infrastructure.

**Step 1** Log in to the vSphere Client and connect to the ESXi server that is running the virtual appliance that you want to uninstall.

**Step 2** Right-click the application, choose **Power > Shut Down Guest** (or choose **Power Off**).

**Step 3** Right-click the application and in the **Confirm Delete** window, choose **Delete from disk**.

Uninstall Cisco Prime Collaboration Assurance



APPENDIX A

# Troubleshooting

This section explains the following:



## Verify the Cisco Prime Collaboration Assurance Installation (for Advanced Mode)

If you are unable to launch Cisco Prime Collaboration Assurance, it could be because the required processes are not running on the Cisco Prime Collaboration Assurance server.

To verify the process status, login to Cisco Prime Collaboration Assurance Serviceability User Interface.

You can view the Cisco Prime Collaboration Assurance processes that are running on the server. You can start or stop the processes apart from viewing the server.

**Note** You cannot start or stop an individual process. You can either Start or Stop all processes.

- **Start All Process** button appears only when all processes are stopped.
- **Stop All Process** button appears when all/some processes are running.
- A notification also appears once the processes are started or stopped.
- You can click on View Process Status Detail link to view the progress of starting / stopping the processes. The View Process Status Detail link appears only when the processes is being started or stopped.

**Note** The process status dashboard automatically refreshes every 6 seconds.

# Downgrade the Cisco Prime Collaboration Deployment Model

Cisco Prime Collaboration does not support the downgrade of the deployment model; that is, you cannot downgrade from the Cisco Prime Collaboration large deployment model to the small deployment model.

# Change the IP Address on the Cisco Prime Collaboration Assurance Server

The **Update System Parameters** menu in Cisco Prime Collaboration Assurance Serviceability User Interface allows you to update the system parameters. It has the provision of either entering or changing the IP address and Time Zone. System Parameters menu refers to a specific system setting. For steps to update system parameters, see Cisco Prime Collaboration Assurance Serviceability User Guide.

# Find the MAC Address of Cisco Prime Collaboration Assurance Servers

To find the MAC address of Cisco Prime Collaboration Assurance

**Step 1** Click the About icon at the top right corner of the user interface.

**Step 2** On the **About** page, click the Assurance Information link to launch the system information details for Cisco Prime Collaboration Assurance.

For all the other versions of Cisco Prime Collaboration, you can check the MAC address through the vSphere Client.

# How to avoid File Not Found error during Upgrade, Restore, and Patch Installation through SFTP?

When you upgrade, restore and patch install through SFTP, copy the image to both root location and show repository output location of SFTP server to avoid **File Not Found** error.

# Remove the SSL Certificate Warning

- Windows Internet Explorer—You can permanently remove the SSL certificate warning by installing the Cisco Prime Collaboration self-signed certificate.
- Mozilla Firefox—You can remove the SSL certificate warning only by adding an exception.

- Google Chrome—You can remove the SSL certificate warning by using the Manage Certificates option under HTTPS/SSL on the Settings page.

# Remove the SSL Certificate Warning in Internet Explorer

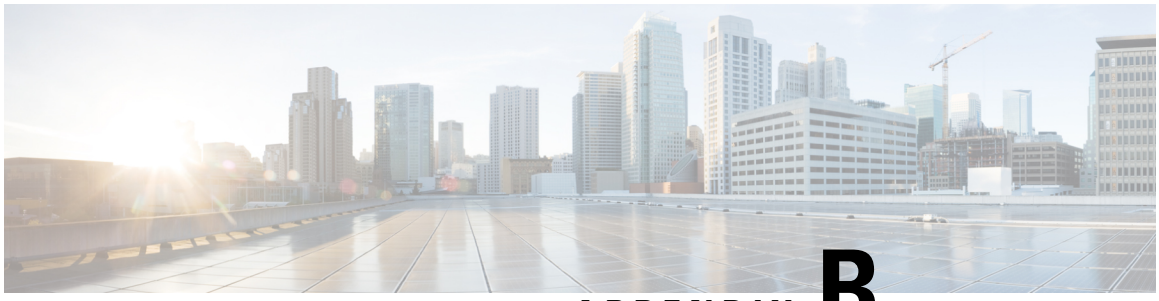
**Step 1** Choose **Continue to this website (not recommended)**.
**Step 2** Choose **Tools** > **Internet Options**.
**Step 3** In the **Internet Options** dialog box, click the **Security** tab, choose **Trusted sites**, and then click **Sites**.
**Step 4** Confirm that the URL that appears in the field and matches the application URL, and then click **Add**.
**Step 5** Close all dialog boxes and refresh the browser.
**Step 6** Choose **Certificate Error** to the right of the address bar, and then click **View certificates**.
**Step 7** In the **Certificate** dialog box, click **Install Certificate**.
**Step 8** In the **Certificate Import Wizard** dialog box, click Next.
**Step 9** Click the **Place all certificates in the following store** radio button, and then click **Browse**.
**Step 10** In the **Select Certificate Store** dialog box, choose **Trusted Root Certification Authorities**, and then click **OK**.
**Step 11** Choose **Next** > **Finish**.
**Step 12** In the **Security Warning** message box, click **Yes**.
**Step 13** In the **Certificate Import Wizard** message box, click **OK**.
**Step 14** In the **Certificate** dialog box, click **OK**.
**Step 15** Repeat Step 2 and Step 3.
**Step 16** Select the URL in the **Websites** section, and then click **Remove**.

# Do You Have a Safe URL Implemented

**Step 1** Choose **Tools** > **Internet Options** .
**Step 2** In the **Internet Options** dialog box, click the **Advanced** tab .
**Step 3** In the **Security** section, uncheck the **Warn about certificate address mismatch** check box.

# Remove the SSL Certificate Warning in Mozilla Firefox

**Step 1** Click **I Understand the Risks** >**Add Exception**.
**Step 2** In the **Add Security Exception** dialog box, click **Confirm Security Exception**.



APPENDIX B

# Frequently Asked Questions

This section explains the following:



# Frequently Asked Questions

**Unified Communications Operations Dashboard**

1. Do all the Responders registered with the Master need to be on Cisco Prime Collaboration Assurance 12.1 version?

   Responders registered with the Master have to be on Cisco Prime Collaboration Assurance 12.1 version.

2. Can the Responders be still accessible using GUI or CLI?

   The Responders cannot be accessed through either GUI or CLI.

**This section is NOT applicable for 12.1 Service Pack 3 and later releases.**

**Migrate Cisco Prime Collaboration Assurance Using Data Migration Assistant Tool**

1. What is the purpose of the script **./pcandma.sh**?

   **Purpose of the script:** The script initiates the DMA backup. This script does not generate any intermediate file that can be used for upgrade.

2. What kind of file will be generated?

   The final backup file .tar.gz is generated in the sFTP server.

3. How do you use the .tar.gz file to upgrade to 12.1?

   During restore, you have to provide the same sFTP server details where the backup is available.

4. How to Turn OFF FIPS mode?

   To take a backup from Cisco Prime Collaboration Assurance 11.x server, go to **System Administration** > **FIPS Setup**. Then, uncheck **FIPS Compliance** check box and click **Apply**. The system reboots.

5. During the launch of Cisco Prime Collaboration Assurance, is the password the GUI password or the CLI password? Provide details on how to change it?

   This is the GUI password. During first invocation, it prompts you to change the default password.

**This section is NOT applicable for 12.1 Service Pack 3 and later releases.**

**Perform Data Migration Assistant Using Interview Wizard**

1. What is an Interview Wizard? How to access it?

   When you deploy Cisco Prime Collaboration Assurance 12.1, you have several installation prompts. You have to enter the required details for setting up the server. This way you will be able to access the Interview Wizard. An Interview Wizard is basically a form that allows you to enter the required details.

2. How to regenerate the license files?

   Licenses are generated through the License Generation Tool.

3. How do you transfer the file generated using DMA to the new version of Cisco Prime Collaboration Assurance 12.1?

   During restore, you must specify the location of sFTP server, where the backup file .tar.gz of Cisco Prime Collaboration Assurance 11.x is saved. The file will be picked as part of the automated process. During the installation of Cisco Prime Collaboration Assurance 12.1, in the Interview Wizard, specify 1 in DMA Upgrade Option to transfer the file generated using DMA.