Installation and Upgrade Guide for Cisco Unified Intelligence Center, Release 12.6(2)

First Published: 2023-04-28

Last Modified: 2023-04-28

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

Preface

Change History

This table lists the changes that are made to this guide. Most recent changes appear at the top.

Change	See	Date
Initial Release of Document for Release 12.6(2)		April 2023
Updated references for 12.6(1) to 12.6(2)	Chapter: Preparation for Unified Intelligence Center and Upgrades.	

About This Guide

This guide explains how to install and upgrade Unified Intelligence Center.

Audience

This guide is prepared for partners, specialists, and system administrators who are responsible for the installation of Unified Intelligence Center.

Note This document might not represent the latest Cisco product information available. Obtain the most current documentation at this URL: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/tsd-products-support-series-home.html.

Related Documentation

This section presents information about product components that are deployed with Unified Intelligence Center.

Cisco Unified Contact Center Express

For Unified CCX documentation, see:
https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series-home.html.

Cisco Packaged Contact Center Enterprise

For Cisco Packaged Contact Center Enterprise documentation, see:
https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html.

Cisco Finesse

For Finesse documentation, see:
https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/tsd-products-support-series-home.html.

Cisco Unified Contact Center Enterprise

For Unified CCE documentation, see:
https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/tsd-products-support-series-home.html.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

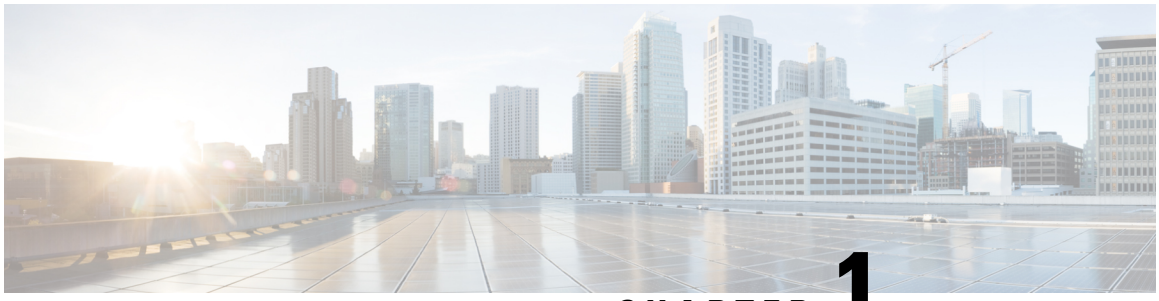
Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

You can provide comments about this document by sending an email to the following address:

contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.



CHAPTER 1

Before You Install

About Cisco Unified Intelligence Center

Unified Intelligence Center can be installed as a standalone server or as a cluster of a maximum of eight server nodes. There is one mandatory publisher node (called the *Controller*) and a maximum of seven subscriber nodes (called *Members*). The Controller node includes a Member; thus a deployment can consist of a Controller only.

All nodes must meet latency requirements as described in the *Cisco Unified Intelligence Center Solution Reference Network Design (SRND) Guide*.

The primary node (the *Controller*) includes both the Administration (Operations, Administration, Maintenance, and Provisioning or OAMP) and the Unified Intelligence Center Reporting web applications. A Controller is required in all deployments. A deployment can consist of a Controller only.

The Member nodes have the Unified Intelligence Center Reporting web application only.

Unified Intelligence Center is installed on Cisco Unified Voice Operating System (VOS). This is an appliance model or "closed box" and does not support navigation into, or manipulation of, the file system.

Unified Intelligence Center must be installed on a Virtual Machine running over UCS B-Series and C-Series Servers or equivalent hardware.

The disk capacity and hardware type of Member nodes should be equal to or greater than those of the Controller node.

For Cisco Unified Intelligence Center Hardware and Software Specification, refer *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html and *Compatibility Matrix for Unified CCX* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

See the *Cisco Unified Intelligence Center Solution Reference Network Design (SRND) Guide*, available in the Design Guides category at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/tsd-products-support-series-home.html.

Prerequisites and Important Considerations

Before you proceed with the installation and upgrade, note these important requirements:

- You must have access to a Network Time Protocol (NTP) server.
- You must have a preconfigured default router.
- You must have a preconfigured Domain Name Server (DNS).
- You must install the primary node (the Controller).
- All configured nodes in a cluster must be installed and started before you install a new node. For example, if the Controller and one Member have been installed and you are about to add a second Member, the Controller and first Member must be started and available so that the second Member is able to access them.
- Installation on an existing (repurposed) server formats the hard drive and erases all data. It might also change the system Basic Input Output System (BIOS), firmware, and Redundant Array of Inexpensive Disks (RAID) configuration.
- On the installation configuration screens:
  - Values—such as host names, User IDs, and passwords—are case-sensitive.
  - You must enter the same security password on all nodes in the cluster. Keep a record of this password; you will need to use it if you replace or add a server in the future or if you want to replace the old security password with a new one.
  - Use the default Maximum Transmission Unit (MTU) setting, for all nodes in the cluster.

Configuration Worksheet

Use this worksheet to record network and password information that the basic installation configuration wizard prompts you to enter. Store this worksheet information for future reference.

Table 2: Configuration Worksheet

Configuration Data	Your Entry
Host Name	Controller
	Member 1
	Member 2
IP Address	Controller
	Member
Gateway (GW) Address	—

Configuration Data	Your Entry
Primary DNS IP Address	Controller
	Member
Secondary DNS IP Address	Controller
	Member
Domain	—
Username	—
	Note Ensure that you use the same System Administrator credentials for all nodes.
System Administrator Password	—
Timezone Use the same Timezone for all nodes.	—
Certificate Information	Organization
	Unit
	Location
	State
	Country
NTP Server Host Name or IP Address	NTP Server 1
	NTP Server 2
	NTP Server 3
	NTP Server 4
	NTP Server 5
Database Access Security Password	Security Password
	Servers in the cluster use the security password to communicate with one another. The security password is also used by the Disaster Recovery System (DRS) for encryption of the backup file. **Note** You must enter the same security password for all servers in the cluster.
Simple Mail Transfer Protocol (SMTP) Location Host Name	SMTP Host Name or IP Address

Configuration Data	Your Entry
Credentials	Application User ID
	Application User Password
	The Application User defined during the Controller installation is the only credential recognized by Unified Intelligence Center. **Note** Ensure that you use the same System Application credentials for all nodes.

Installation Sequence and Time

A Unified Intelligence Center can include one or multiple nodes. The installation for each node can take about an hour. For most of that time, it can run unattended.

You must perform the installation on the primary node/Controller first.

Some configuration and installation processes differ slightly for the first node (Controller) and for the Members. This is noted in these instructions.

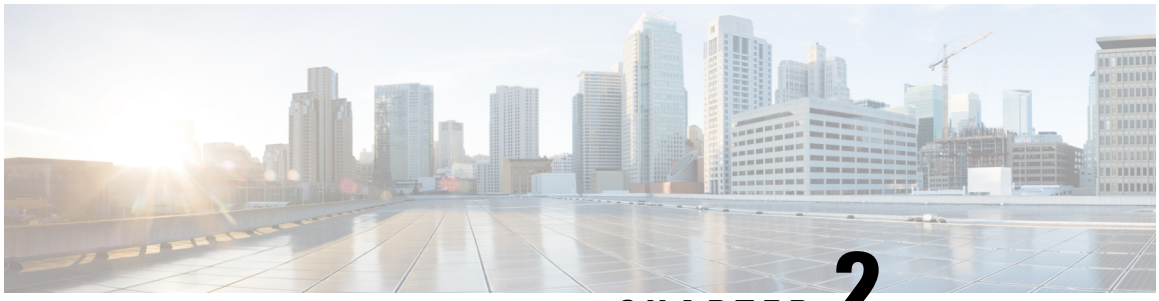
Installation Wizard Navigation

Much of the installation requires no action on the part of the person who runs it. When user input *is* required, use the following *keyboard* navigation and selection actions.

The installation wizard screens do not recognize a mouse or a touchpad.

Table 3: Installation Wizard Navigation

To Do This	Press This Key
Move to the next field	Tab
Move to the previous field	Alt-Tab
Choose an option	Spacebar
Scroll up or down a list	Up or Down arrow keys
Go to the previous screen	Tab to Back and press the Spacebar
Get information on a screen	Tab to Help and press the Spacebar
Scroll up and down a list	Up or Down arrow keys



CHAPTER 2

Preparation for Unified Intelligence Center

You can perform a fresh installation or upgrade of Unified Intelligence Center on supported virtual machines. Also, you can perform an upgrade from previous versions to 12.6(2). For base versions prior to 12.0(1), you should upgrade Unified Intelligence Center to 12.0(1) first and then to 12.6(2). For more information, see *About Upgrades*.

Install VMware ESXi

Before you begin your Unified Intelligence Center installation, you must install VMware ESXi and configure the virtual server.

Step 1 Refer to Unified Communication Virtualization at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-intelligence-center.html to install, setup, and configure the UCS Hardware.

Step 2 Configure the UCS Network. See UCS Network Configuration at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html for more information.

Step 3 Use the instructions mentioned in the https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-intelligence-center.html to install VMWare ESXi 6.5 and 6.7 (with VMFSv6) on your **UCS B-series and C-series** server.

Step 4 After ESXi is installed successfully, reboot the server.

Deploy Unified Intelligence Center Open Virtualization Format/Open Virtual Appliance (OVF/OVA) Template

Open Virtualization Format/Open Virtual Appliance (OVF/OVA) is an open standard for packaging and distributing virtual appliances. Files in this format have an extension of .ova. The naming convention for the OVF/OVA template is `PRODUCT_COMPONENT_USER COUNT_VERSION_VMVER.ova`.

The OVF/OVA template defines the configuration of the virtual machine hardware. The configuration of a Cisco Unified Communications application virtual machine must match a supported virtual machine template. This section describes the steps to deploy a Unified Intelligence Center OVF/OVA template on the virtual machine.

Step 1 Log in to **ESXi** using *VMWare Vsphere* or any other compatible client.

Step 2 Highlight the host or cluster to which you want to deploy the Virtual Machine.

Step 3 Select **File** > **Deploy OVF/OVA Template**.

Step 4 Click **Deploy from File/Template** and specify the name and location of the OVF/OVA file (with a *.ova* extension)

Alternatively, you can click **Deploy from URL** and specify the URL of the OVF/OVA file.

Step 5 Click **Next**.

Step 6 Verify the details of the template, and click **Next**.

Step 7 Specify a name for the **Virtual Machine** that you are about to create and choose an inventory location on your host.

Step 8 Click **Next**.

Step 9 Choose the **Deployment Configuration Type** from the drop-down.

a) **Co-Resident**: To deploy options with CUIC, LD and IdS.
b) **Stand-Alone**: To deploy option with CUIC only.

Step 10 Click **Next**.

Step 11 In Disk Format, click **Next** .

Step 12 Verify the deployment settings, and click **Finish**.

The virtual machine that you added is listed under the UCS server tree in the **vSphere Client** home page.

Specify Location of Unified Intelligence Center Installable

Step 1 Select the newly added Virtual Machine.

Step 2 From the **Inventory** menu, select **Virtual Machine** > **Edit Settings**.

Step 3 In the **Hardware** tab, select **CD/DVD Drive 1**.

Step 4 Select one of the following options to specify the location where you have the bootable Unified Intelligence Center installer file:

a) **Client Device** – If you want to use the CD/DVD drive on the client machine from where you are accessing the virtual machine remotely.
b) **Host Device** – If you want to use the CD/DVD drive on the ESXi host machine.
c) **Datastore ISO file** – If you want to use the datastore on the virtual machine. Before using this option, ensure that the Bootable iso image of Unified Intelligence Center is copied to the datastore of the ESXi host.

Note Ensure that you set the boot order by making **CD ROM** the first device upon power up. For details, refer to Set Boot Order, on page 7.

Step 5 Click **OK** to save and close the **Virtual Machine Properties** window.

Important: Make sure that you have copied or inserted the CD/DVD with the Unified Intelligence Center installable in the appropriate location before you proceed with the next step.

Related Topics

Set Boot Order, on page 7

Set Boot Order

To set the boot order:

Step 1 From the **Inventory** menu, select **Virtual Machine** > **Edit Settings**.

The Virtual Machine Properties window appears.

Step 2 In the **Options** tab, select **Boot Options**.

Step 3 Select **Force BIOS Setup**.

Note When you restart the Virtual Machine, you will see the BIOS screen in the **VM console** tab.

Step 4 In the **BIOS** screen, select **Boot Options** > **make the CD/DVD ROM as the first device for bootup**.

Step 5 Click **Save**.

Install Cisco Unified Intelligence Center on Virtual Machine

Step 1 Select the virtual machine and click **Power** > **Power On** from the shortcut menu. Alternatively, from the **Inventory** menu, select **Power** > **Power On**.

Step 2 The virtual machine powers on and Unified Intelligence Center installation starts up automatically. Follow the steps mentioned in Installation — All Nodes, on page 9 to complete the Unified Intelligence Center installation.

When using Unified Intelligence Center on the UCS Servers, note the following:

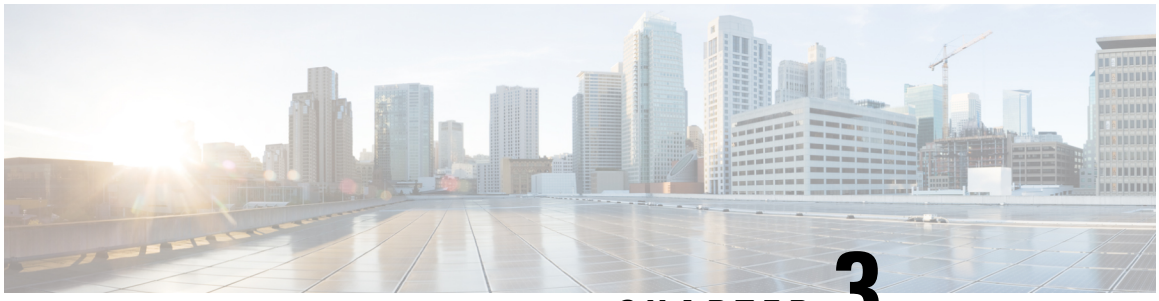
- The answer file generated by the Answer File Generator (platformConfig.xml) is not readable from a USB key. The Answer File Generator generates a floppy image [FLP - virtual floppy] for performing an unattended installation.
- USB tape backup is not supported. Use SFTP instead.

- Install logs are written only to the virtual serial port.
- Unattended installs use virtual floppy instead of USB.
- Boot order is controlled by the BIOS of the VMware VM.
- Hardware BIOS, firmware, and drivers must be the required level and configured for compatibility with Unified Intelligence Center-supported VMware product and version.

Note vSphere provides you with a console that you can use to provide inputs during the installation. To open the console, select the virtual machine from the vSphere home page and click **Open Console** from the shortcut menu. Alternatively, select the virtual machine and click the **Console** tab in the right pane of the **vSphere** home page. Pointing and clicking anywhere in the console window will allow you to enter data in the console. Once you start working on the console, the mouse is locked and you can no longer use it. Use **Tab** key to navigate and use the **Enter** button to commit the values you entered. To release the mouse from the console window, press **Ctrl + Alt**.

Related Topics

Installation Media, on page 9
Before You Begin, on page 9
Enter Pre-Existing Configuration Information, on page 11
Configure Basic Install, on page 11
Post-Install Configuration , on page 13



CHAPTER 3

Installation — All Nodes

Installation Media

The installation for Unified Intelligence Center is delivered on DVD media. Run the DVD installation on each node, and use the same DVD for all nodes.

Note All nodes must be running the same version of Cisco Unified Intelligence Center.

Before You Begin

Every installation begins with an optional pre-install media check, which includes a hardware check. You then make your product deployment selection before continuing to the basic install configuration.

Step 1 Mount ISO to the virtual DVD drive. Then restart or power on the server so that it boots from the DVD.

You see messages as the pre-install script runs. When the pre-install script ends, the **DVD Found** screen opens.

Step 2 In the **DVD Found** screen, you have the option to perform a media check to verify the integrity of the DVD.

If you want to check the media:

a. Select **Yes** to begin the verification of the media integrity.

Note The media check can take up to an hour. If the media check for the Controller passes, you can safely skip the media check when you install the Members.

b. If the media check passes, select **OK**. The **Product Deployment Selection** screen appears, and you can continue to Step 3.

If the media check fails, the DVD is ejected and the installation terminates. Contact your support provider for assistance.

If you want to skip the media check:

a. Select **No**. The **Product Deployment Selection** appears.

b. Proceed to Step 3.

Step 3 Choose one of the following options:

- **Cisco Unified Intelligence Center**
- **Live Data**
- **Cisco Identity Service (IdS)**
- **Cisco Unified Intelligence Center with Live Data and IdS**

Note
- For the 2000 agent reference design, choose the co-resident deployment option **Cisco Unified Intelligence Center** with **Live Data** and **IdS**; and then select **OK**. The **Cisco Unified Intelligence Center**, **Live Data**, and **IdS** option installs **Cisco Unified Intelligence Center**, **Live Data** and **Cisco Identity Service (IdS)** on the same server.
- For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center, Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

Step 4 Click **OK** to initiate a hard drive check, during which the installation checks for a supported hardware platform with the correct number of disks.

A successful hardware check opens the **Proceed with Install** screen. The **Proceed with Install** screen shows the version of the product that is currently on the hard drive (if any) and the version of the product that is on the DVD. For the initial installation, the version on the hard drive shows NONE.

Note If the server hardware is unsupported, a message appears indicating that the installation cannot proceed, and the installation halts. If you require assistance understanding the message, write it down to facilitate your conversation with your support provider. See *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for details on supported hardware.

Step 5 Select **Yes** on the **Proceed with Install** screen.
The **Platform Installation Wizard** screen appears.

Step 6 In the **Platform Installation Wizard** screen, select **Proceed** to open the **Apply Patch** screen.

Step 7 Select **No** at the **Apply Patch** screen. Do not apply patches from the Installation wizard. See *About Upgrades* for instructions on upgrading Unified Intelligence Center software with Engineering Specials, Minor Releases, and Maintenance Releases.

Your selection of **No** opens the **Basic Install** screen.

If you select **Yes** by mistake and open the **Apply Patch** screen, select **Back**. Then choose one of the following options:

- To enter your configuration information manually and have the installation program install the configured software on the server, choose **Proceed** and continue with this procedure.
- To do any of the following tasks, choose **Skip**; then continue with the *Entering Preexisting Configuration Information* procedure:

- Manually configure the software that is preinstalled on your server — In this case you do not need to install the software, but you must configure the preinstalled software.
- Perform an unattended installation — In this case, you provide preexisting configuration information on a USB key or floppy disk.
- Install the software before manually configuring it — In this case the installation program installs the software, then prompts you to configure it manually. You can choose **Skip** if you want to preinstall the application on all your servers first and then enter information at a later time. This method might cause you to spend more time performing the installation than the other methods.

Step 8 Select **Continue** at the **Basic Install** screen to enter the configuration screens.

Related Topics

Before You Upgrade, on page 29
Enter Pre-Existing Configuration Information, on page 11

Enter Pre-Existing Configuration Information

Start here if you have a server that has the product pre-installed or if you chose **Skip** in the Platform Installation Wizard window.

Step 1 After the system restarts, the Pre-existing Installation Configuration window displays.

Step 2 If you have pre existing configuration information (Created by Answer File Generator) in a floppy disc or a USB key, insert the disc or the USB key now and choose **Continue**. The installation wizard will read the configuration information during the installation process.

Note If a popup window states that the system detected new hardware, press any key and then choose Install from the next window.

The Platform Installation Wizard window displays.

Step 3 To continue with the Platform Installation Wizard, choose **Proceed**.

Step 4 In the Basic Install window, choose **Continue**. Continue with the "Configure basic install" section.

Configure Basic Install

The basic install launches a series of screens that present questions and options pertinent to the platform and the setup configuration. There is online help for each wizard screen.

Note You can change many of the basic installation configuration settings after the installation using the Set commands in the Command Line Interface (CLI). The CLI is documented in the *Administration Console User Guide for Cisco Unified Intelligence Center*.

The first Basic Install wizard screen is Timezone Configuration.

Step 1 In the **Timezone Configuration** screen:

a) Use the down arrow to select the local timezone that most closely matches where your server is located. You can also type the initial character of the timezone to move to that item in the list. The timezone field is based on country/city and is mandatory. Setting it incorrectly can affect system operation.

Note Use the same timezone for all nodes.

b) Select **OK** to open the Auto Negotiation Configuration screen.

Step 2 In the **Auto Negotiation Configuration** screen, select whether or not you want to use automatic negotiation for the settings of the Ethernet network interface card (NIC).

If	Then
You want to disable auto-negotiation and specify NIC speed and duplex settings.	Select **No** to open the NIC Speed and Duplex Configuration screen, where you can manually configure the settings. Proceed to Step 3.
The ethernet network interface card (NIC) attached to your hub or Ethernet switch supports automatic negotiation.	Select **Yes** to open the MTU Configuration screen. Proceed to Step 4.

Step 3 In the **NIC Speed and Duplex Configuration** screen, configure settings as follows:

a) Specify the speed of the Network Interface (NIC) card in megabits per second. Speed options are **10** or **100**.
b) Specify the duplex setting of the server NIC. Options are **Full** or **Half**.
c) Select **OK** to open the MTU Configuration screen.

Step 4 In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units (1500). If you do not accept the default and configure the MTU size incorrectly, your network performance can be affected.

Your selection of No opens the DHCP Configuration screen.

Step 5 In the **DHCP Configuration** screen, select **No** to open the Static Network Configuration screen.

Step 6 At the **Static Network Configuration** screen, enter static network configuration values as follows, referring to the *Configuration Worksheet* if necessary:

a) Enter the **Host Name**.
b) Enter the **IP Address**.
c) Enter the **IP Mask**.
d) Enter the **GW Address**,
e) Select **OK** to open the **Domain Name System (DNS) Client Configuration** screen.

Step 7 Select **Yes** to enable the Domain Name System (DNS) Client.

Step 8 Enter your DNS client information as follows:

a) *Configuration Worksheet* Enter the **Primary DNS** (mandatory).
b) Enter the **Secondary DNS** (optional).
c) Enter the **Domain** (mandatory).
d) Select **OK** to open the Administrator Login Configuration screen.

Step 9 In the **Administrator Login Configuration** screen:

a) Enter the ID for the System Administrator.
b) Enter and then confirm the password for the administrator.
c) Select **OK** to open the Certificate Information screen.

Step 10 In the **Certificate Information** screen:

a) Enter data to create your Certificate Signing Request—Organization, Unit, Location, State, and Country.
b) Select **OK** to open the First Node Configuration screen. ("Is this server the First Node in the cluster?")

Step 11 In the **First Node Configuration** screen, specify whether you are configuring the first node (the Controller).

If	Then
You are installing and configuring the primary node (the Controller).	Select **Yes** to open the Network Time Protocol Client Configuration screen. Continue to *Controller Configuration.*
You are installing and configuring a secondary node (a Unified Intelligence Center Member).	Select **No** to open the First Node Configuration Warning screen. Continue to *Complete Configuration for Member Node* .

Post-Install Configuration

If Live data is supported and installed in the customer deployment, you must also perform some Live Data configuration tasks. Refer chapter 4 on *Live Data Installation* in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Cross-Origin Resource Sharing (CORS)

For Unified Intelligence Centre gadgets (Live Data and Historical) to load in Cisco Finesse, ensure to run the following commands in the Unified Intelligence Center server:

- Enable CORS using the `utils cuic cors enable` command.
- Set the Finesse host URL in the `utils cuic cors allowed_origin add URLs` command.

  Examples:

  - https://<finesse-FQDN>
  - https://<finesse-FQDN>:port

For Live Data gadgets, in addition to the above settings, ensure to enable CORS using the `utils live-data cors enable` command and set the Finesse host URL in the `utils live-data cors allowed_origin add` URLs command. If Live Data is coresident to Unified Intelligence Center, then run these Live Data commands on the same Unified Intelligence Center system; Otherwise, run on the standalone Live Data system.

For more information, see *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

Self-Signed Certificates

Note Follow the below steps, if you are using self-signed certificates.

Prerequisite—Download the Unified Intelligence Center tomcat certificate from Cisco Unified OS Administration page of Unified Intelligence Center.

Perform the following tasks to upload the Unified Intelligence Center server certificate to Cisco Finesse.

1. Sign in to Cisco Unified OS Administration on Cisco Finesse using the following URL: `https://FQDN of Finesse server:8443/cmplatform`.
2. Select **Security** > **Certificate Management** > **Upload Certificate/Certificate chain**.
3. From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
4. In the **Upload File** field, click **Choose File** and browse to the tomcat.pem file that you saved on your system.
5. Click **Upload**.
6. Restart the Cisco Finesse Tomcat on the Cisco Finesse server.

Note
- Follow the same steps for both the Cisco Finesse publisher and subscriber nodes.
- If there is a standalone Live Data system in this deployment, then upload Live Data tomcat certificate in addition to Cisco Finesse, using the above-stated procedure.

For more information, see the *Certificates for Live Data* chapter in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Hazelcast Cluster Configuration

Note Follow the below steps, if your network does not support multicasting, and when the Unified Intelligence Center administrator sign-in page displays a banner message about the application cluster issues.

Perform the following tasks change the discovery mechanism to `tcp-ip` mode.

1. Log in to the Cisco Unified Intelligence Center CLI. Specify the System Administrator username and password.

Note Run the following CLIs on all nodes in the given sequence, starting from the publisher node.

2. Enter the command **utils service stop** *Intelligence Center Reporting Service*.
3. Enter the command **utils cuic cluster mode**.

4. Select cluster mode **2) Enable tcp-ip**.
5. Enter the command **utils cuic cluster show**.

Note Ensure that all nodes have an identical configuration.

6. Enter the command **utils service start** Intelligence Center Reporting Service.

Note If there happens to be a disconnect and reconnect, check that the database replication is successfully set up across all nodes in the cluster. Perform "Synchronize Cluster" from Cisco Unified Intelligence Center to ensure that cache is in sync across the cluster.

For more information, see the *Cluster Configuration for JVM Using Hazelcast* section in *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

Cisco Unified Intelligence Center Answer File Generator

Unified Intelligence Center Answer File Generator, a web application, generates answer files for unattended Unified Intelligence Center installations. Individual answer files get copied to the root directory of a USB key or a floppy diskette and are used in addition to the Unified Intelligence Center DVD during the installation process.

The web application supports the following features:

- Allows simultaneous generation and saving of answer files for unattended installs on the publisher server and all subscriber servers.
- Provides syntactical validation of data entries.
- Provides online help and documentation.

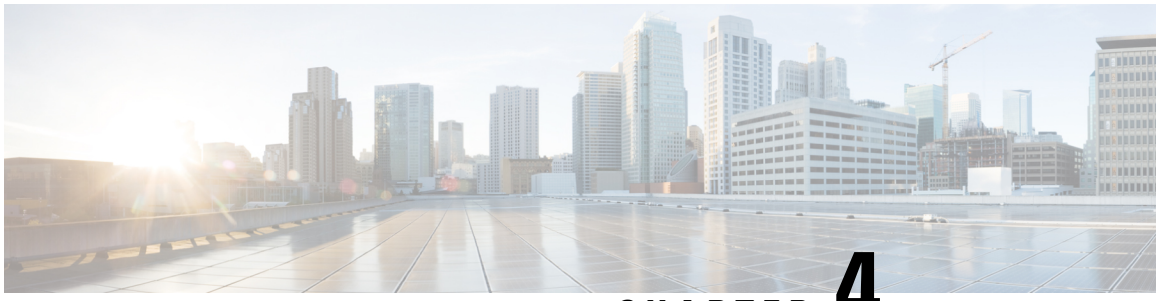
The following usage requirements apply:

- The web application supports only fresh installs and does not support upgrades.
- If DHCP client is being used on the publisher server, and subscriber server answer files are also being generated, you must specify the publisher server IP address.

You can access the Cisco Unified Communications Answer File Generator at the following URL:

https://www.cisco.com/c/en/us/applicat/content/cuc-afg/index.html

Note Cisco requires that you use USB keys that are compatible with Linux 2.6.32 You should use USB keys that are preformatted to be compatible with Linux 2.6.32 for the configuration file. These keys will have a W95 FAT32 format.



CHAPTER 4

Controller Configuration

Complete Configuration for First Node

When you complete the basic install configuration and select **Yes** to indicate that you are installing the first node, perform the following steps to complete the configuration for the Controller.

The first screen you see is the **Network Time Protocol Client Configuration** screen.

This screen gives the option of setting the time for the first node (the Controller) from a time that you set on the Hardware Clock screen - or - from an external Network Time Protocol server that you define.

Note NTP server configuration is mandatory and is set for the first node. Other nodes set their time to the time on the first node.

Step 1 Select **Yes** at the **Network Time Protocol Client Configuration** screen.

The **Network Time Protocol Client Configuration** screen opens.

Step 2 Enter the IP address, NTP server name, or NTP Server Pool name for at least one external NTP server.

You can add up to five NTP servers and make changes to the NTP server list at a later time.

Note You should use a minimum of three external NTP servers.

Step 3 When you complete the NTP configuration, select **OK**.

The Security Configuration screen opens.

Step 4 In the **Security Configuration** screen:

a) Enter the Database Access Security password. This is the password that servers in the cluster use to communicate with each another. *You must enter the same security password for all servers.*

b) Select **OK** to open the SMTP Host Configuration screen.

Step 5 In the **SMTP Host Configuration** screen, select whether you want to configure an SMTP host to receive platform-level emails, for example, emails about certificate expiration. This field is optional. You will configure email for report scheduling in the Administration console.

Note The Unified Intelligence Center email client does not support SSL/TLS based SMTP servers to email the scheduled Unified Intelligence Center reports.

If	Then
You want to configure an SMTP Host.	Select **Yes** to open the second SMTP screen opens. Proceed to Step 6.
You do not want to configure an SMTP Host.	Select **No** to open the Application User Configuration screen. Proceed to Step 7.

Step 6 In the second **SMTP Host Configuration** screen:

a) Enter the hostname or IP address for the SMTP server.
b) Select **OK** to open the Application User Configuration screen.

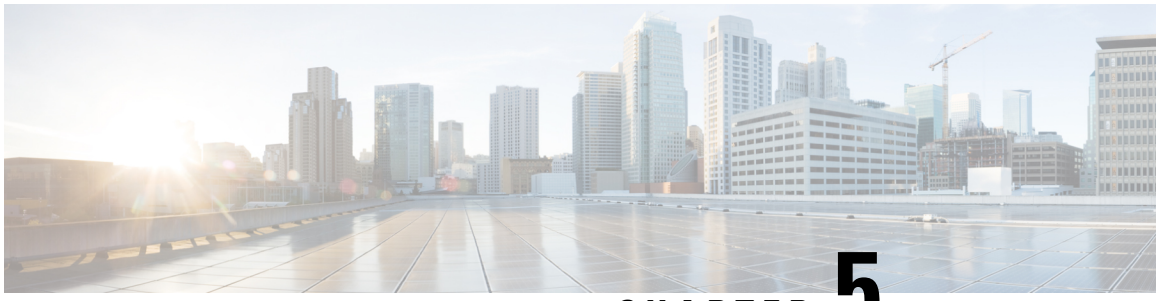
Step 7 Complete the **Application User Configuration** screen. The application user for the Controller becomes the System Application User and the default Super User.

Note Although it is possible to enter unique Application User credentials on each installed node, you should enter the *same* Application User Name and password on all nodes. The Application User credentials entered during the Controller installation are the only ones recognized by Unified CCE.

a) Enter the application username.
b) Enter and confirm the application user password.
c) Select **OK** to open the Platform Configuration Confirmation screen. This screen states that the platform configuration is complete.

Step 8 In the **Platform Configuration Confirmation** screen, select **OK**.
The installation begins. The system displays a Virtual Machine Question message about a locked CD-ROM door.

Step 9 In the **Virtual Machine Question** message, click **Yes** and click **OK** to continue the installation.
The system displays a reboot message. After the reboot, the system automatically proceeds with the installation.



CHAPTER 5

Installation

Installation Duration

The installation can take from 60 to 75 minutes to complete and can run unattended for most of that time.

Installation Processes

During the installation, the monitor shows a series of processes, as follows:

- Formatting Progress Bars
- Copying File Progress Bar
- Platform Installation Progress Bars (as multiple packages are installed)
- Post Install Progress Bar
- Application Installation Progress Bars (multiple packages are backed up to the archive directory)
- An informational screen saying that the system reboots.

Note At the start of the reboot, the CD tray holding the DVD ejects. This is usual behavior. You can remove the DVD.

- A System Reboot, which includes a second hardware check.

  Messages appear during the reboot, some of which prompt you to press a key. Do not respond to these prompts to press a key.

- Application Pre Install Progress Bars
- Configure and Setup Network Progress Bars

Note If a Network Connectivity Failure screen opens during the Configure and Setup Network process, click **Review**. Then click **OK** at the Errors screen. Follow the prompts to reenter your hostname, IP Address, and so forth. The installation continues when the connection information is complete.

- Member Nodes only - Connection Validation message.
- Security Configuration
- Member Nodes only - A screen stating that there is a successful connection to the first node (select **Continue**).
- The SMTP Host Configuration screen(s). Select **Yes** or **No**, according to your preference.
- Platform Configuration Complete screen. Select **OK**.
- Display of Cryptographic Information screen.
- Application Post-Install Progress Bars

The installation ends at a login prompt, at which you can enter CLI commands.

To access the web interface, you need to open a browser and enter the URL *https://Controller hostname or IP/oamp* and User ID/Password of the System Application user.

Related Topics

Frequently Asked Questions

Installation Failure

Mount ISO to the virtual DVD drive and perform all steps in Chapter 2, and proceed to *Configure Basic Install*.

If a critical error occurs during installation, you are prompted to collect log files. To do this, insert a USB memory key in any available USB port and follow the instructions on the screen.

If the installation fails over a Virtual Machine. For more information, see *Frequently asked Questions*.

Related Topics

Configure Basic Install, on page 11
Frequently Asked Questions

Post Installation

The action to take after the installation, depends on the type of node you installed.

Note After installing the Unified Intelligence Center, you can download the Unified CCE templates from the Download Software page at https://software.cisco.com/download/home/282163829/type. You can then import these templates to Unified Intelligence Center.

Note After installing Cisco Unified Intelligence Center release 11.6, ensure to perform the following actions:

1. Disable the Unified CCE User Integration. (Uncheck the **Enable UCCE User Integration** check box in **OAMP** > **Cluster Configuration** > **UCCE User Integration**
2. Install the latest Cisco Options Package (COP) file for Unified Intelligence Center 11.6 release.
3. Enable the Unified CCE User Integration.

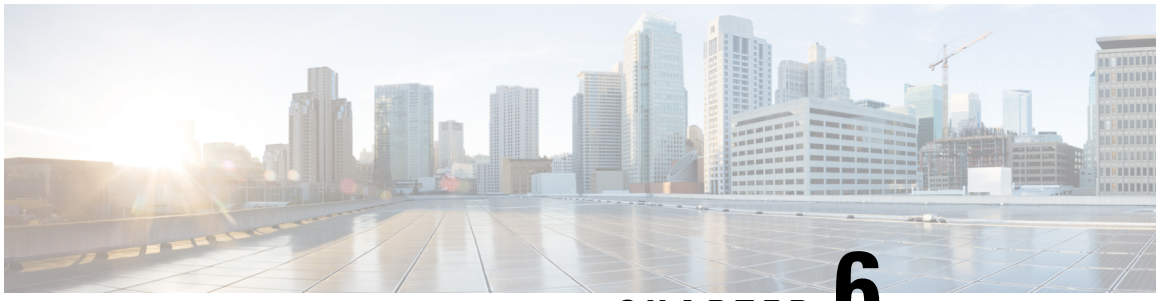
If	Then
If you have installed a Controller, and your cluster consists of a Controller node only	The installation is complete. **1.** Open a browser and enter the URL for your Controller (*https://Controller hostname or IP/oamp*). This opens the Administration Console. Sign in using the System Application credentials. **Note** This is not applicable for Live Data and Ids installation.
If you have installed a Controller, and you intend to install a Member	**1.** Open a browser and enter the URL for your Controller (*https://Controller hostname or IP/oamp*). This opens the Administration Console. **2.** Sign in using the System Application credentials. **3.** *Define the Member node in the Administration console.* **Note** This is not applicable for Live Data and Ids installation.
If you have installed a Member node	Open a browser and enter the URL for your Member *https://IP/cuicui/Main.jsp*. This opens the Unified Intelligence Center Reporting web page. Sign in using the System Application credentials. Until other users are added or integrated, the System Application user has full access to the Unified Intelligence Center Member nodes. **Note** This is not applicable for Live Data and Ids installation.

If	Then
If you are using self-signed certificates	Prerequisite—Download the Unified Intelligence Center tomcat certificate from Cisco Unified OS Administration page of Unified Intelligence Center. Perform the following tasks to upload the Unified Intelligence Center server certificate to Cisco Finesse. 1. Sign in to Cisco Unified OS Administration on Cisco Finesse using the following URL: `https://FQDN of Finesse server:8443/cmplatform`. 2. Select **Security** > **Certificate Management** > **Upload Certificate/Certificate chain**. 3. From the **Certificate Purpose** drop-down list, select **tomcat-trust**. 4. In the **Upload File** field, click **Choose File** and browse to the tomcat.pem file that you saved on your system. 5. Click **Upload**. 6. Restart the Cisco Finesse Tomcat on the Cisco Finesse server. **Note** • Follow the same steps for both the Cisco Finesse publisher and subscriber nodes. • If there is a standalone Live Data system in this deployment, then upload Live Data tomcat certificate in addition to Cisco Finesse, using the above-stated procedure. For more information, see the *Certificates for Live Data* chapter in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

If	Then
If your network does not support multicasting, and when the Unified Intelligence Center administrator sign-in page displays a banner message about the application cluster issues.	Perform the following tasks change the discovery mechanism to `tcp-ip` mode. **1.** Log in to the Cisco Unified Intelligence Center CLI. Specify the System Administrator username and password. **Note** Run the following CLIs on all nodes in the given sequence, starting from the publisher node. **2.** Enter the command **utils service stop** *Intelligence Center Reporting Service*. **3.** Enter the command **utils cuic cluster mode**. **4.** Select cluster mode **2) Enable tcp-ip**. **5.** Enter the command **utils cuic cluster show**. **Note** Ensure that all nodes have an identical configuration. **6.** Enter the command **utils service start** Intelligence Center Reporting Service. **Note** If there happens to be a disconnect and reconnect, check that the database replication is successfully set up across all nodes in the cluster. Perform "Synchronize Cluster" from Cisco Unified Intelligence Center to ensure that cache is in sync across the cluster. For more information, see the *Cluster Configuration for JVM Using Hazelcast* section in *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

Related Topics

Define Member Node in Administration Console, on page 25



CHAPTER 6

Administration Console Sign-In

After you install the Controller, you must sign in to the Administration Console to perform tasks as explained in this chapter.

Note The tasks below are not applicable for a Live Data and IdS deployment.

To sign in, open a browser and enter the URL for your Controller (*https://<HostAddress>/oamp*), where HostAddress is the host name or IP Address of the *Controller*. This opens the Administration Console.

Sign in using the System Application credentials.

- Define Member Node in Administration Console, on page 25
- Verify Controller Is Synchronized with NTP Server, on page 26

Define Member Node in Administration Console

If you intend to add a Member node, you must define the Member in the Administration console before you run the installation for the Member.

Step 1 To access the Administration console, direct a browser to the URL `https://<HOST ADDRESS>/oamp` where HOST ADDRESS is the IP Address or Hostname of your server.

Step 2 Sign in using the system application user ID and password that you defined during installation. For more information, see *Configuration Worksheet*.

Step 3 From left panel, select **Device Configuration**.

The **Device Configuration** page shows the Controller that you have installed. Note that the hostname defaults to the alias CUIC1. (You can change it.)

Step 4 On the **Device Configuration** page, click **New**.

Step 5 On the Device Configuration fields for the new Member, enter a name by which you can identify the Member, the hostname or IP address, and a description for the device.

Step 6 Click **OK**.

The Member appears on the **Device Configuration** list.

Related Topics

Configuration Worksheet, on page 2

Verify Controller Is Synchronized with NTP Server

Make sure that the Network Time Protocol (NTP) on the Controller node is synchronized with the NTP server before you install the Member node.

To do this:

Step 1 Access the Command Line Interface on the Controller node directly, by using the monitor and keyboard at the server console. At the login prompt:

a) Enter the ID for the System Administrator user (created during Basic Install configuration).
b) When prompted, enter the password for the System Administration user.

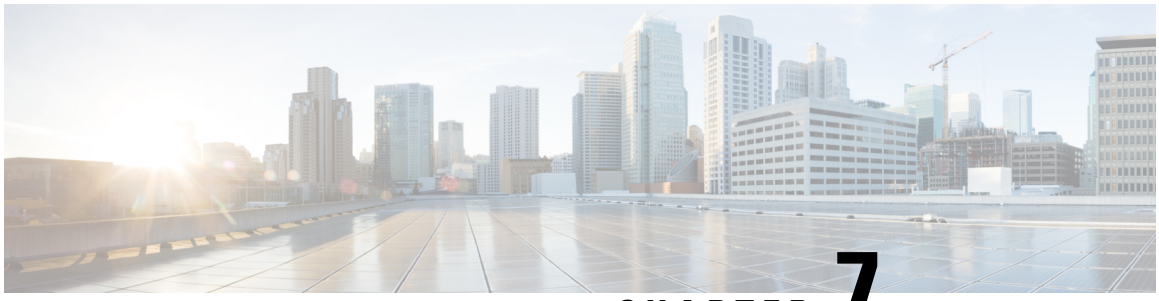
Step 2 Enter this command: *utils ntp status*.

The output must indicate that the node is synchronized with an NTP server. If the Controller node is not synchronized with an NTP server, the installation of the Member node will fail.

Now that the Member is defined in Device Configuration and the NTP synchronization is verified, you can begin to configure and install that member. For more information, see *Installation and Configuration for Member Node*.

Related Topics

Installation and Configuration for Member Node, on page 27



CHAPTER 7

Member Configuration

Installation and Configuration for Member Node

Note All configured nodes in a cluster must be up and running before you install a new Member node.

Note To add a member node in a Live Data only deployment, see *Live Data Standalone Installation*, in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Note To add a member node in a IdS only deployment, see *Install Cisco Identity Service Standalone Deployment*, in the Cisco Unified Contact Center Enterprise Features Guide https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html.

Complete Configuration for Member Node

Step 1 Install the member node following the steps in *Preparation for Unified Intelligence Center Installation on a Virtual Machine*, under sections:

- *Deploy Unified Intelligence Center Open Virtualization Format/Open Virtual Appliance (OVF/OVA)Template*
- *Specify Location of Unified Intelligence Center Installable, on page 9*
- *Install Cisco Unified Intelligence Center on Virtual Machine, on page 10*

Step 2 At the **First Node Configuration Screen**, select **No.**

The First Node Configuration Warning screen opens. This screen advises you that you must configure the server on the first node before you can proceed. You completed this configuration in Define Member Node in Administration Console.

Step 3 Select **OK** at the screen.

Step 4 In the **Network Connectivity Test Configuration** screen, you can verify the connection of this node to the first node (the Controller).

Note The **Network Connectivity Test Configuration** screen refers to the first node as the *publisher*, in reference to its role in database replication. The first node *publishes* or replicates, the databases to the Member nodes, which are referred to as *subscribers* of the database replication. Select **No** to open the First Node Access Configuration screen.

Step 5 In the **First Node Access Configuration** screen, enter connection values *for the first node (the Controller)*:

a) Host Name *of the Controller*
b) IP Address *of the Controller*
c) Security Password (enter and confirm)
d) Select **OK** to open the SMTP Host Configuration screen.

Step 6 In the **SMTP Host Configuration** screen, select whether you want to configure an SMTP host to receive platform-level emails; for example, emails about certificate expiration. This field is optional. You configure email for report scheduling in the Administration console.

If	Then
You want to configure an SMTP Host.	Select **Yes** to open the second SMTP screen. Proceed to Step 7.
You do not want to configure an SMTP Host.	Select **No** to open the Platform Configuration Confirmation screen. Proceed to Step 8.

Step 7 In the second **SMTP Host Configuration** screen:

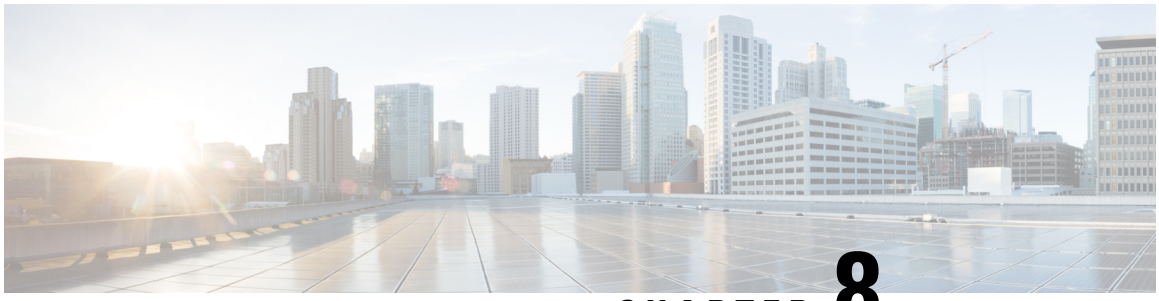
a) Enter the hostname or IP address for the SMTP server.
b) Select **OK** to open the Platform Configuration Confirmation screen.

Step 8 In the **Platform Configuration Confirmation** screen:

If	Then
You want to proceed.	Select **OK**. The installation begins.
You want to revisit screens to modify the configuration.	Select **Back**.

Related Topics

Define Member Node in Administration Console, on page 25



CHAPTER 8

Upgrades

Before You Upgrade

Note

- For important notes, caveats, and other considerations, see the *Cisco Unified Intelligence Center* chapter in the *Release Notes for Cisco Unified Contact Center Enterprise Solution* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-release-notes-list.html.
- If you're upgrading the Cisco Unified Intelligence Center (coresident) deployment, Live Data is also upgraded. As Live Data must be of the same version as Central Controller Components, Central Controller Components must be upgraded in the same window.

Unsupported Widgets

The Cisco Unified Intelligence Center 12.6 interface for Dashboards doesn't support the following widgets:

- Schedule Report widgets
- URL widgets containing Dashboard permalinks (Nested Dashboards)

Migration Limitations

To address injection vulnerabilities, the **Custom Widget** feature in **Dashboards** is disabled by default. If any custom widgets were added to the **Dashboards** in versions earlier to Cisco Unified Intelligence Center 12.6, those widgets are visible in the read-only mode post upgrade to the 12.6 version. You can opt to retain or delete them.

To enable the **Custom Widget** feature, use the CLI and**set cuic properties dashboard-customwidget-enabled** set the parameter value to "on".

For more information, see the *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

Note

- For base version before 12.0(1), you must first upgrade to 12.0(1) and then upgrade to Cisco Unified Intelligence Center12.6(2).
- Cisco Unified Intelligence Center 12.0(1), 12.5(1), 12.5(1) SU, and 12.6(1) users can directly upgrade to 12.6(2).

Upgrade Prerequisites

Before starting the software upgrade,

- Perform the Unified CCE User Integration to import supervisors and their teams from Unified CCE into the Cisco Unified Intelligence Center.
- Back up your system data using the Disaster Recovery system application. To access the DRS application, direct your browser to https://*IP address of Intelligence Center*:8443/drf. For more information, see the online help provided with the DRS application.
- Ensure that the certificates aren't expired. If the certificates are expired, regenerate the certificates.

Upgrade and restart the Controller node first. Then upgrade and restart the members. All nodes must be on the same version of the Cisco Unified Intelligence Center.

Post-Upgrade Tasks

- After upgrading Cisco Unified Intelligence Center to release 12.6(2), ensure to perform the following:

1. Disable the Unified CCE User Integration. (Uncheck the **Enable UCCE User Integration** check box in OAMP > Cluster Configuration > UCCE User Integration.)
2. Install the latest Cisco Options Package (COP) file for the Cisco Unified Intelligence Center 12.6(2) release.
3. Enable the Unified CCE User Integration manually to import the Supervisors with the required roles. This setting is required to view gadgets in the Cisco Finesse Desktop for Supervisors. For more information on User Integration, see the *Unified CCE User Integration Configuration* section in the *Administration Console User Guide for Cisco Unified Intelligence Center* at

   https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.
4. Configure CORS and reset the cluster configuration. For more information on enabling the CORS CLI and to reset the cluster configuration, see Post-Install Configuration , on page 13.
5. When you upgrade Cisco Unified Intelligence Center from earlier releases to release 12.6(2), permissions of all the STOCK value lists for the ALLUSERS group is set to NONE. Therefore, you must reset the permissions manually in 12.6(2) if you want users to use the entire value list.

Your configuration information moves automatically to the upgraded version in the active partition.

Note After the successful upgrade, the CAs that are unapproved by Cisco are removed from the platform trust store. You can add them back, if necessary.

- For information about the list of CAs that Cisco supports, see the Cisco Trusted External Root Bundle at https://www.cisco.com/security/pki.
- For information about adding a certificate, see **Insert a new tomcat-trust certificate** at https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/210541-CUCM-Certificate-Management-and-Change-N.html

Note If you upgrade Cisco Unified Intelligence Center to version 12.6(2) and your Live Data (standalone) server remains on an earlier version (12.0(1), 12.5(1), 12.5(1) SU, or 12.6(1)), ensure that you update the Live Data server with the latest ES for that release. This is required for the Live Data gadgets to work in the Finesse desktop.

Download Unified Intelligence Center Upgrade File

Step 1 Point your browser to the Download Software page for Cisco Unified Intelligence Center: https://software.cisco.com/download/type.html?mdfid=282163829&i=rm, and click the Unified Intelligence Center Software link.

Step 2 Navigate to the folder and subfolder for the release you want.

Step 3 Select the Unified Intelligence Center installer .iso file and click **Download**.

Step 4 Click **Log in**.

Refresh Upgrade

You can perform an upgrade from 12.0(1) to 12.6(2) on the publisher and subscriber nodes of Unified Intelligence Center. Before you begin upgrade, perform a backup. For more information, see *Before You Upgrade*.

Related Topics

Before You Upgrade, on page 29

Upgrade VMware vSphere ESXi for Upgrade

If you use VMware vCenter Server in your deployment, upgrade VMware vCenter Server before upgrading VMware vSphere ESXi.

Upgrade VMWare vSphere ESXi on Side A and Side B servers to the latest version supported with this release of Packaged CCE. Packaged CCE uses standard upgrade procedures, which you can find using VMware documentation (https://www.vmware.com/support/pubs/).

Upgrade Unified Intelligence Center

Follow the steps to install the ISO file using the Unified Intelligence Center CLI.

You can also install the ISO using the upgrade procedure in the Cisco Unified Operating System Administration web interface. For more information, see *Access Unified OS Administration*.

Before you begin

Before you begin the upgrade from 12.0(1) to 12.6(2), you must install the COP `ucos.keymanagement.v01.cop.sgn` on the base version.

Download the ISO file from https://software.cisco.com/download/home/282163829/type/282377062/release to the SFTP server that can be accessed from the Cisco Unified Intelligence Center system.

Note In 12.6(2), the Hazelcast library is upgraded. In TCP mode, Hazelcast can't start with nodes having different versions. In TCP mode, the nodes that are upgraded to 12.6(2) have the **Intelligence Center Reporting Service** in **starting** state until all the remaining nodes in the cluster are upgraded to 12.6(2).

As mentioned earlier in this chapter, all the nodes in a cluster must be on the same version. However, if you have upgraded only some nodes and want **Intelligence Center Reporting Service** available on the upgraded nodes, do one of the following:

- Stop the **Intelligence Center Reporting Service** on all the nodes that aren't upgraded and then restart the upgraded nodes.
- Before the upgrade, change the cluster mode to UDP on all the nodes using the **utils cuic cluster mode** CLI command. After upgrading all the nodes, set the cluster mode to TCP. For more information, see the *Cluster Configuration for JVM Using Hazelcast* section in the Administration Console User Guide for Cisco Unified Intelligence Center.

Step 1 Log in to Unified Intelligence Center CLI and specify the System Administration username and password.

Step 2 Enter the command `utils system upgrade initiate` to initiate the ISO installation.

Step 3 Select **Remote File System** from the source list page.

Step 4 Enter the remote path to the directory on the SFTP server where you have downloaded the ISO file.

Note If the ISO file is located on a Linux or UNIX server, you must enter a forward slash (/) at the beginning of the directory path. For example, if the COP file is in the patches directory, enter **/patches**. If the ISO file is located on a Windows server, check with your system administrator for the correct directory path.

Step 5 Enter the SFTP server name or IP address and then enter the credentials.
It's optional for you to enter the SMTP Host Server name.

Step 6 Select the transfer protocol as SFTP. The system displays the list of ISO files available in the SFTP location.

Step 7 Select the number corresponding to the ISO file that you want to install, and press **Enter**.

Step 8 Enter the relevant option when you're prompted `Switch to new version if the upgrade is successful (yes/no).`

- Enter **yes** to automatically switch the version .

- Enter **no** if you need to manually switch the version after all the nodes are upgraded (refer step 10 for more details).

Note After successfully switching the version, verify if the node is upgraded. You can upgrade from Cisco Unified Intelligence Center 12.0(1) to 12.6(2):

- If you upgrade from 12.0(1) to 12.6(2), the inactive version is 12.0(1), and the active version is 12.6(2).

Step 9 Enter **yes** when you're prompted `Start Refresh Upgrade (yes/no).`

Step 10 In cluster setup, first complete the upgrade on the publisher node and perform the upgrade on the subscriber node. After successful upgrades, switch the version using the command `utils system switch-version` first on the publisher node and later on the subscriber nodes.

Note After successfully switching the version of the publisher node and subscriber node, verify if the nodes are upgraded. You can upgrade from Cisco Unified Intelligence Center 12.0(1) to 12.6(2):

- If you upgrade from 12.0(1) to 12.6(2), the inactive version is 12.0(1), and the active version is 12.6(2).

Related Topics

Access Unified OS Administration , on page 35

L2 Upgrade for Unified Intelligence Center

Follow the steps to install the ISO file using the Unified Intelligence Center CLI.

You can also install the ISO using the upgrade procedure in the Cisco Unified Operating System Administration web interface. For more information, see *Access Unified OS Administration*.

Before you begin

Before you begin the upgrade from 12.5(1) to 12.6(2), you must install the COP `ucos.keymanagement.v01.cop.sgn` on the base version.

Before you begin the upgrade from 12.6(1) to 12.6(2), you must install the COP `ucos.keymanagement.v02.cop.sgn` on the base version.

Note For 12.5(1) SU to 12.6(2) upgrade no COP is required to be applied.

Download the ISO file from https://software.cisco.com/download/home/282163829/type/282377062/release to the SFTP server that can be accessed from the Cisco Unified Intelligence Center system.

Step 1 Log in to Unified Intelligence Center CLI and specify the System Administration username and password.

Step 2 Enter the command `utils system upgrade initiate` to initiate the ISO installation.

Step 3 Select **Remote File System** from source list page.

Step 4 Enter the remote path to the directory on the SFTP server where you have downloaded the ISO file.

Note If the ISO file is located on a Linux or UNIX server, you must enter a forward slash (/) at the beginning of the directory path. For example, if the COP file is in the patches directory, enter **/patches**. If the ISO file is located on a Windows server, check with your system administrator for the correct directory path.

Step 5 Enter the SFTP server name or IP address and then enter the credentials.
It is optional for you to enter the SMTP Host Server name.

Step 6 Enter the relevant option when you are prompted `Continue with upgrade after download (yes/no).`

- Enter **`yes`** to continue with upgrade after the download is complete.
- Enter **`no`** if you want to cancel the upgrade.

Step 7 Enter the relevant option when you are prompted `Switch-version server after upgrade [valid only for ISO] (yes/no).`

- Enter **`yes`** to automatically switch the version after upgrade.
- Enter **`no`** if you need to manually switch the version after all the nodes are upgraded (refer step 11 for more details).

Note After successfully switching the version, verify if the node is upgraded. You can upgrade from Cisco Unified Intelligence Center 12.5(1), 12.5(1) SU, or 12.6(1) to 12.6(2):

- If you upgrade from 12.5(1) to 12.6(2), the inactive version is 12.5(1), and the active version is 12.6(2).
- If you upgrade from 12.5(1) SU to 12.6(2), the inactive version is 12.5(1) SU, and the active version is 12.6(2).
- If you upgrade from 12.6(1) to 12.6(2), the inactive version is 12.6(1), and the active version is 12.6(2).

Step 8 If the transfer protocol is selected as SFTP, the system displays the list of ISO files available in the SFTP location.

Step 9 Select the number corresponding to the ISO file that you want to install, and press **`Enter`**.
When the download is complete, the nodes are automatically upgraded.

Step 10 In cluster setup, first complete the upgrade on the publisher node and perform the upgrade on the subscriber node. If you chose to manually switch version, after successful upgrades, switch the version using the command `utils system switch-version` first on the publisher node and later on the subscriber nodes.

Note After successfully switching the version of the publisher node and subscriber node, verify if the nodes are upgraded. You can upgrade from Cisco Unified Intelligence Center 12.5(1), 12.5(1) SU, or 12.6(1) to 12.6(2):

- If you upgrade from 12.5(1) to 12.6(2), the inactive version is 12.5(1), and the active version is 12.6(2).
- If you upgrade from 12.5(1) SU to 12.6(2), the inactive version is 12.5(1) SU, and the active version is 12.6(2).
- If you upgrade from 12.6(1) to 12.6(2), the inactive version is 12.6(1), and the active version is 12.6(2).

Upgrade VMware Tools

Use this procedure to upgrade VMware tools from the VMware vSphere Client followed by the CLI command.

To upgrade VMware tools for Cisco Unified Intelligence Center:

Step 1 Power on the virtual machine.

Step 2 Right-click the VM and select **Guest** > **Install/Upgrade VMware Tools**.

Step 3 Select the **Interactive Tools Upgrade** option and click **OK**.

Step 4 Open the administrator console and log in to command prompt.

Step 5 Run the command *utils vmtools refresh* and confirm.
The server automatically reboots twice. This process takes a few minutes.

Step 6 After reboot, from the vSphere client, select the VM and click the **Summary** tab.

Step 7 Check for the **VMware Tools** status is "Running (Current)".

Access Unified OS Administration

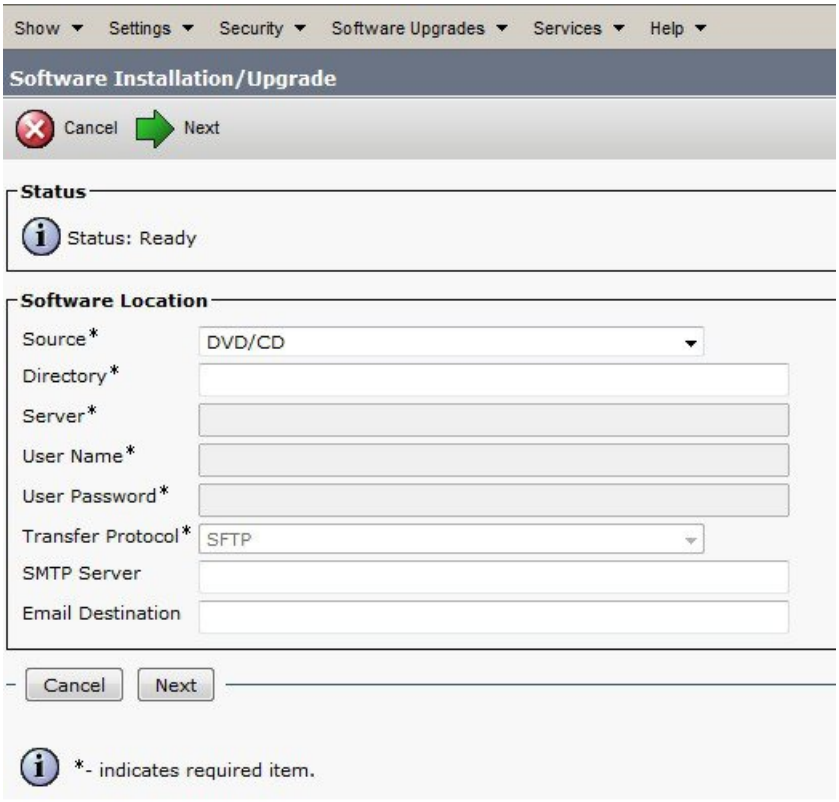
To perform an upgrade from the Cisco Unified OS Administration application, follow the steps.

Step 1 Enter `https://x.x.x.x/cmplatform`, where x.x.x.x is the IP address of the node.

Step 2 Sign in using the username and password of the system administrator account.

Step 3 Select **Software Upgrades** > **Install/Upgrade** to display the Software Installation/Upgrade page.

Figure 1: Software Upgrade Page



Step 4 Select source: Upgrade From DVD/CD or Upgrade From Remote Filesystem.

Upgrade From DVD/CD

Follow these steps if a DVD/CD is the source for your install or upgrade.

Step 1 Prepare a writeable DVD and insert it into the disc drive on the server that is to be upgraded.

Step 2 Select DVD/CD from the Source list on the **Software Upgrades** > **Install/Upgrade page**.

Step 3 In the Directory field, enter the path to the upgrade file.

If the file is in the root directory, enter a slash (/) in the Directory field.

Step 4 To continue the upgrade process, click **Next**.

Step 5 Choose the upgrade version that you want to install and click **Next**.

Step 6 In the next window, monitor the progress of the download.

Step 7 When the download completes, Click **Next**.

Step 8 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts running the upgraded software.

Step 9 If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, do the following:

a) Choose **Do not reboot after upgrade**.
b) Click **Next**. The Upgrade Status window displays the Upgrade log.
c) When the installation completes, click **Finish**.
d) To restart the system and activate the upgrade, choose **Settings** > **Version**, and then click **Switch Version**.

The system restarts running the upgraded software.

Step 10 Run the utility to update the VMware settings. See *Upgrade VMWare Settings Utility*.

Step 11 Clear the browser cache and cookies manually before you start working on the new version of Unified Intelligence Center. For more information about clearing the cache and cookies, see your browser-specific documentation.

Related Topics

Frequently Asked Questions

Upgrade From Remote Filesystem

Follow these steps if Remote Filesystem is the source for your install or upgrade.

Step 1 Choose **Remote Filesystem** from the Source list on the **Software Upgrades** > **Install/Upgrade** page.

Step 2 Enter the path to the directory that contains the patch file on the remote system in the Directory field.

If the upgrade file is on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, enter **/patches**. If the upgrade file is on a Windows server, check with your system administrator for the correct directory path.

Step 3 In the **Server** field, enter the server name or IP address.

Step 4 In the **User Name** field, enter your username on the remote server.

Step 5 In the **User Password** field, enter your password on the remote server.

Step 6 Select the transfer protocol from the **Transfer Protocol** field.

Step 7 To continue the upgrade process, click **Next**.

Step 8 In the next window, monitor the progress of the download.

Step 9 When the download completes, click **Next**.

Step 10 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts running the upgraded software.

Step 11 If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, do the following:

a) Choose **Do not reboot after upgrade**.
b) Click **Next**. The Upgrade Status window displays the Upgrade log.
c) When the installation completes, click **Finish**.
d) To restart the system and activate the upgrade, choose **Settings** > **Version**, and then click **Switch Version**.

The system restarts running the upgraded software.

Note It takes about half an hour to complete the Switch Version and the restart.

Step 12 Run the utility to update the VMware settings. See *Upgrade VMWare Settings Utility*.

Step 13 Clear the browser cache before you start working on the new version of Unified Intelligence Center. For more information about clearing the cache and cookies, see your browser-specific documentation.

Related Topics

Frequently Asked Questions

Revert to Previous Version

After upgrading, you can revert to the software version that was running before the upgrade, by restarting your system and switching to the software version on the inactive partition

Note All nodes must be running the same version of Unified Intelligence Center. Reverting is an all-or-none operation when you operate a cluster of Unified Intelligence Center nodes.

Procedure to Revert to Previous Version

Revert to previous version can be performed in two ways. You can use the CLI command `utils system switch-version` on each node or you can also use the user interface in the Unified OS Administration.

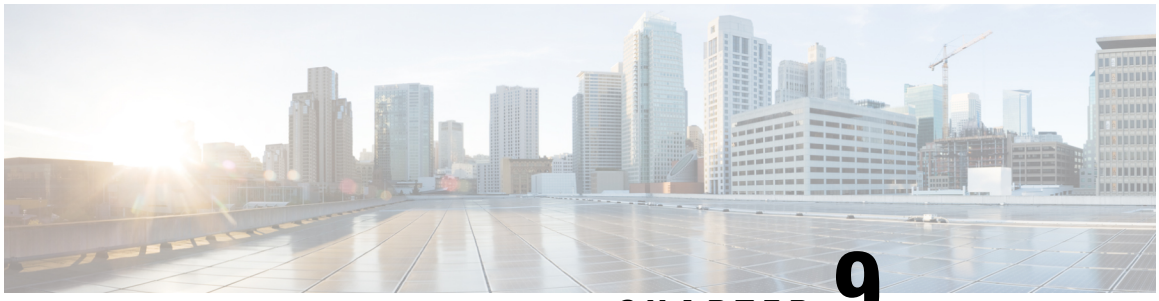
Note

- If you have upgraded from 12.0(1) to 12.6(2), you cannot revert to versions earlier than 12.0(1).
- If you have upgraded from 12.5(1) to 12.6(2), you cannot revert to versions earlier than 12.5(1).
- If you have upgraded from 12.5(1) SU to 12.6(2), you cannot revert to versions earlier than 12.5(1) SU.
- If you have upgraded from 12.6(1) to 12.6(2), you cannot revert to versions earlier than 12.6(1).

Follow these steps to revert using Unified OS Administration:

Procedure

	Command or Action	Purpose
Step 1	Open Unified OS Administration page entering the following URL: `https://server-name/cmplatform`, where server-name is the hostname or IP address of the node.	
Step 2	Sign in using the system administrator credentials.	
Step 3	Choose **Settings** > **Version**. This opens the Version Settings screen, which shows the software version on both the active and inactive partitions. To switch versions and restart, click **Switch Versions**. When the system restarts, it boots to the now-active (formerly inactive) partition with your migrated data in place.	**Note** It takes about half an hour to complete the Switch Version and the restart.



CHAPTER 9

Frequently Asked Questions

Frequently Asked Questions

Can I install on a virtual machine?

Starting with Cisco Unified Intelligence Center release 8.0(3), you can install Unified Intelligence Center on a virtual machine.

Can my Cisco Support Provider log in to assist me?

Yes. There is a utility that allows Cisco technicians to troubleshoot your system, its configurations, and databases.

Set up and enable a time-limited access account to your system using the CLI commands under the `utils remote_account` command or run the utility from the Cisco Unified Operating System Administration Console (select **Services** > **Remote Support**).

The procedure to do this is documented in the online help for the Cisco Unified Operating System Administration Console.

How do I handle "No Such File or Directory" error?

During installation on some servers, you might see an error similar to this:

```
rmmod: ohci_hcd: no such file or directory
```

This is a message related to USB driver modules and can be safely ignored.

The installation attempts to delete all modules on the server before loading new ones. If a module does not exist on the server where the installation is running, a message indicates that there is no such file to be deleted. Messages differ slightly for different driver names.

How do I access log files?

If you encounter problems with the installation, you can obtain and examine the install log files by entering the following commands in Command Line Interface.

- Enter the CLI command `file list install *` to obtain a list of all install log files from the command line.
- Enter the CLI command `file view install <log_file>` to view the log file from the command line where log_file is the log file name.

Other ways to access log files are as follows:

- Use the CLI file dump commands.
- Use the Syslog Viewer in the Real-Time Monitoring Tool (RTMT). Download RTMT from the Administration console (**Tools** > **RTMT Plugin Download**).

How do I add or replace devices in the cluster?

To add a device (for example, to add an additional Member to the cluster):

1. Verify that the virtual machine meets the hardware requirements.
2. Make sure that the other devices in the cluster are up and running.
3. Run a fresh (DVD) installation on the new or replacement device. It must be the same version of Unified Intelligence Center that is currently installed on all other nodes.
4. Test that the new device can connect to the other devices in the cluster. See *How do I test server connectivity?*.

How do I sign in to the Administration Console?

1. Direct a browser to the URL for the administration console.

   The URL is `https://<HOST ADDRESS:8443/oamp/` where HOST ADDRESS is the IP address or host name of your controller node with the default port.
2. Enter the System Application user ID and password that you defined during installation.

   This person is the initial, default Super User.

Any Super Users who were added after the installation can also log in.

How do I sign in to Unified Intelligence Center Reporting?

There are two ways to do this:

- From the browser:
  1. Direct a browser to the URL for the reporting application.

     The URL is `https://<<host>:8444/cuicui/Main.jsp` where HOST ADDRESS is the IP address or host name of your member node.
  2. Enter your login credentials.

The System Application user ID and password defined during installation can log in to the Reporting application. Any additional Login Users who have been created and authenticated can also log in.

How do I access the Command-Line Interface?

You can access the CLI directly from any node, using the monitor and keyboard at the server console.

1. Enter the ID for the System Administrator account created during install.

   See *What accounts and passwords are defined during the installation?*.
2. When prompted, enter the password for the System Administrator account.

The CLI is documented in the *Administration Console User Guide for Cisco Unified Intelligence Center* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

How do I test server connectivity?

There is a step to test network connectivity during the installation of the Controller and Member servers. You can also run a basic check that one server can connect to another using this CLI command: `utils network ping`. See *Complete Configuration for Member Node*.

How do I use the Recovery Disk?

The installation package includes a Recovery Disk on CD media to help you to recover from a catastrophic failure, such as an unbootable system.

To use the Recovery Disk, insert it into the tray and boot up into it.

For more information on Server Recovery, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucm/recovery_cd/Server_Recovery-README.pdf.

Note The recovery disk menu option [A] [a] is not supported.

How do I uninstall?

There is no way to uninstall other than reinserting the installation DVD, which will reformat the hard disk.

How is data handled during an upgrade?

Data migration occurs during an upgrade installation. This includes the database, configuration properties, and licensing files. See *Where is an upgrade installation installed?*.

Warning Do not make configuration changes from the start of the upgrade process until you have activated the inactive partition and re-booted the system.

If you decide to downgrade or switch the system to the inactive partition that contains the older version of the software, any configuration changes that you made since upgrading will be lost.

Is Unified Intelligence Center supported in a hosted deployment?

Yes, deployment in a hosted environment is qualified and tested. The deployments tested are Unified Intelligence Center with Live Data, Live Data, IdS and Unified Intelligence Center only.

What if the installation fails?

If the installation fails, you see a screen asking if you want to copy diagnostic information to a device.

Figure 2: Installation Failed Screen

1. Insert a USB key.
2. Select **Yes**.
3. Select **Continue** at the next two screens.

Note The CLI command to view the install logs is file view install.

The CLI is documented in the *Administration Console User Guide for Cisco Unified Intelligence Center* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

If the installation fails over a virtual machine, you see a screen asking if you want to copy diagnostic information to a device.

Which accounts and passwords are defined during the installation?

During the installation, you specify three passwords: the System Administrator user, the System Application user, and the database access security password. All three must start with an alphabetic character, must be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. Only the application user and password are passed to the online Administration console.

- **System Administrator account:** The System Administrator account User ID and password are configured at installation for each node. Enter the same user name and password for all nodes. The System Administrator for the Controller can access:
  - The CLI for the Controller.
  - The Cisco Systems tools on the Navigation dropdown in the Administration console: Disaster Recovery System, Cisco Unified Serviceability, and Cisco Unified OS Administration interfaces.

  The System Administrator has no access to functions in the Unified Intelligence Center reporting application.

Note If you configure unique System Administrator credentials for Member nodes, you must use those credentials to access the CLI for those Member servers only.

- **System Application User account:** The System Application account User ID and password are configured at installation for each node. Enter the same user name and password for all nodes.

  The System Application user name and password that are configured for the Controller allow an initial login to the Administration console. This user becomes that initial Super User and, can log in to the Unified Intelligence Center Reporting application on all Member nodes.

  As the initial Super User, the System Application User can create additional Super Users in the User Management screen or by using the CLI command set account. This user can also sign in to the Unified Intelligence Center Reporting interface with full access to all functions.

  The initial Super User (the System Application user) created in the installation does not need to be set up in Active Directory. Any additional Super Users created through the Administration console are considered to be IMS users. They can sign into Unified Intelligence Center Reporting and will be limited to the Login User role until they are given additional privileges.

Note If you configure unique System Application credentials for Member nodes, those users have no login rights.

- **Security Password:** The security password defined in the installation wizard is used by the system for the database security password to authorize communications between devices. This password is identical on all servers in the cluster. The security password is also used by the Disaster Recovery System (DRS) for encryption of the backup file.

  You can change the security password using the CLI command set password security.

How do I dump install logs to the serial port of the virtual machine?

1. Configure a serial port on the virtual machine.

   While the virtual machine is powered OFF, edit settings and add a serial port to the virtual machine. You cannot add a serial port while the virtual machine is running. Attach the serial port to a .tmp file, and then power on the virtual machine and start the install.

2. When you are ready to dump the log files, attach a new, empty file to the serial port.

   If the system halts due to an install failure and asks if you want to dump the logs, before you answer yes, you must edit settings on the virtual machine and attach the actual file name where you want to dump the logs. The reason for originally attaching the .tmp file to the serial port is that during the boot-up of Linux, a few garbage characters (terminal escape sequences) get output to that port. If you dump the logs into that file, these characters will corrupt the .tar format of the file. In order to create a valid .tar file, you must connect the serial port to a new and empty file just before you dump the logs to it.

3. Return to the virtual machine console and proceed to dump the logs to the serial port.

   After the file is complete, open it with 7-zip, which you can download from http://www.7-zip.org/download.html.

4. After a successful install, power off the virtual machine, edit settings, and remove the serial port from the virtual machine.

Important Leaving the serial port (or any other virtual hardware) can negatively impact performance of the virtual machine. The serial port has no other use other than dumping the install logs and you will not need it again, unless you perform a fresh install.

What do I do if the upgrade stalls?

During the installation of upgrade software, the upgrade may appear to stall. The upgrade log stops displaying new log messages. When the upgrade stalls, you must cancel the upgrade, disable I/O throttling, and restart the upgrade procedure. When you successfully complete the upgrade, you do not need to reenable I/O throttling.

- To disable I/O throttling, enter the CLI command `utils iothrottle disable`.
- To display the status of I/O throttling, enter the CLI command `utils iothrottle status`.
- To enable I/O throttling, enter the CLI command `utils iothrottle enable`. By default, iothrottle is enabled.

If the system does not respond to the cancellation, you must reboot the server, disable I/O throttling, and restart the upgrade process procedure.

Where is a fresh installation installed?

All Controller servers have an active bootable partition, an inactive bootable partition, and a common partition. The installation creates these partitions, and a fresh (first-time) installation places the new software and operating system on the active partition. The system boots up and operates on the active partition.

Where is an upgrade installation installed?

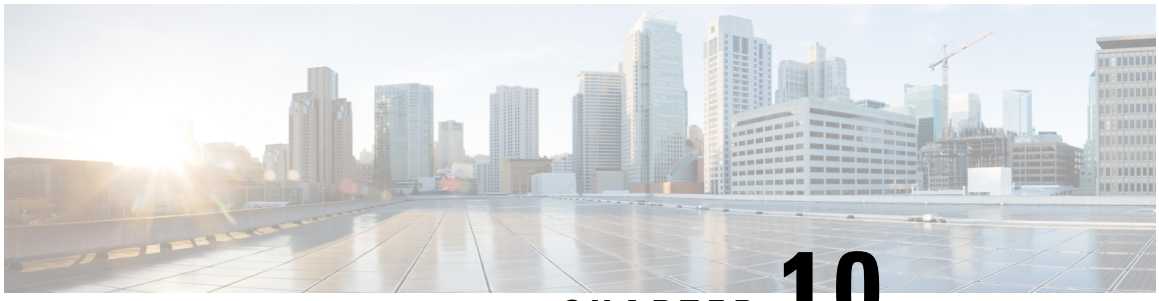
All Controller servers have an active bootable partition, an inactive bootable partition, and a common partition. Upgrade versions are installed on the inactive partition.

To complete the upgrade, you switch partitions using the CLI command `utils system switch-version`.

You can also do this from the Cisco Unified Communications Operating System Administration screen. Navigate to **Settings** > **Version**. This opens the **Version Settings** screen, which shows the software version on both the active and inactive partitions. To switch versions and restart, click **Switch Versions**. When the system restarts, it boots to the now-active (formerly inactive) partition with your migrated data in place. For more information, see *Upgrades*.

What is the supported screen resolution?

Supported screen resolution for Cisco Unified Intelligence Center: 1366 x 768 or higher.



CHAPTER 10

Language Pack for Unified Intelligence Center

Install Language Pack

Post successful install or upgrade, if you want to use the Cisco Unified Intelligence Center interface in a language other than English, you have to download and install the language pack COP.

The language pack for Cisco Unified Intelligence Center is delivered as a single Cisco Option Package (COP) file. The file is available to download from Cisco.com and contains a single installer for all language variants.

You can download the language pack for Cisco Unified Intelligence Center at:

https://software.cisco.com/download/home/282163829/type/282377062/release/12.6(1)

COP files can generally be installed on an active, running system. However, language COP files cannot be removed or rolled back.

Step 1 Download the Cisco Unified Intelligence Center Language Pack COP file from the Cisco Software site to a local source or an SFTP server that can be accessed by the Cisco Unified Intelligence Center server.

Step 2 Use SSH to log in to your Cisco Unified Intelligence Center system with the platform administration account.

Step 3 Use the CLI to run the command **utils system upgrade initiate**.

Step 4 Follow the instructions provided by the utils system upgrade initiate command.

Step 5 Reboot the server.

Step 6 Repeat step 2 through step 5 on the secondary Cisco Unified Intelligence Center server.

Step 7 When the installation is complete on both Cisco Unified Intelligence Center servers, and all Cisco Unified Intelligence Center users must clear their browser cache and cookies.