Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide, Release 12.6(2)

First Published: 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 changes 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
Simplified upgrade using orchestration	CCE Orchestration	
	CLI to configure software download schedule	
	CLI to configure the bandwidth for Orchestration software download	
	Enforce software download from Cisco hosted software artifactory	
	CLI to configure proxy for orchestration	
	Serviceability enhancement for entitlement failure update in CLI to configure artifactory URL and API key	
Unified ICM upgrade Path	Upgrade Path	
Multistage upgrade	Multistage UpgradeWorkflow for 4000 Agents and above Deployments	
Java Upgrade	Java Requirements	

About This Guide

This guide explains how to install, configure, and upgrade Cisco Packaged Contact Center Enterprise (Packaged CCE).

Packaged CCE is a solution deployment for delivering Cisco Unified Contact Center Enterprise in a virtualized environment. Packaged CCE requires strict adherence to capacity limits that are detailed in the *Solution Design Guide for Cisco Packaged Contact Center Enterprise*, available at https://www.cisco.com/en/US/products/ps12586/prod_technical_reference_list.html. It is mandatory to follow all rules and requirements stated in the Design Guide.

This document does not discuss the Packaged CCE Lab Only deployment. For information about that deployment, see the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Audience

This guide is prepared for partners and service providers who will be implementing Packaged CCE, who are familiar with Cisco contact center applications, and who are experienced regarding the deployment and management of virtual machines using VMware technology.

Related Documents

Subject	Link
Cisco Packaged Contact Center Enterprise	https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html
Cisco Unified Contact Center Enterprise	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/tsd-products-support-series-home.html
Cisco Unified Communications Manager	https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html
Cisco Unified Intelligence Center	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/tsd-products-support-series-home.html
Cisco Finesse	https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/tsd-products-support-series-home.html
Cisco Unified Customer Voice Portal	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html
Cisco Enterprise Chat and Email	https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/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.

Field Alerts and Field Notices

Note that Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Field Alert and Cisco Field Notice mechanisms. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest. Log into www.cisco.com; then access the tool at:

https://www.cisco.com/cisco/support/notifications.html

Documentation Feedback

To provide comments about this document, send an email message to the following address:

contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Conventions

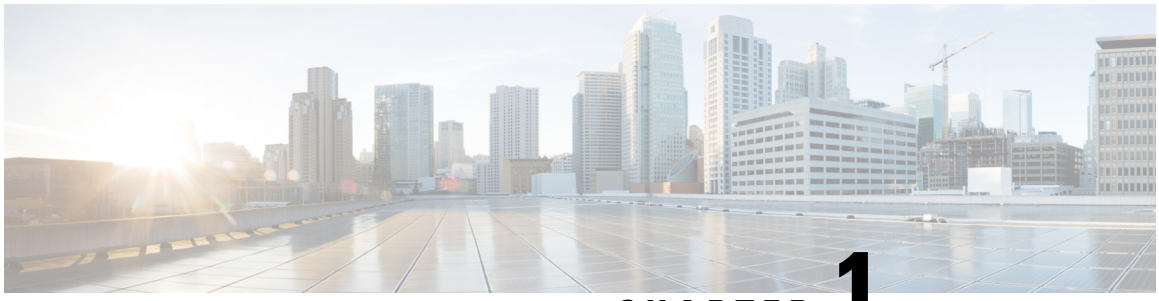
This document uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.

Convention	Description
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems, Inc. </title></html>`
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

PART I

Preparation



CHAPTER 1

System Requirements

Set up Active Directory

Ensure that you have a completed plan for your domain structure and Active Directory implementation before you set up your network.

Warning The Unified CCE servers should be in the same domain, and multiple domains are not supported.

For more information, see the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Transport Layer Security Version 1.2 Required

Contact center enterprise solutions require the use of TLS 1.2 only connections in this release. Our services accept incoming TLS connections only over TLS 1.2. All outgoing TLS connection use only TLS 1.2.

All clients that connect to either our web interfaces or databases must support TLS 1.2.

Note The older versions of the TLS/SSL are disabled by installer.

For more information 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.

Installation Tools

During installation, use one or all of the following tools, as required:

- ICM-CCE-Installer—The main Unified CCE Installer copies all files into relevant folders, creates the base registries, and installs needed third-party software such as JRE and Apache Tomcat. It uses the Microsoft .NET Framework which is an integral software of Windows Server.

Note Optionally, you can update the JRE installed by the Unified CCE Installer with a later version of the JRE. See Java Upgrades, on page 161.

If the ICM-CCE installer installs JRE on the Windows platform, the system retains only the Cisco approved CA certificates in the java certificate store, and removes all the unapproved certificates.

Do not run the installer remotely. Download the installer to a local machine for installation.

- ICM12.6.2.exe—The Unified CCE patch installer. It copies all files into relevant folders, updates the registries, and installs needed third-party software such as JRE, Apache Tomcat, and Microsoft .NET Framework.
- Cisco Unified Intelligent Contact Management Database Administration (ICMDBA) Tool—Used to create new databases, modify or delete existing databases, and perform limited SQL Server configuration tasks.
- Domain Manager—Used to provision Active Directory.
- Web Setup—Used to set up the Call Routers, Loggers, Network Gateways, Network Interface Controllers, and Administration & Data Servers.
- Peripheral Gateway (PG) Setup—Used to set up MR PIMs and CG.

VMware Hosting and Hardware Support

See the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html for the supported specification based hardware, Cisco UCS C-Series servers for Packaged CCE fresh installs and upgrades, and supported VMware vSphere ESXi versions.

Software Compatibility

See the Contact Center Enterprise Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html

- Endpoints for agents and callers
- Cisco gateway hardware and software
- Third-party software

Software Licenses

The following table lists the Cisco components that comprise a Packaged CCE solution:

Components	License requirements
Cisco Packaged Contact Center Enterprise	One server license for each of the voice applications. One agent license for each concurrent user with different feature tiers.
Cisco Unified Communications Manager	One license for each Cisco Unified Communications Manager node, plus device licenses for connected devices.
Cisco Unified Customer Voice Portal (CVP)	You must register CVP instance with Cisco Smart Licensing Server which includes CVP Call Server and VXML Server in order to use the appropriate licenses. For more information, see *Administration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.
Cisco Finesse	Cisco Finesse: User licenses included with selected tiers of Cisco Unified Contact Center Enterprise user licenses. One license for each server pair. One license for each Media Kit.
Cisco Customer Collaboration Platform	User license included with Packaged CCE Agent License. One server license for each Customer Collaboration Platform server.

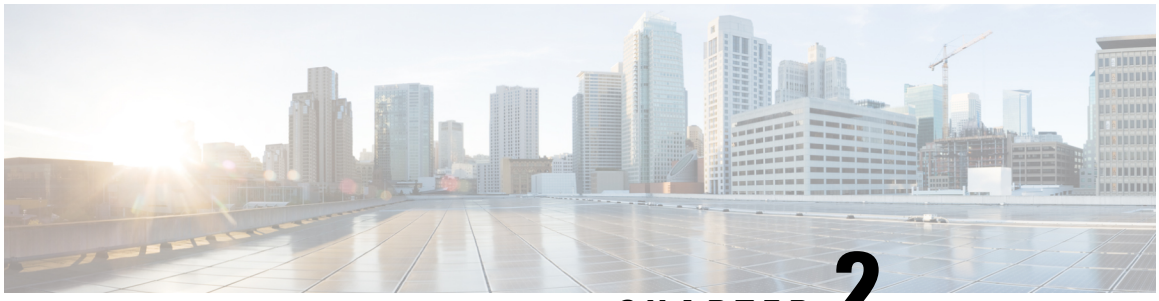
Note Packaged Contact Center Enterprise is enabled with Smart Licensing. For information on Smart Licensing, see the Packaged Contact Center Enterprise Administration and Configuration Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Before you begin an installation or upgrade of any part of your contact center, confirm the following:

- That you have all the required software products.
- That all the software versions are compatible with each other.
- That all software versions are also compatible with all hardware and VMware.

Java Requirements

CCE has transitioned from Oracle to OpenJDK for the Java runtime environment (JRE). All CCE components require OpenJDK JRE version 1.8 (32-bit), update 352 or later. The 12.6(2) installer will install the required OpenJDK 1.8 version. If the existing Oracle JRE is not needed, you may uninstall it from the system manually.



CHAPTER 2

Prepare Customer Site Servers

Prepare Customer Site Servers

Perform all the procedures in this section on the Side A and the Side B servers.

Prepare Cisco UCS C-Series Customer Site Servers

Configure RAID for Cisco UCS C240 M4SX

The disk array configuration for the Cisco UCS C240 M4SX is already set up to match what is required for Packaged CCE. Verify the settings as follows.

Using Cisco Integrated Management Controller, check that the following settings are configured correctly:

- Virtual Drive Info: RAID 5 with 5 (Physical Disks) * 4 (Virtual Drives/Datastores)
- Stripe Size: 128KB
- Write Policy: Write Back with BBU
- Read Policy: Read Ahead Always

For more information regarding RAID configuration for Cisco UCS C240 M4SX in Configure RAID with GUI (UCS C-Series M4 Servers) section, refer to Cisco Collaboration on Virtual Servers Guide.

Configure RAID for Cisco UCS C240 M5SX and Cisco UCS C240 M6SX

The disk array configuration for the Cisco UCS C240 M5SX and Cisco UCS C240 M6SX is already set up to match the requirements. Verify the settings as follows:

Procedure

Using Cisco Integrated Management Controller, check that the following settings are configured correctly:

- Virtual Drive Info: RAID 5 with 6 (Physical Disks) * 4 (Virtual Drives or Datastores)
- Stripe Size: 128KB
- Write Policy: Write Back with BBU
- Read Policy: Read Ahead Always

For more information regarding RAID configuration for Cisco UCS C240 M5SX or Cisco UCS C240 M6SX, see the *Installation and Configuration* section of the Cisco Collaboration on Virtual Servers Guide.

Install VMware vSphere ESXi

Packaged CCE uses standard VMware vSphere ESXi installation procedures. For installation procedures to install the supported version of vSphere ESXi that you are installing, see the VMware documentation at https://www.vmware.com/support/pubs/.

For Packaged CCE, you must install the ESXi on the first drive as the default boot drive for the server.

Add the Datastores to the Host Server

After installing vSphere ESXi, add the remaining datastores. Refer to the *vSphere Storage Guide* for the vSphere ESXi version in your deployment, available at https://www.vmware.com/support/pubs/.

Required datastores are dictated by the hardware platform used. Cisco UCS C-Series servers require a fixed and validated configuration.

See the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html for IOPs requirements.

Add the Customer ESXi Host to the vCenter

Refer to the vCenter Server and Host Management documentation at https://www.vmware.com/support/pubs/

Customers without vCenter can install on management desktops to administer the Packaged CCE servers.

Prepare HyperFlex M5 series Customer Site Servers

Cisco HyperFlex HX-Series System provides a unified view of the storage across all nodes of the HyperFlex HX cluster via the HX Data Controller Platform. For optimal performance, it is recommended that all VMs are mapped to the single unified datastore. This mapping enables the HX Data Platform to optimize storage access based on the workload and other operating parameters.

For more information, see the documentation on Cisco HyperFlex HX Data Platform at https://www.cisco.com/c/en/us/support/hyperconverged-systems/hyperflex-hx-data-platform-software/products-installation-guides-list.html.

For information on installing collaboration software, see the *Cisco Collaboration on Virtual Servers* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

NTP and Time Synchronization

Packaged CCE requires that all parts of the solution have the same time. While time drift occurs naturally, it is critical to configure NTP to keep solution components synchronized.

To prevent time drifts on Live Data reports, the NTP settings on the Rogger VMs, the PG VMs, the AW VMs, and on the Cisco Unified Intelligence Center Publisher and Subscriber VMs must be synchronized.

Important Microsoft periodically releases cumulative time zone updates. These updates include worldwide changes to time zone names, bias (the amount of time in minutes that a time zone is offset from Coordinated Universal Time (UTC)), and observance of daylight saving time. These patches update the information in the Windows registry. When these updates are available, apply them to all virtual machines in the deployment that are running a Microsoft Windows operating system.

Windows Active Directory Domain

The Windows Active Directory Primary Domain Controller (PDC) emulator for the forest in which the Packaged CCE domain resides (whether same, parent, or peer) must be properly configured to use an external time source. This external time source should be a trusted and reliable NTP provider, and if already configured for the customer's forest, must be used (and useable) as same source for all other applications as detailed in this section for the Packaged CCE solution.

See the following references for properly configuring Windows Active Directory Domain for NTP external time source:

- How to configure an authoritative time server in Windows Server.

Note Do not use the "Fix it for me" function in this article.

- AD DS: The PDC emulator in this forest should be configured to correctly synchronize time from a valid time source.

Microsoft Windows Server Domains do not automatically recover or fail over the authoritative internal time source for the domain when the PDC emulator server is lost, due to hardware failure or otherwise. This article, Time Service Configuration on the DCwith PDC Emulator FSMO Role, helps describe how you must additionally configure the new target server to be the authoritative internal time source for the domain. It also covers manual intervention to recover and seize or reassign the PDC FSMO role to another domain controller.

Windows Components in the Domain

Windows hosts in the domain are automatically configured to synch their time with a PDC emulator, whether by the PDC emulator with authoritative internal time source or chained from same in the domain forest hierarchy.

Windows Components Not in the Domain

Use the following steps to set NTP time source for a Windows Server that is not joined to a domain:

1. Log in as a user with administrative privileges.
2. In the Command Prompt window, type the following line and press ENTER: `w32tm /config /manualpeerlist:PEERS /syncfromflags:MANUAL`

Note Replace peers with a comma-separated list of NTP servers.

3. Restart the w32time service: `net stop w32time && net start w32time`.
4. Synch w32time service with peers: `w32tm /resync`.
5. Use the following Service Control command to ensure proper start of the w32time service on any reboot of the server: `sc triggerinfo w32time start/networkon stop/networkoff`.

Cisco Integrated Service Routers

Cisco IOS Voice Gateways must be configured to use the same NTP source for the solution in order to provide accurate time for logging and debugging. See Basic System Management Configuration Guide, Cisco IOS Release 15M&T: Setting Time and Calendar Services.

VOS Components

Components such as Unified Intelligence Center, Finesse, Customer Collaboration Platform, and Unified Communications Manager must point to the same NTP servers as the domain authoritative internal time source.

CLI commands for NTP Servers

While NTP servers are typically specified at install time, here a few commands you can use from the platform cli of the above listed components, to list, add and remove ntp servers. From the platform CLI:

- To list existing ntp servers: `utils ntp servers list`
- To add an additional ntp server: `utils ntp server add <host or ip address to add>`
- To delete an existing ntp server: `utils ntp server delete (row number of the item to delete)`. Press **Enter**.

ESXi Hosts

All Packaged CCE ESXi hosts (including those for optional components), must point to the same NTP server(s) used by the Windows domain PDC emulator as the their external time source.

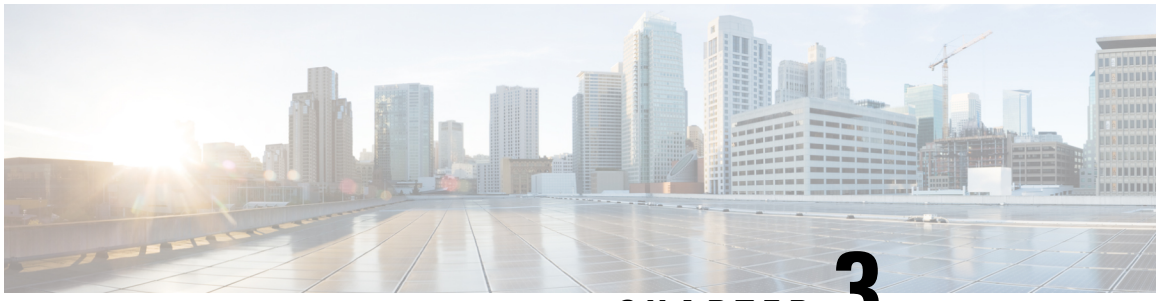
For details on configuring NTP on ESXi hosts, see the VMware documentation athttps://www.vmware.com/support/pubs/ .

Global Catalog Requirements

Packaged CCE uses the Global Catalog for Active Directory Lookup. All domains in the AD Forest in which the Packaged CCE Hosts reside must publish the Global Catalog for that domain. This includes all domains with which your solution interacts, for example, Authentication, user lookup, and group lookup.

In a multi-domain forest, a Global Catalog is required at each AD site. Global Catalog is a central repository of domain information in an AD forest. A significant performance degradations and failure occur without local or Global Catalog. It is important for every AD query to search each domain in the forest. The multi-site deployments are required to query across WAN links.

Note This does not imply cross-forest operation. Cross-forest operation is not supported.



CHAPTER 3

Network Design Considerations

Network Design Considerations

See the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html for network design requirements and considerations for Cisco UCS C-Series servers.

Bandwidth Provisioning and Network QoS Considerations

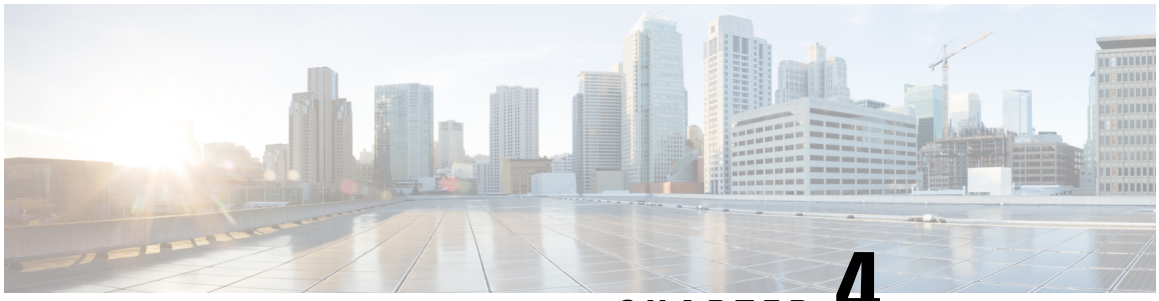
Your Wide Area Network must support QoS. For details, refer to the *Bandwidth Provisioning and QoS considerations* section in the *Solution Design Guide for Cisco Unified Contact Center Enterprise*. at https://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html.

For bandwidth provisioning information for video calls, refer to the "Cisco Collaboration Solutions Design and Deployment Sizing Considerations" chapter of the *Cisco Collaboration System Solution Reference Network Designs*, at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html.

For Nexus 1000V QoS provisioning information and example configuration, see the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html.

PART II

Installation



CHAPTER 4

Packaged CCE 2000 Agents Installation

Installation Tasks

This section provides tasks to create and set up virtual machines (VM) of various components that are required for the Packaged CCE 2000 Agents installation. For information about creating VMs on the appropriate data centers for specific components, see the *Unified CCE Reference Designs* section in the Solution Design Guide for Cisco Packaged Contact Center Enterprise.

Note If your Reference Design layout is on the Cisco HX220c-M5SX or Cisco HX220c-M6S servers, auto-discovery (to identify and validate the components on ESXi servers) is based only on the first node of the Hyperflex cluster.

Note If you have Cisco UCS C240 M5SX or Cisco UCS C240 M6SX or Cisco HX220c-M5SX or Cisco HX220c-M6S Tested Reference Configuration or Specification-Based hardware, make sure that the following core components are added on-box without changing the default annotations:

- Unified CCE Rogger
- Unified CCE AW/HDS/DDS
- Unified CCE PG
- Unified CVP Server
- Unified Intelligence Center (with coresident LiveData and IDS)
- Finesse

The following terms are reserved for core component annotations: Cisco, Finesse, CUIC, and CVP. Do not use these reserved terms in the annotations of any of the non-core component VMs.

Note Take a backup of the VM Snapshot before installing the Packaged CCE software, because uninstallation support is not provided.

The table outlines the Packaged CCE 2000 Agents installation tasks.

Table 1: Packaged CCE 2000 Agents Installation

Component Installation Tasks	
1	Create VM for Unified CCE PG, on page 17
2	Create VM for Unified CCE Rogger, on page 17
3	Create VM for Unified CCE AW-HDS-DDS, on page 18
4	Create VMs for the Cisco Unified Customer Voice Portal Servers, on page 18
5	Create VM for Cisco Unified Communications Manager Publisher, on page 19
6	Create VM for Cisco Unified Communications Manager Subscriber, on page 20
7	Create VM for Cisco Finesse Primary, on page 20
8	Create VM for Cisco Finesse Secondary, on page 20
9	Create VM for Cisco Unified Intelligence Center Publisher, on page 21
10	Create VM for Cisco Unified Intelligence Center Subscriber, on page 21
11	Install Cisco Virtualized Voice Browser, on page 205
12	(Optional) Create VM for Cloud Connect Publisher, on page 22
13	(Optional) Create VM for Cloud Connect Subscriber, on page 22
14	(Optional) Create VM for Cisco Unified CVP Reporting Server, on page 21
15	(Optional) Install Media Server, on page 19
16	(Optional) Install Enterprise Chat and Email, on page 204
17	(Optional) Install the External HDS, on page 200

For the post installation configurations of each component, see *Post Installation Configuration* section in the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/pcce/pcce_12_5_1/configuration/guide/pcce_b_admin-and-config-guide_12_5/pcce_b_admin-and-config-guide_12_5_chapter_01.html.

Create Virtual Machines for Components

Create VM for Unified CCE PG

Follow this sequence of tasks to create a virtual machine for the Unified CCE PG.

Sequence	Task
1	Using Packaged-CCE-UCCE.ova, Create a Virtual Machine from the OVA, on page 166. Select **Medium PG** from the drop-down list.
2	Install Microsoft Windows Server, on page 172
3	Install VMware Tools, on page 179
4	Configure Network Adapters , on page 180
5	Add Machine to Domain, on page 179
6	Install Antivirus Software, on page 171
7	Set Persistent Static Routes, on page 182
8	Run Windows Updates, on page 182
9	Install Cisco Unified Contact Center Enterprise, on page 183

Create VM for Unified CCE Rogger

Follow this sequence of tasks to create a virtual machine for the Unified CCE Rogger.

Sequence	Task
1	Using Packaged-CCE-UCCE.ova, Create a Virtual Machine from the OVA, on page 166. Select **Rogger** from the drop-down list.
2	Install Microsoft Windows Server, on page 172
3	Install VMware Tools, on page 179
4	Configure Network Adapters , on page 180
5	Add Machine to Domain, on page 179
6	Install Antivirus Software, on page 171
7	Configure Database Drive, on page 169
8	Set Persistent Static Routes, on page 182
9	Run Windows Updates, on page 182
10	Install Microsoft SQL Server, on page 174

Sequence	Task
11	Install Cisco Unified Contact Center Enterprise, on page 183

Create VM for Unified CCE AW-HDS-DDS

Follow this sequence of tasks to create a virtual machine for the Unified CCE AW-HDS-DDS.

Sequence	Task
1	Using Packaged-CCE-UCCE.ova, Create a Virtual Machine from the OVA, on page 166. Select **AW-HDS-DDS** from the drop-down list.
2	Install Microsoft Windows Server, on page 172
3	Install VMware Tools, on page 179
4	Configure Network Adapter for Unified CCE AW-HDS-DDS, AW-HDS, HDS-DDS , on page 181
5	Add Machine to Domain, on page 179
6	Install Antivirus Software, on page 171
7	Configure Database Drive, on page 169
8	Run Windows Updates, on page 182
9	Install Microsoft SQL Server, on page 174
10	Install Cisco Unified Contact Center Enterprise, on page 183
11	Configure Permissions in the Local Machine, on page 185

Create VMs for the Cisco Unified Customer Voice Portal Servers

Follow this sequence of tasks to create the virtual machines for the Unified CVP Servers. Each Unified CVP Server combines the Unified CVP Call Server, Media Server, and VXML Server functionality.

Sequence	Task
1	Using Packaged-CCE-CVP.ova, Create a Virtual Machine from the OVA, on page 166. From the drop-down list: • Select **Cisco Unified CVP Call Server-VXML Server** from the drop-down list when you create the Unified CVP Server VM.
2	Install Microsoft Windows Server, on page 172 NTP configuration is required if this machine is not in the same domain as the Unified CCE Roggers, AWs, and PGs. See NTP and Time Synchronization, on page 7.
3	Install VMware Tools, on page 179

Sequence	Task
4	Configure Network Adapters for Cisco Unified CVP, on page 187
5	Add Machine to Domain, on page 179
6	Install Antivirus Software, on page 171
7	Run Windows Updates, on page 182
8	Install Cisco Unified CVP Server, on page 188
9	Install FTP Server, on page 190

Install Media Server

If the Media Server is external, install the following on the Media Server:

Sequence	Installation Tasks
1	Setup Unified CVP Media Server IIS, on page 189
2	Install FTP Server, on page 190

Create VM for Cisco Unified Communications Manager Publisher

Follow this sequence of tasks to create the virtual machine for the Unified Communications Manager Publisher.

Note For the Cisco UCS C240 M4SX Server, the Unified Communications Manager (CUCM) 12.5 and above installation must be off-box.

Sequence	Task
1	Using Packaged-CCE-CUCM.ova. Create a Virtual Machine from the OVA, on page 166. Select **CUCM 10000 user node** from the drop-down list.
2	Configure DNS Server, on page 168
3	Install the Unified Communications Manager Publisher. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 192.
4	Install VMware Tools, on page 179
5	Configure the Cluster for Cisco Unified Communications Manager, on page 195
6	Create a Unified Communications Manager AXL User Account, on page 195
7	Generate and install the Unified Communications Manager License, on page 194.
8	Activate Services, on page 198

Create VM for Cisco Unified Communications Manager Subscriber

Follow this sequence of tasks to create the virtual machine for the Cisco Unified Communications Manager Subscriber.

Sequence	Task
1	Using Packaged-CCE-CUCM.ova, Create a Virtual Machine from the OVA, on page 166. Select **CUCM 7500 user node** from the drop-down list.
2	Configure DNS Server, on page 168
3	Install the Unified Communications Manager Subscriber. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 197.
4	Install VMware Tools, on page 179
5	Generate and install the Unified Communications Manager License, on page 194.
6	Activate Services, on page 198

Create VM for Cisco Finesse Primary

Follow this sequence of steps to create a virtual machine for the Cisco Finesse Primary node.

Sequence	Task
1	Using the Packaged-CCE-Finesse.ova, Create a Virtual Machine from the OVA, on page 166. Select **2000 HTTPS Agent** from the drop-down list.
2	Configure DNS Server, on page 168
3	Install the Cisco Finesse Primary node. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 192.
4	Install VMware Tools, on page 179
5	Configure the Cluster for Cisco Finesse, on page 196

Create VM for Cisco Finesse Secondary

Follow this sequence of tasks to create the virtual machine for the Cisco Finesse Secondary node.

Sequence	Task
1	Using Packaged-CCE-Finesse.ova, Create a Virtual Machine from the OVA, on page 166. Select **2000 HTTPS Agent** from the drop-down list.
2	Configure DNS Server, on page 168

Sequence	Task
3	Install the Cisco Finesse Secondary node. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 197.
4	Install VMware Tools, on page 179

Create VM for Cisco Unified Intelligence Center Publisher

Follow this sequence of tasks to create the virtual machine for the Unified Intelligence Center Publisher. Live Data and the Cisco Identity Service are also installed on the same VM.

Sequence	Task
1	Using Packaged-CCE-CUIC.ova, Create a Virtual Machine from the OVA, on page 166. Select **Co-Resident** from the drop-down list.
2	Configure DNS Server, on page 168
3	Install the Cisco Unified Intelligence Center Publisher. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 192.
4	Install VMware Tools, on page 179
5	Configure the Cluster for Cisco Unified Intelligence Center, on page 194

Create VM for Cisco Unified Intelligence Center Subscriber

Follow this sequence of tasks to create the virtual machine for the Unified Intelligence Center Subscriber. Live Data and the Cisco Identity Service are also installed on this VM.

Sequence	Task
1	Using Packaged-CCE-CUIC.ova, Create a Virtual Machine from the OVA, on page 166. Select **Co-Resident** from the drop-down list.
2	Configure DNS Server, on page 168
3	Install the Cisco Unified Intelligence Center Subscriber. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 197.
4	Install VMware Tools, on page 179

Create VM for Cisco Unified CVP Reporting Server

Follow this sequence of tasks to create a virtual machine for the Unified CVP Reporting Server. The Unified CVP Reporting Server is an optional component.

Sequence	Task
1	Using the Packaged-CCE-CVP.ova template, create a virtual machine. For more information, see Create a Virtual Machine from the OVA, on page 166. **Note** The CVP Reporting Server can use the CVP Call Server's OVA template. However, the annotation name used should be generic. By default, the VM annotation is named as CVP VM template. After the VM is deployed, you must change the name. Do not use the terms Cisco, Finesse, CUIC, and CVP in the name because they are reserved for the core components. For example, instead of CVP-VM-Reporting-Server.ova, use SelfService-Reporting-Server.ova. If any of the core component names are used, the CVP Reporting Server fails the VM validation. Select **Cisco Unified CVP Reporting Server** from the drop-down list.
2	Install Microsoft Windows Server, on page 172 NTP configuration is required if this machine is not in the same domain as the Unified CCE Roggers, AWs, and PGs. See NTP and Time Synchronization, on page 7.
3	Install VMware Tools, on page 179
4	Configure Network Adapters for Cisco Unified CVP, on page 187
5	Install Antivirus Software, on page 171
6	Configure Database Drive, on page 169
7	Run Windows Updates, on page 182
8	Install Cisco Unified CVP Reporting Server, on page 191
9	Add Machine to Domain, on page 179

Create VM for Cloud Connect Publisher

Follow this sequence of tasks to create the virtual machine for the Cloud Connect Publisher.

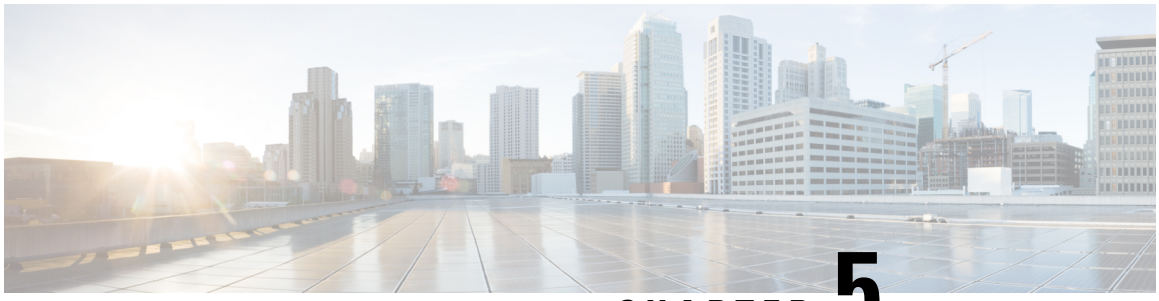
Sequence	Task
1	Using Packaged-CCE-cloudconnect.ova, Create a Virtual Machine from the OVA, on page 166.
2	Install the Cloud Connect Publisher. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 192.

Create VM for Cloud Connect Subscriber

Follow this sequence of tasks to create the virtual machine for the Cloud Connect Subscriber.

Sequence	Task
1	Using Packaged-CCE-cloudconnect.ova, Create a Virtual Machine from the OVA, on page 166.
2	Set Cloud Connect Secondary Node. See Set Subscriber or Secondary Node of Cloud Connect.

Sequence	Task
3	Install the Cloud Connect Subscriber. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 197.



CHAPTER 5

Packaged CCE 4000 Agents Installation

Installation Tasks

This section provides the sequence to create and set up virtual machines of various components that are required for the Packaged CCE 4000 Agents fresh installation. For information about creating VMs on the appropriate data centers for specific components, see *Unified CCE Reference Designs* section in the *Solution Design Guide for Cisco Unified Contact Center Enterprise*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/pcce/pcce_12_5_1/design/guide/pcce_b_soldg-for-packaged-cce-12_5/pcce_b_soldg-for-packaged-cce-12_5_chapter_01.html.

The table outlines the Packaged CCE 4000 Agents fresh installation tasks.

Table 2: Packaged CCE 4000 Agents Installation

Component Installation Tasks	
1	Create VM for Unified CCE PG, on page 26
2	Create VM for Unified CCE Rogger, on page 26
3	Create VM for Unified CCE AW-HDS-DDS, on page 27
4	Create VMs for the Cisco Unified Customer Voice Portal Servers, on page 28
5	Create VM for Cisco Unified Communications Manager Publisher, on page 29
6	Create VM for Cisco Unified Communications Manager Subscriber, on page 29
7	Create VMs for Cisco Finesse Primary Nodes, on page 29
8	Create VMs for Cisco Finesse Secondary Nodes, on page 30
9	Create VM for Cisco Unified Intelligence Center Publisher, on page 30
10	Create VM for Cisco Unified Intelligence Center Subscriber, on page 30
11	Create VM for Live Data Primary Node, on page 31

Component Installation Tasks	
12	Create VM for Live Data Secondary Node, on page 31
13	Create VM for Cisco Identity Service Publisher, on page 31
14	Create VM for Cisco Identity Service Subscriber, on page 32
15	Install Cisco Virtualized Voice Browser, on page 205
16	(Optional) Create VM for Cisco Unified CVP Reporting Server, on page 28
17	(Optional) Install Media Server, on page 19
18	(Optional) Install Enterprise Chat and Email, on page 204
19	(Optional) Install the External HDS, on page 200

For the post installation configurations of each component, see *Post Installation Configuration* section in the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/pcce/pcce_12_5_1/configuration/guide/pcce_b_admin-and-config-guide_12_5/pcce_b_admin-and-config-guide_12_5_chapter_01.html.

Create Virtual Machines for Components

Create VM for Unified CCE PG

Follow this sequence of tasks to create a virtual machine for the Unified CCE PG.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Install Microsoft Windows Server, on page 172
3	Install VMware Tools, on page 179
4	Configure Network Adapters , on page 180
6	Add Machine to Domain, on page 179
7	Install Antivirus Software, on page 171
8	Set Persistent Static Routes, on page 182
9	Run Windows Updates, on page 182
10	Install Cisco Unified Contact Center Enterprise, on page 183

Create VM for Unified CCE Rogger

Follow this sequence of tasks to create a virtual machine for the Unified CCE Rogger.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Install Microsoft Windows Server, on page 172
3	Install VMware Tools, on page 179
4	Configure Network Adapters , on page 180
5	Add Machine to Domain, on page 179
6	Install Antivirus Software, on page 171
7	Configure Database Drive, on page 169
8	Set Persistent Static Routes, on page 182
9	Run Windows Updates, on page 182
10	Install Microsoft SQL Server, on page 174
11	Install Cisco Unified Contact Center Enterprise, on page 183

Create VM for Unified CCE AW-HDS-DDS

Follow this sequence of tasks to create a virtual machine for the Unified CCE AW-HDS-DDS.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Install Microsoft Windows Server, on page 172
3	Install VMware Tools, on page 179
4	Configure Network Adapter for Unified CCE AW-HDS-DDS, AW-HDS, HDS-DDS , on page 181
5	Add Machine to Domain, on page 179
6	Install Antivirus Software, on page 171
7	Configure Database Drive, on page 169
8	Run Windows Updates, on page 182
9	Install Microsoft SQL Server, on page 174
10	Install Cisco Unified Contact Center Enterprise, on page 183
11	Configure Permissions in the Local Machine, on page 185

Create VMs for the Cisco Unified Customer Voice Portal Servers

Follow this sequence of tasks to create the virtual machines for the Unified CVP Servers. Each Unified CVP Server combines the Unified CVP Call Server, Media Server, and VXML Server functionality.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Install Microsoft Windows Server, on page 172 NTP configuration is required if this machine is not in the same domain as the Unified CCE Roggers, AWs, and PGs. See NTP and Time Synchronization, on page 7.
3	Install VMware Tools, on page 179
4	Configure Network Adapters for Cisco Unified CVP, on page 187
5	Add Machine to Domain, on page 179
6	Install Antivirus Software, on page 171
7	Run Windows Updates, on page 182
8	Install Cisco Unified CVP Server, on page 188
9	Install FTP Server, on page 190

Create VM for Cisco Unified CVP Reporting Server

Follow this sequence of tasks to create a virtual machine for the Unified CVP Reporting Server.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166. **Note** The CVP Reporting Server can use the CVP Call Server's OVA template. However, the annotation name used should be generic. By default, the VM annotation is named as CVP VM template. After the VM is deployed, you must change the name. Do not use the terms Cisco, Finesse, CUIC, and CVP in the name because they are reserved for the core components. For example, instead of CVP-VM-Reporting-Server.ova, use SelfService-Reporting-Server.ova. If any of the core component names are used, the CVP Reporting Server fails the VM validation.
2	Install Microsoft Windows Server, on page 172 NTP configuration is required if this machine is not in the same domain as the Unified CCE Roggers, AWs, and PGs. See NTP and Time Synchronization, on page 7.
3	Install VMware Tools, on page 179
4	Configure Network Adapters for Cisco Unified CVP, on page 187
5	Install Antivirus Software, on page 171
6	Configure Database Drive, on page 169
7	Run Windows Updates, on page 182

Sequence	Task
8	Install Cisco Unified CVP Reporting Server, on page 191
9	Add Machine to Domain, on page 179

Create VM for Cisco Unified Communications Manager Publisher

Follow this sequence of tasks to create the virtual machine for the Unified Communications Manager Publisher.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Configure DNS Server, on page 168
3	Install the Unified Communications Manager Publisher. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 192.
4	Install VMware Tools, on page 179
5	Configure the Cluster for Cisco Unified Communications Manager, on page 195
6	Create a Unified Communications Manager AXL User Account, on page 195
7	Generate and install the Unified Communications Manager License, on page 194.
8	Activate Services, on page 198

Create VM for Cisco Unified Communications Manager Subscriber

Follow this sequence of tasks to create the virtual machine for the Cisco Unified Communications Manager Subscriber.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Configure DNS Server, on page 168
3	Install the Unified Communications Manager Subscriber. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 197.
4	Install VMware Tools, on page 179
5	Generate and install the Unified Communications Manager License, on page 194.
6	Activate Services, on page 198

Create VMs for Cisco Finesse Primary Nodes

Follow this sequence of steps to create a virtual machine for each of the Cisco Finesse Primary nodes.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Configure DNS Server, on page 168
3	Install the Cisco Finesse Primary node. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 192.
4	Install VMware Tools, on page 179
5	Configure the Cluster for Cisco Finesse, on page 196

Create VMs for Cisco Finesse Secondary Nodes

Follow this sequence of tasks to create the virtual machine for each of the Cisco Finesse Secondary nodes.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Configure DNS Server, on page 168
3	Install the Cisco Finesse Secondary node. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 197.
4	Install VMware Tools, on page 179

Create VM for Cisco Unified Intelligence Center Publisher

Follow this sequence of tasks to create the virtual machine for the Unified Intelligence Center Publisher.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Configure DNS Server, on page 168
3	Install the Cisco Unified Intelligence Center Publisher. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 192.
4	Install VMware Tools, on page 179
5	Configure the Cluster for Cisco Unified Intelligence Center, on page 194

Create VM for Cisco Unified Intelligence Center Subscriber

Follow this sequence of tasks to create the virtual machine for the Unified Intelligence Center Subscriber nodes.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Configure DNS Server, on page 168
3	Install the Cisco Unified Intelligence Center Subscriber. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 197.
4	Install VMware Tools, on page 179

Create VM for Live Data Primary Node

Follow this sequence of steps to create a virtual machine for the Cisco Live Data Primary node.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Configure DNS Server, on page 168
3	Install the Cisco Live Data Primary node. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 192.
4	Install VMware Tools, on page 179

Create VM for Live Data Secondary Node

Follow this sequence of steps to create a virtual machine for the Cisco Live Data Secondary node.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166. Select **Small Live Data Server** from the drop-down list for 4000 Agents deployment. Select **Larger Live Data Server** from the drop-down list for 12000 Agents deployment.
2	Configure DNS Server, on page 168
3	Install the Cisco Live Data Secondary node. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 197.
4	Set Live Data Secondary Node, on page 203
5	Install VMware Tools, on page 179

Create VM for Cisco Identity Service Publisher

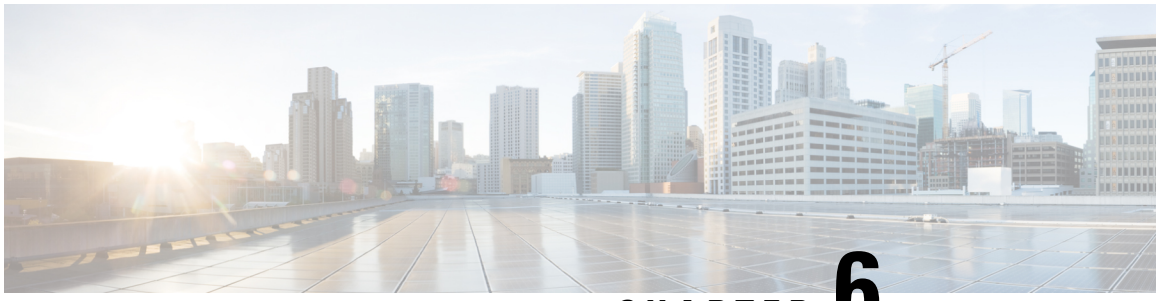
Follow this sequence of steps to create a virtual machine for the Cisco Identity Service Publisher node.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Configure DNS Server, on page 168
3	Install the Cisco Identity Service Publisher node. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 192.
4	Install VMware Tools, on page 179

Create VM for Cisco Identity Service Subscriber

Follow this sequence of steps to create a virtual machine for the Cisco Identity Service Subscriber node.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Configure DNS Server, on page 168
3	Install the Cisco Identity Service Subscriber node. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 197.
4	Set IdS Subscriber Node, on page 204
5	Install VMware Tools, on page 179



CHAPTER 6

Packaged CCE 12000 Agents Installation

Installation Tasks

This section provides the sequence to create and set up virtual machines of various components that are required for the Packaged CCE 12000 Agents fresh installation. For information about creating VMs on the appropriate data centers for specific components, see *Unified CCE Reference Designs* section in the *Solution Design Guide for Cisco Unified Contact Center Enterprise*, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/pcce/pcce_12_5_1/design/guide/pcce_b_soldg-for-packaged-cce-12_5/pcce_b_soldg-for-packaged-cce-12_5_chapter_01.html.

The table outlines the Packaged CCE 12000 Agents fresh installation tasks.

Table 3: Packaged CCE 12000 Agents Installation

Component Installation Tasks	
1	Create VM for Unified CCE PG, on page 26
2	Create VM for Unified CCE Logger, on page 34
3	Create VM for Unified CCE Router, on page 35
4	Create VM for Unified CCE AW-HDS, on page 35
5	Create VM for Unified CCE HDS-DDS, on page 35
6	Create VMs for the Cisco Unified Customer Voice Portal Servers, on page 28
7	Create VM for Cisco Unified Communications Manager Publisher, on page 29
8	Create VM for Cisco Unified Communications Manager Subscriber, on page 29
9	Create VMs for Cisco Finesse Primary Nodes, on page 29
10	Create VMs for Cisco Finesse Secondary Nodes, on page 30
11	Create VM for Cisco Unified Intelligence Center Publisher, on page 30

Component Installation Tasks	
12	Create VM for Cisco Unified Intelligence Center Subscriber, on page 30
13	Create VM for Live Data Primary Node, on page 31
14	Create VM for Live Data Secondary Node, on page 31
15	Create VM for Cisco Identity Service Publisher, on page 31
16	Create VM for Cisco Identity Service Subscriber, on page 32
17	Install Cisco Virtualized Voice Browser, on page 205
18	(Optional) Create VM for Cisco Unified CVP Reporting Server, on page 28
19	(Optional) Install Media Server, on page 19
20	(Optional) Install Enterprise Chat and Email, on page 204
21	(Optional) Install the External HDS, on page 200

For the post installation configurations of each component, see *Post Installation Configuration* section in the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/pcce/pcce_12_5_1/configuration/guide/pcce_b_admin-and-config-guide_12_5/pcce_b_admin-and-config-guide_12_5_chapter_01.html.

Create Virtual Machines for Components

Create VM for Unified CCE Logger

Follow this sequence of tasks to create a virtual machine for the Unified CCE Logger.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Install Microsoft Windows Server, on page 172
3	Install VMware Tools, on page 179
4	Configure Network Adapters , on page 180
5	Add Machine to Domain, on page 179
6	Install Antivirus Software, on page 171
7	Configure Database Drive, on page 169
8	Run Windows Updates, on page 182
9	Install Microsoft SQL Server, on page 174
10	Install Cisco Unified Contact Center Enterprise, on page 183

Create VM for Unified CCE Router

Follow this sequence of tasks to create a virtual machine for the Unified CCE Router.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Install Microsoft Windows Server, on page 172
3	Install VMware Tools, on page 179
4	Configure Network Adapters , on page 180
5	Add Machine to Domain, on page 179
6	Install Antivirus Software, on page 171
7	Run Windows Updates, on page 182
8	Install Cisco Unified Contact Center Enterprise, on page 183

Create VM for Unified CCE AW-HDS

Follow this sequence of tasks to create a virtual machine for the Unified CCE AW-HDS.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Install Microsoft Windows Server, on page 172
3	Install VMware Tools, on page 179
4	Configure Network Adapter for Unified CCE AW-HDS-DDS, AW-HDS, HDS-DDS , on page 181
5	Add Machine to Domain, on page 179
6	Install Antivirus Software, on page 171
7	Configure Database Drive, on page 169
8	Run Windows Updates, on page 182
9	Install Microsoft SQL Server, on page 174
10	Install Cisco Unified Contact Center Enterprise, on page 183
11	Configure Permissions in the Local Machine, on page 185

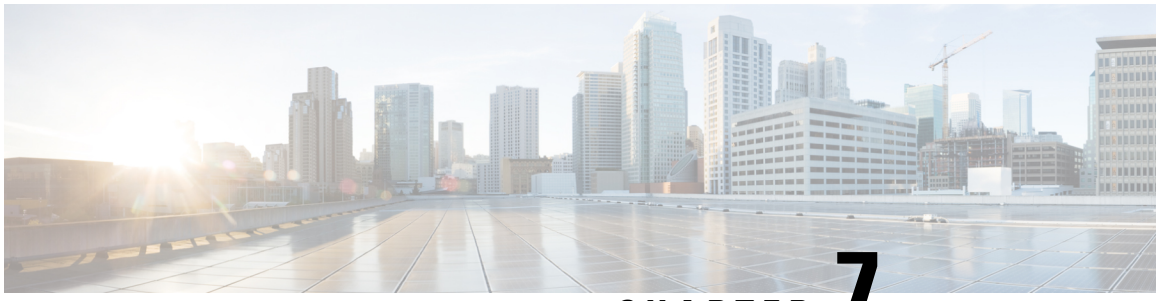
Create VM for Unified CCE HDS-DDS

Follow this sequence of tasks to create a virtual machine for the Unified CCE HDS-DDS.

Sequence	Task
1	Create a Virtual Machine from the OVA, on page 166.
2	Install Microsoft Windows Server, on page 172
3	Install VMware Tools, on page 179
4	Configure Network Adapter for Unified CCE AW-HDS-DDS, AW-HDS, HDS-DDS , on page 181
5	Add Machine to Domain, on page 179
6	Install Antivirus Software, on page 171
7	Configure Database Drive, on page 169
8	Run Windows Updates, on page 182
9	Install Microsoft SQL Server, on page 174
10	Install Cisco Unified Contact Center Enterprise, on page 183
11	Configure Permissions in the Local Machine, on page 185

PART III

Version Upgrade



CHAPTER 7

Upgrade Overview

Following are the two supported upgrade methods:

- **Common Ground Upgrades**: The Common Ground method is an in-place upgrade performed on your existing virtual machine which involves upgrading the Packaged CCE and all other associated software hosted on it. If your hardware meets the requirements for this release, you can perform a Common Ground upgrade without acquiring additional hardware.

Note

- CCE components can be upgraded using common ground or technology refresh upgrade.
- Common Ground Upgrade is not supported if the platform upgrade from Windows Server 2016 and SQL Server 2017 to Windows Server 2019 and SQL Server 2019 is planned as part of upgrade process.

- **Technology Refresh Upgrades**: Use the Technology Refresh upgrade method to set up all the virtual machines (VMs) or the required set of VMs on a different hardware. You can also upgrade the solution components and the associated software hosted on it.

Note For better performance, Media Routing PG (MR PG), Dialer, and Agent PG should be on the same VM.

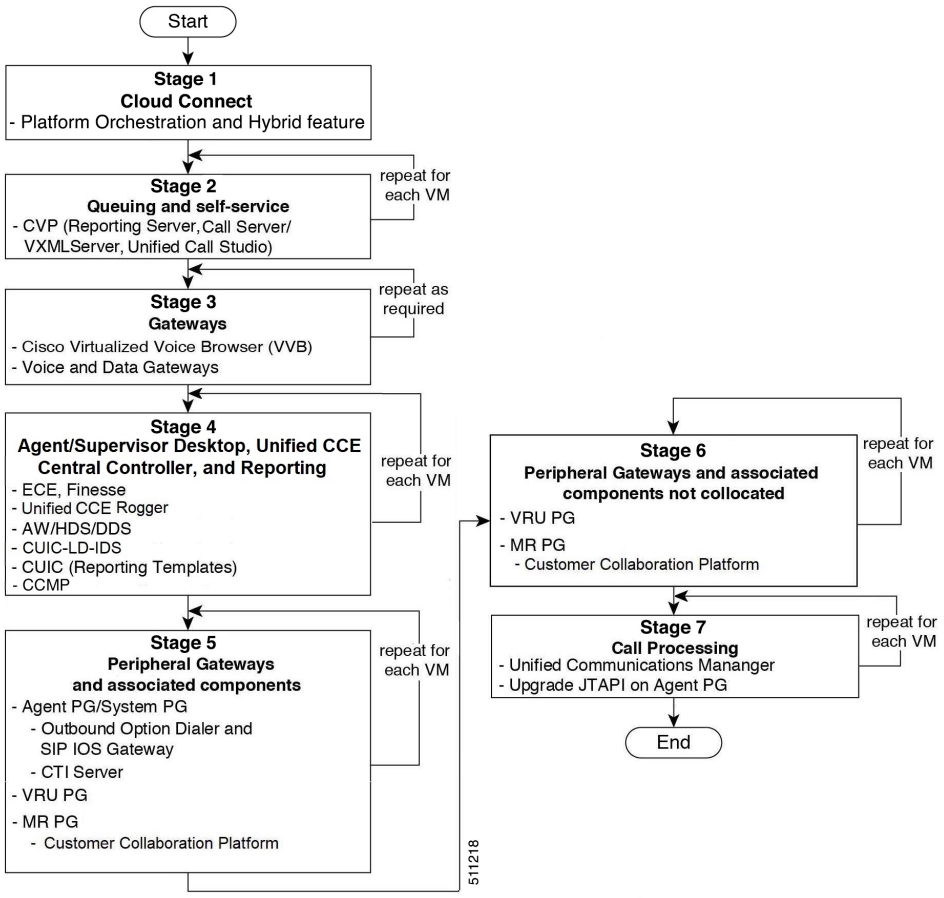
- Upgrade Flow, on page 39
- Silent Upgrade, on page 57
- Upgrade CCE Minor/Maintenance Release Software, on page 57
- Custom Truststore to Store Component Certificates, on page 58

Upgrade Flow

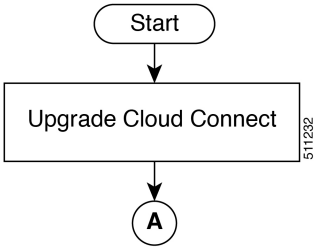
Upgrade Flowcharts for 2000 Agent Deployments

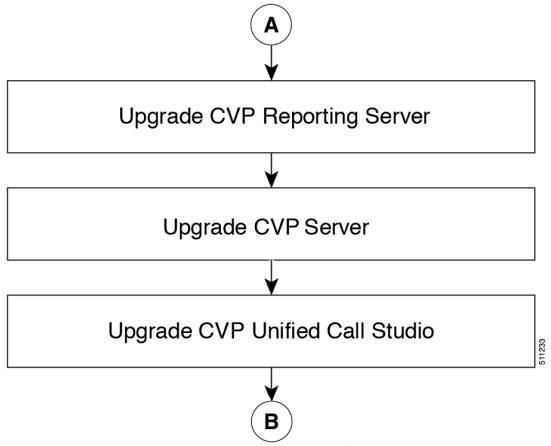
The following diagram illustrates the solution-level upgrade flow for the Packaged CCE 2000 Agent Deployment solution upgrade.

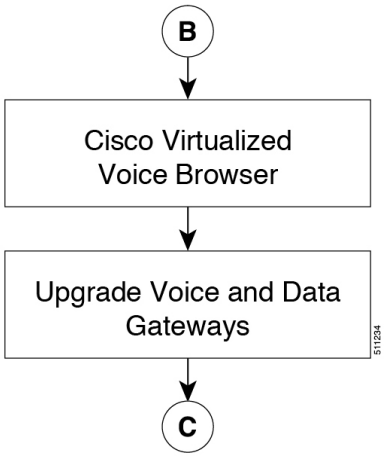
Note This flowchart is not applicable for redundant upgrade workflow.

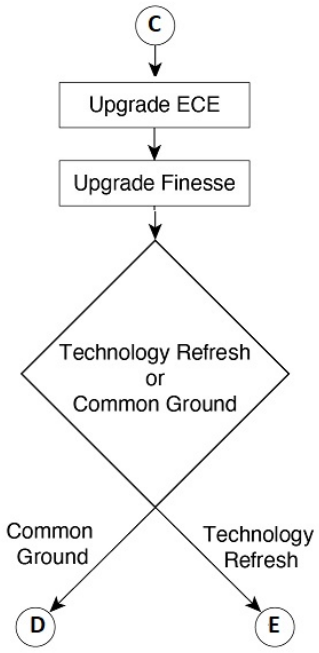


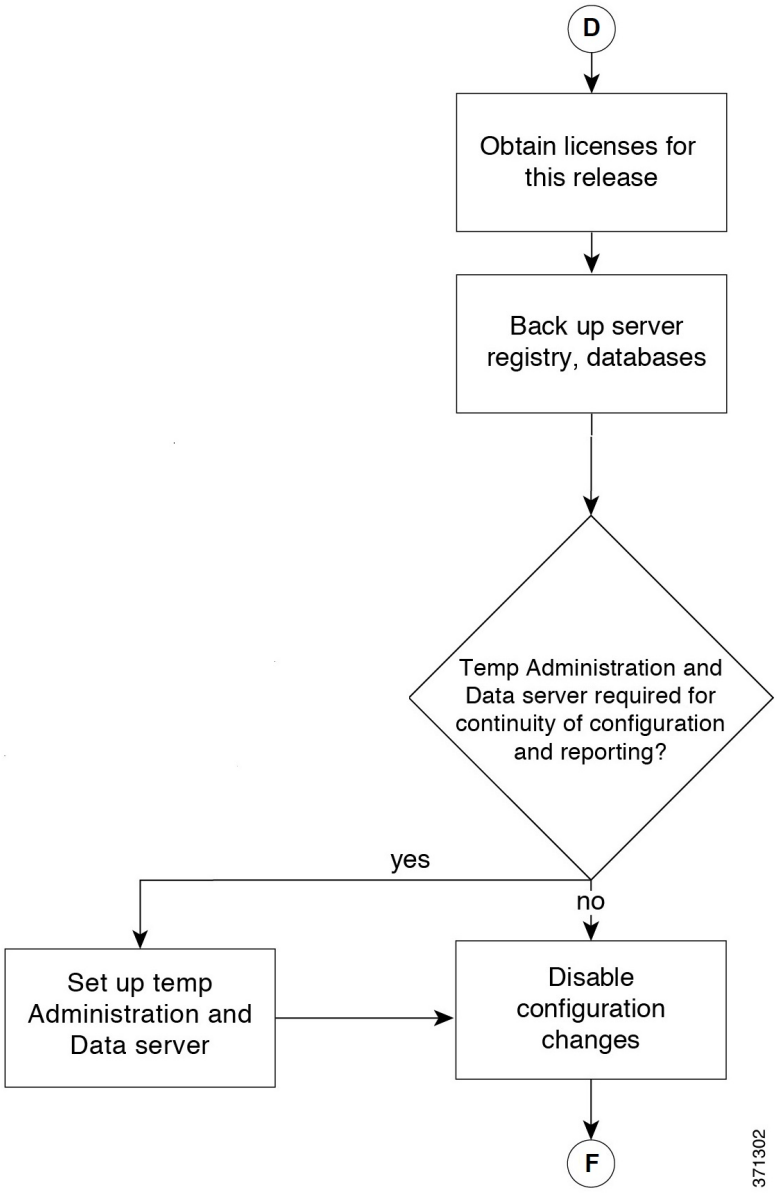
The following diagrams illustrate the stages of the component-level upgrade flows for the Packaged CCE 2000 Agent Deployment solution upgrade. Each diagram covers one of the stages. The letter at the end of each flow indicates the start of the next flow that you are required to perform.

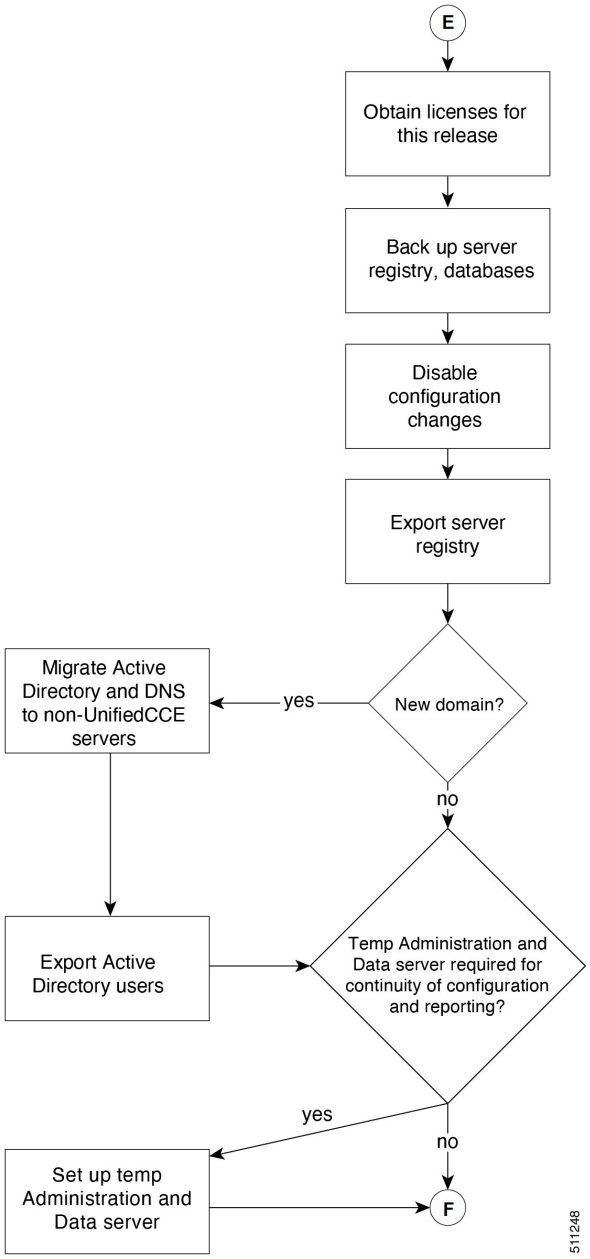


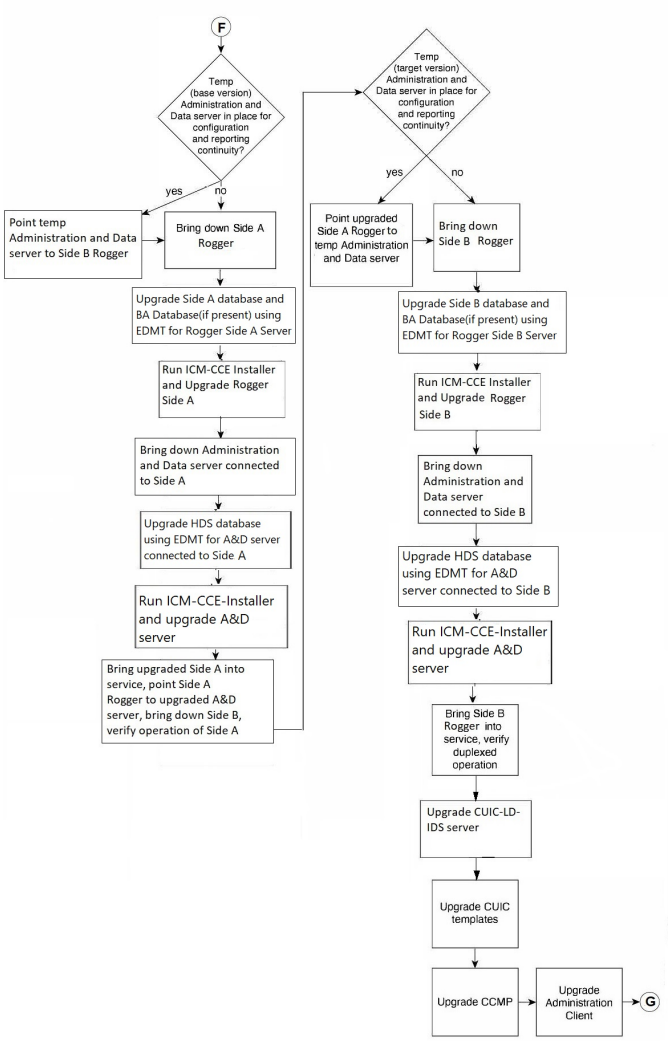

A
Upgrade CVP Reporting Server
Upgrade CVP Server
Upgrade CVP Unified Call Studio
511233
B

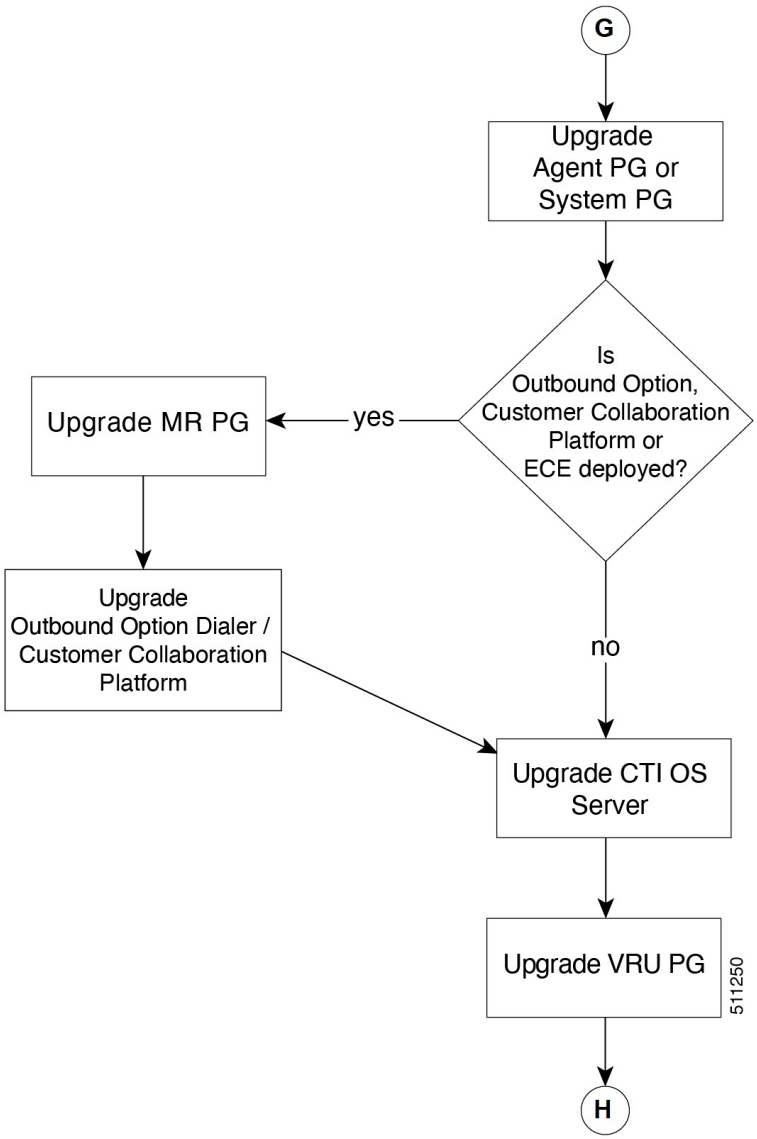

B
Cisco Virtualized Voice Browser
Upgrade Voice and Data Gateways
511234
C

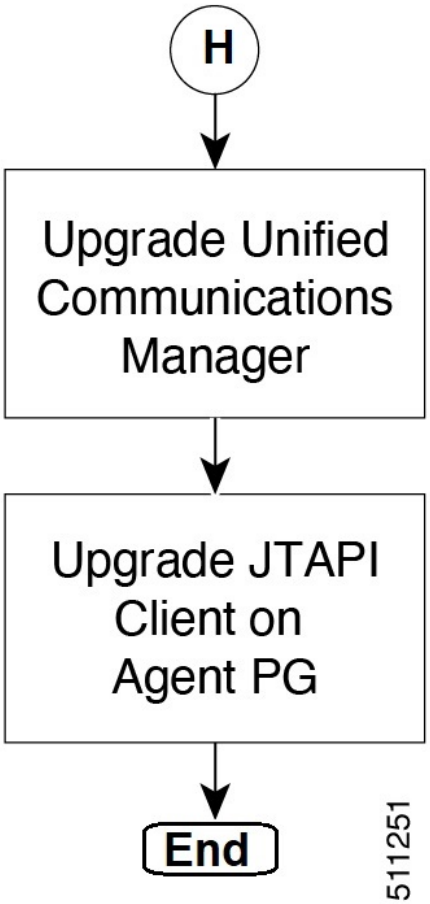

C
Upgrade ECE
Upgrade Finesse
Technology Refresh
or
Common Ground
Common
Ground
Technology
Refresh
D
E


D
Obtain licenses for this release
Back up server registry, databases
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
Disable configuration changes
F
371302


E
Obtain licenses for this release
Back up server registry, databases
Disable configuration changes
Export server registry
New domain?
yes
Migrate Active Directory and DNS to non-UnifiedCCE servers
no
Export Active Directory users
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
F
511248

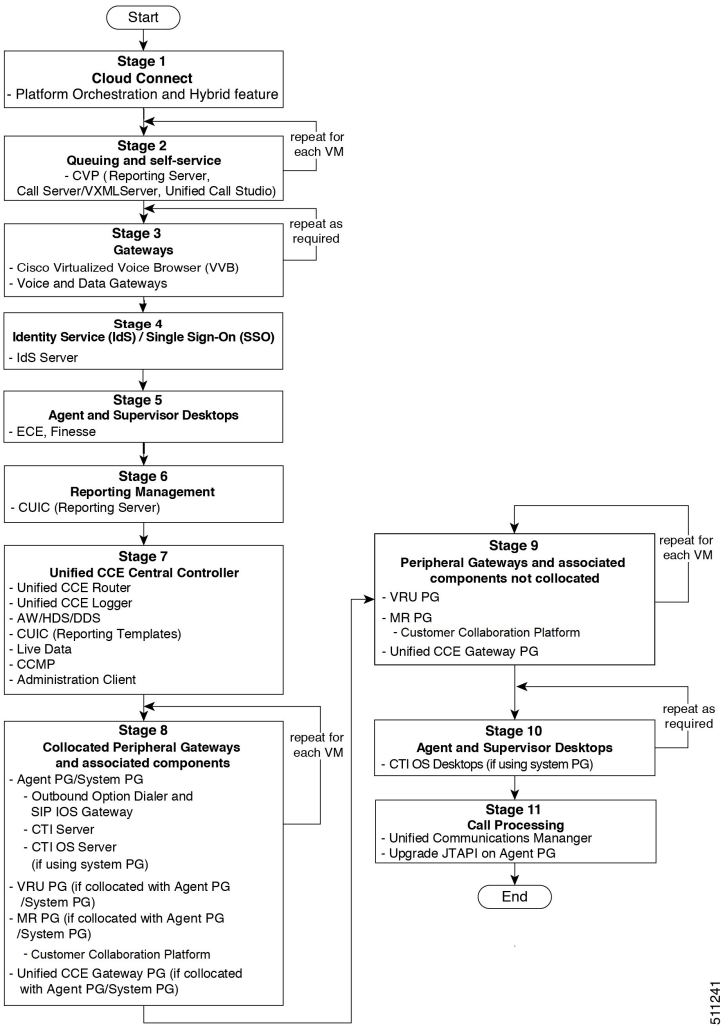

F
Temp (base version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point temp Administration and Data server to Side B Rogger
Bring down Side A Rogger
Upgrade Side A database and BA Database(if present) using EDMT for Rogger Side A Server
Run ICM-CCE Installer and Upgrade Rogger Side A
Bring down Administration and Data server connected to Side A
Upgrade HDS database using EDMT for A&D server connected to Side A
Run ICM-CCE-Installer and upgrade A&D server
Bring upgraded Side A into service, point Side A Rogger to upgraded A&D server, bring down Side B, verify operation of Side A
Temp (target version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point upgraded Side A Rogger to temp Administration and Data server
Bring down Side B Rogger
Upgrade Side B database and BA Database(if present) using EDMT for Rogger Side B Server
Run ICM-CCE Installer and Upgrade Rogger Side B
Bring down Administration and Data server connected to Side B
Upgrade HDS database using EDMT for A&D server connected to Side B
Run ICM-CCE-Installer and upgrade A&D server
Bring Side B Rogger into service, verify duplexed operation
Upgrade CUIC-LD-IDS server
Upgrade CUIC templates
Upgrade CCMP
Upgrade Administration Client
G


G
Upgrade Agent PG or System PG
Is Outbound Option, Customer Collaboration Platform or ECE deployed?
yes
Upgrade MR PG
Upgrade Outbound Option Dialer / Customer Collaboration Platform
no
Upgrade CTI OS Server
Upgrade VRU PG
H
511250

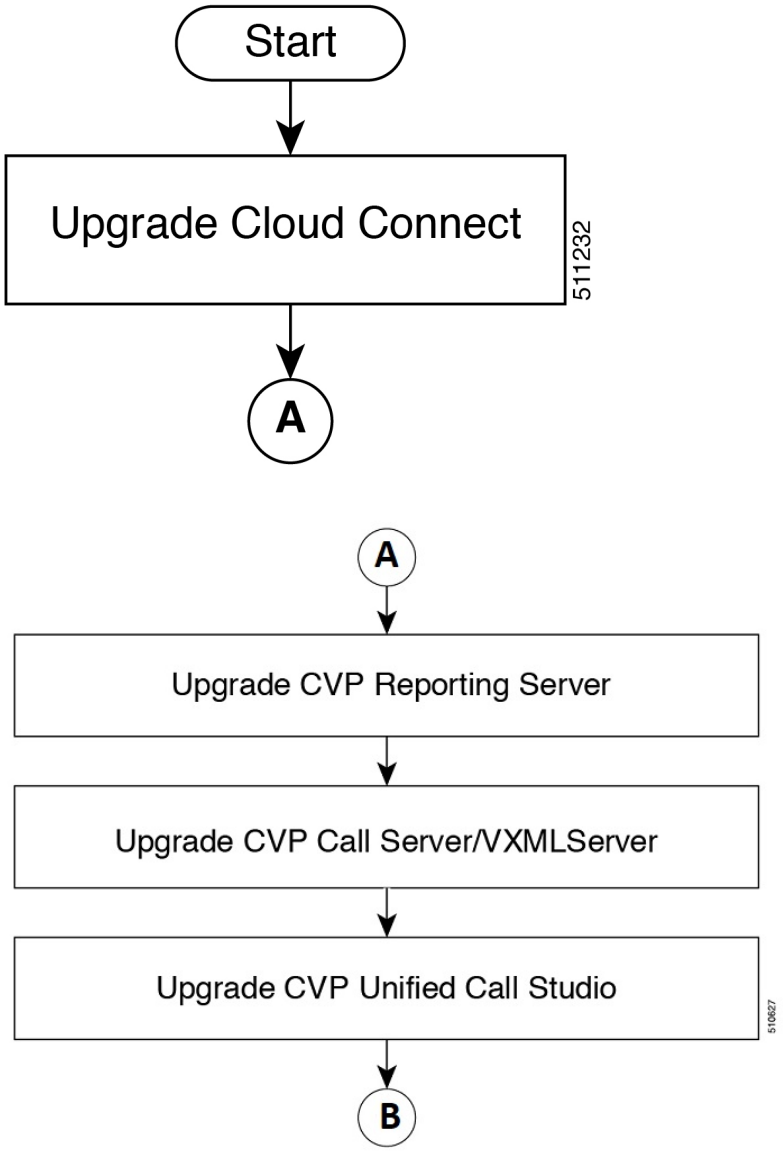


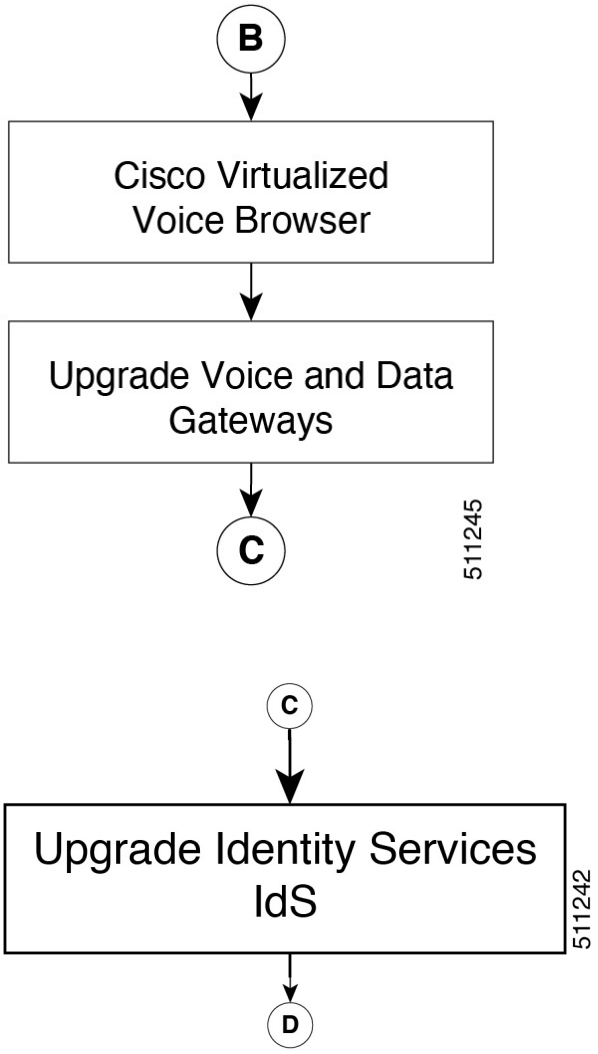
Upgrade Flowcharts for 4000 Agents and above Deployments

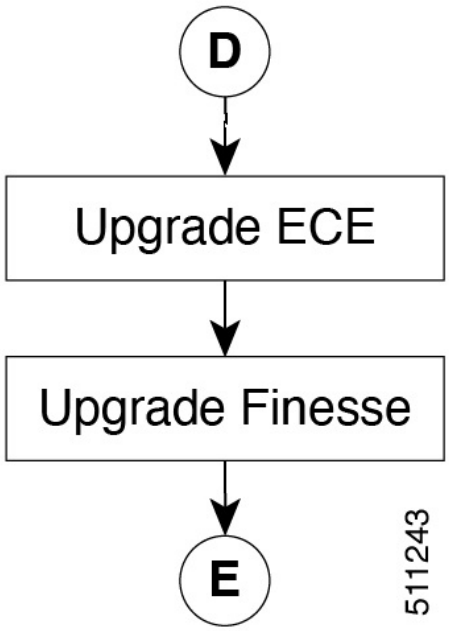
The following diagram illustrates the solution-level upgrade flow for the Packaged CCE 4000 Agents and above Deployment solution upgrade.

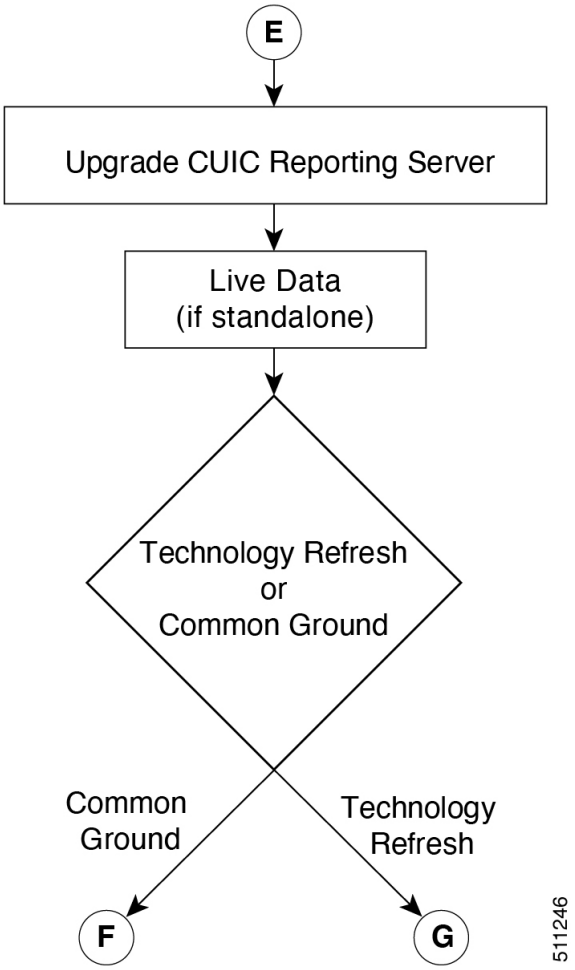


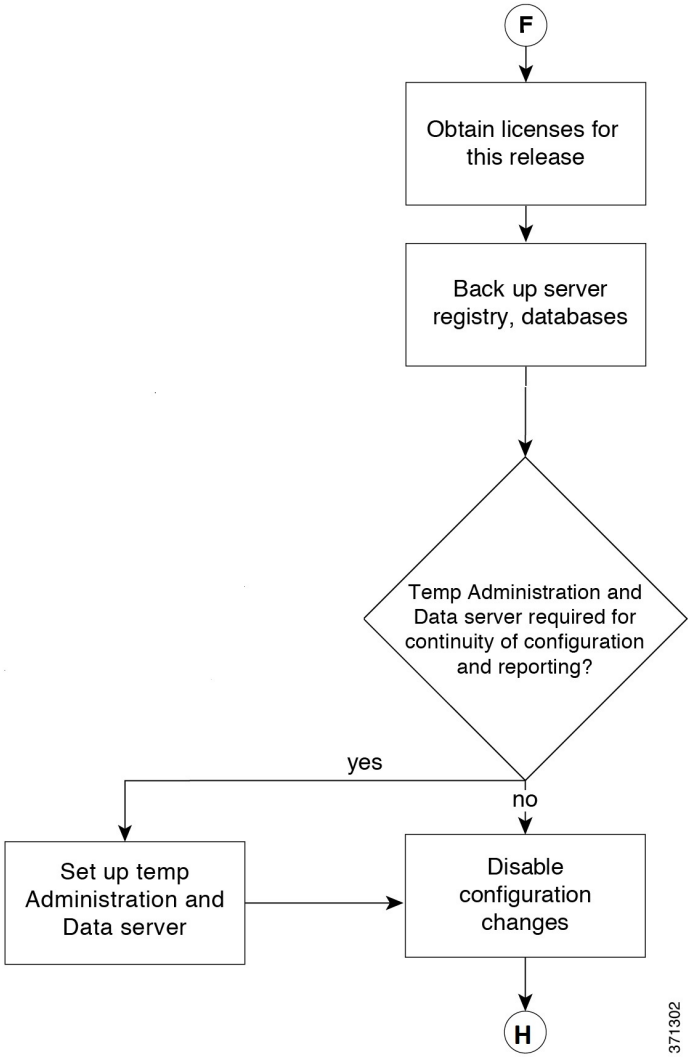
The following diagrams illustrate the stages of the component-level upgrade flows for the Packaged CCE 4000 Agents and above Deployment solution upgrade. Each diagram covers one of the stages. The letter at the end of each flow indicates the start of the next flow that you are required to perform.

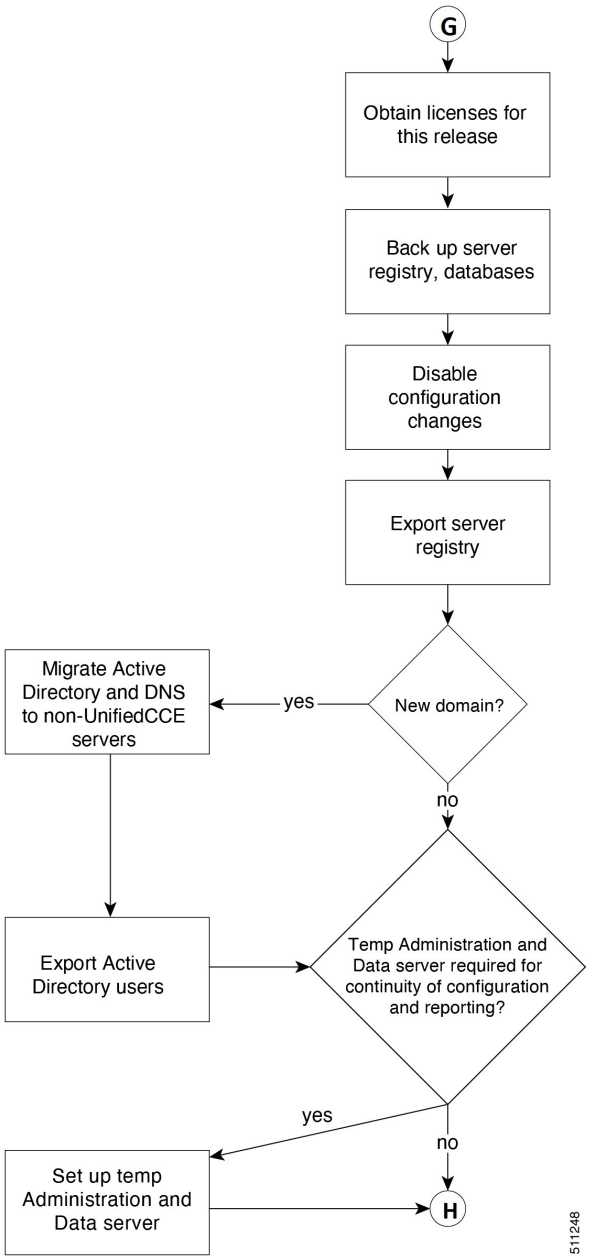

Start
Upgrade Cloud Connect
511232
A
A
Upgrade CVP Reporting Server
Upgrade CVP Call Server/VXMLServer
Upgrade CVP Unified Call Studio
510627
B

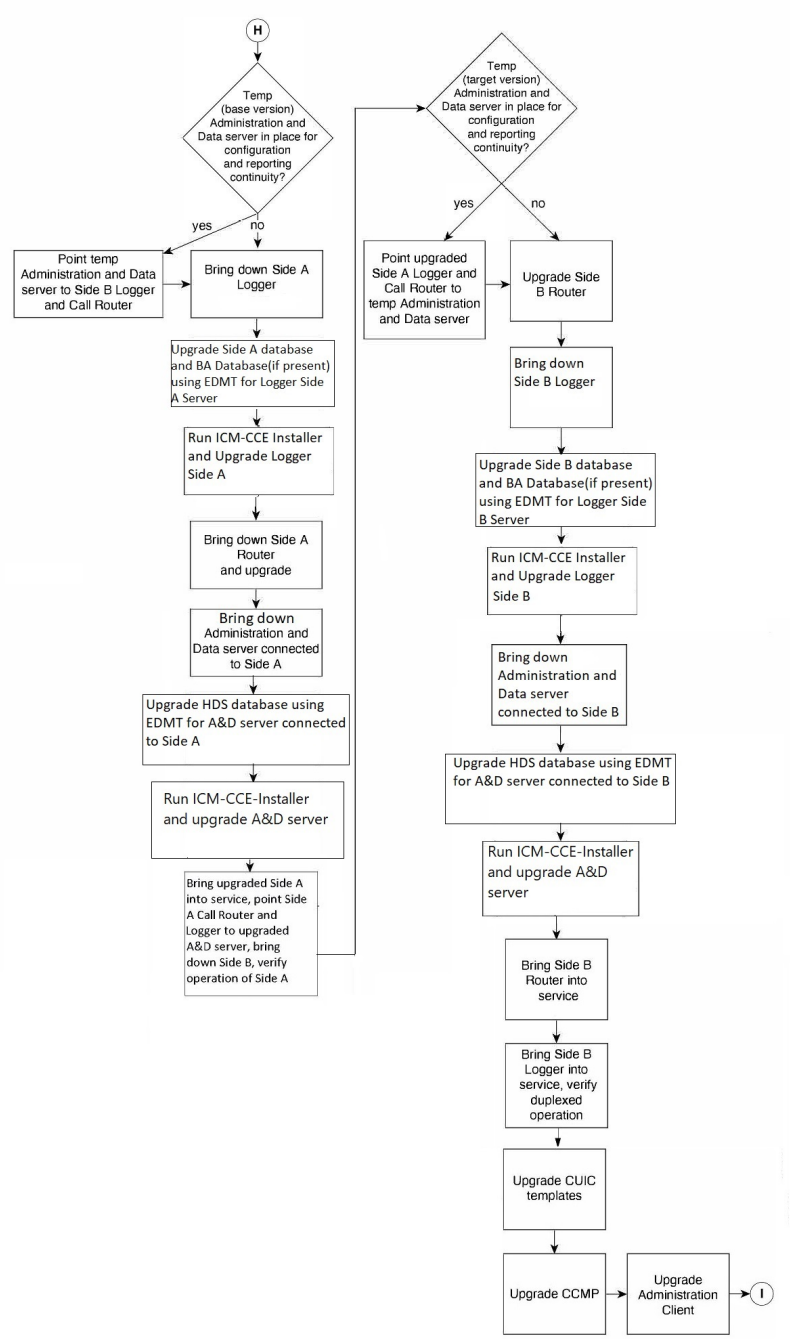

B
Cisco Virtualized Voice Browser
Upgrade Voice and Data Gateways
C
511245
C
Upgrade Identity Services IdS
511242
D

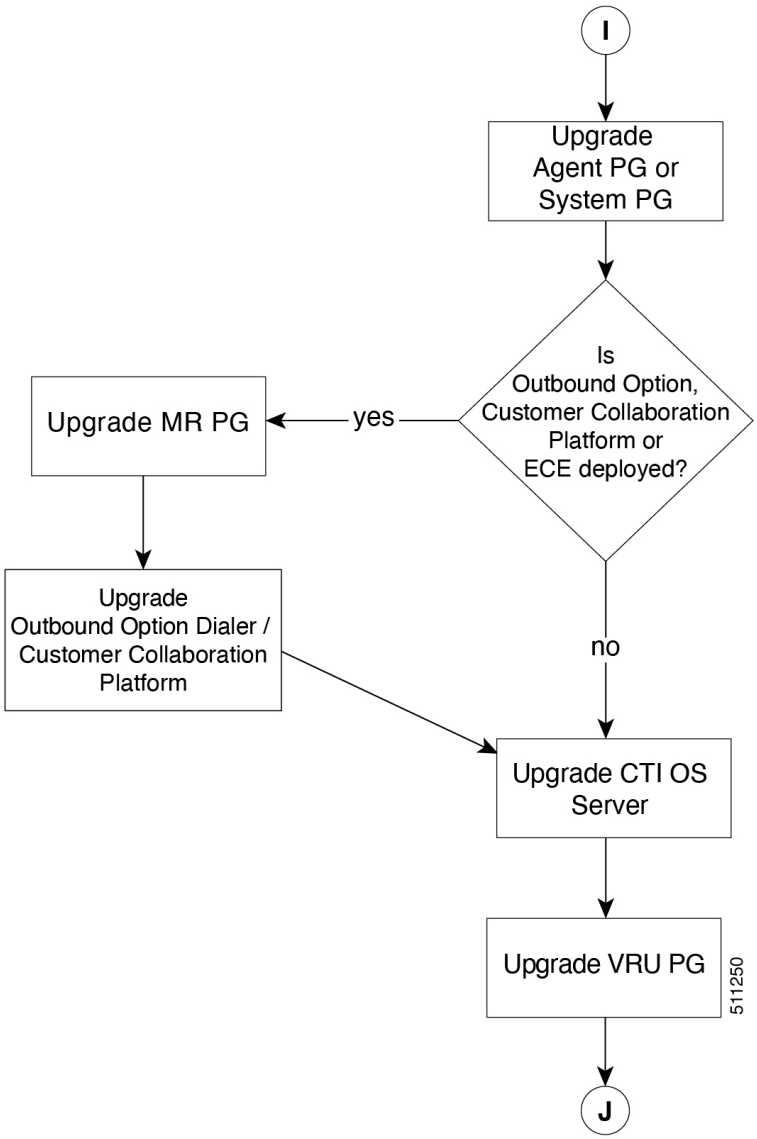

D
Upgrade ECE
Upgrade Finesse
E
511243

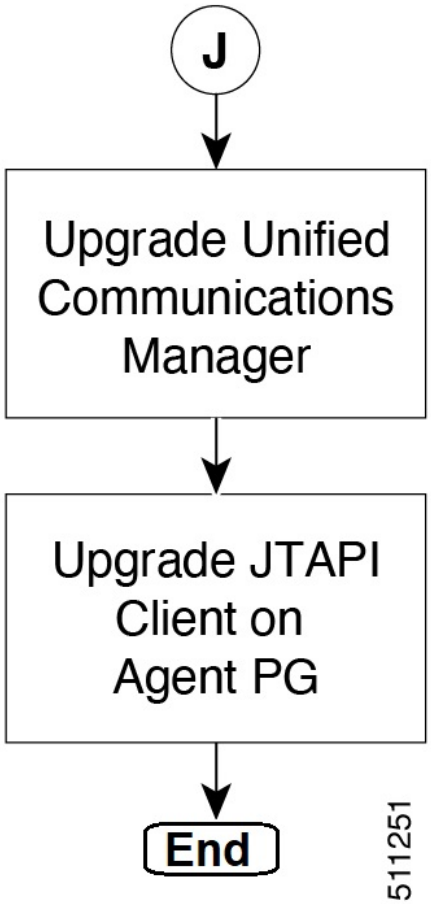

E
Upgrade CUIC Reporting Server
Live Data
(if standalone)
Technology Refresh
or
Common Ground
Common
Ground
Technology
Refresh
F
G
511246


F
Obtain licenses for this release
Back up server registry, databases
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
Disable configuration changes
H
371302


G
Obtain licenses for this release
Back up server registry, databases
Disable configuration changes
Export server registry
New domain?
yes
Migrate Active Directory and DNS to non-UnifiedCCE servers
no
Export Active Directory users
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
H
511248


H
Temp (base version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point temp Administration and Data server to Side B Logger and Call Router
Bring down Side A Logger
Upgrade Side A database and BA Database(if present) using EDMT for Logger Side A Server
Run ICM-CCE Installer and Upgrade Logger Side A
Bring down Side A Router and upgrade
Bring down Administration and Data server connected to Side A
Upgrade HDS database using EDMT for A&D server connected to Side A
Run ICM-CCE-Installer and upgrade A&D server
Bring upgraded Side A into service, point Side A Call Router and Logger to upgraded A&D server, bring down Side B, verify operation of Side A
Temp (target version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point upgraded Side A Logger and Call Router to temp Administration and Data server
Upgrade Side B Router
Bring down Side B Logger
Upgrade Side B database and BA Database(if present) using EDMT for Logger Side B Server
Run ICM-CCE Installer and Upgrade Logger Side B
Bring down Administration and Data server connected to Side B
Upgrade HDS database using EDMT for A&D server connected to Side B
Run ICM-CCE-Installer and upgrade A&D server
Bring Side B Router into service
Bring Side B Logger into service, verify duplexed operation
Upgrade CUIC templates
Upgrade CCMP
Upgrade Administration Client
I


I
Upgrade Agent PG or System PG
Is Outbound Option, Customer Collaboration Platform or ECE deployed?
yes
Upgrade MR PG
Upgrade Outbound Option Dialer / Customer Collaboration Platform
no
Upgrade CTI OS Server
Upgrade VRU PG
J
511250



Silent Upgrade

There are situations when silent upgrade can be used in running an installation wizard. You can run a silent installation while performing a fresh install or an upgrade.

For more information, see Silent Installation, on page 183.

Upgrade CCE Minor/Maintenance Release Software

To perform the upgrade from CCE 12.5(x) or CCE 12.6(1) release, do the following:

Procedure

Step 1 Log in to your system using domain credentials with administrative privileges.

Step 2 Launch the CCE 12.6(2) installation wizard. Click **Next** to proceed.

Step 3 Select the radio button to accept the license agreement and click **Next**.

Step 4 Click **Install** to begin the installation.

Step 5 Select the radio button to restart the system and click **Finish**.

Custom Truststore to Store Component Certificates

Starting Unified CCE 12.6(x), a new custom truststore is created under the Unified ICM Installation directory `<ICM install directory>\ssl\cacerts` to store all the component certificates. With this new custom truststore, you don't need to export and import the certificates each time Java is updated in the system.

After upgrading from Unified CCE 12.5(x) to Unified CCE 12.6(x), you should export the certificates from the Java truststore to the custom truststore under the Unified ICM Installation directory `<ICM install directory>\ssl\cacerts`.

Export the certificate from the Java truststore:

- Run the command at the command prompt: `cd %JAVA_HOME%\bin`.

Important Use CCE_JAVA_HOME if upgrading from Unified CCE 12.5(1a) or Unified CCE 12.5(1) with ES55 (mandatory OpenJDK ES).

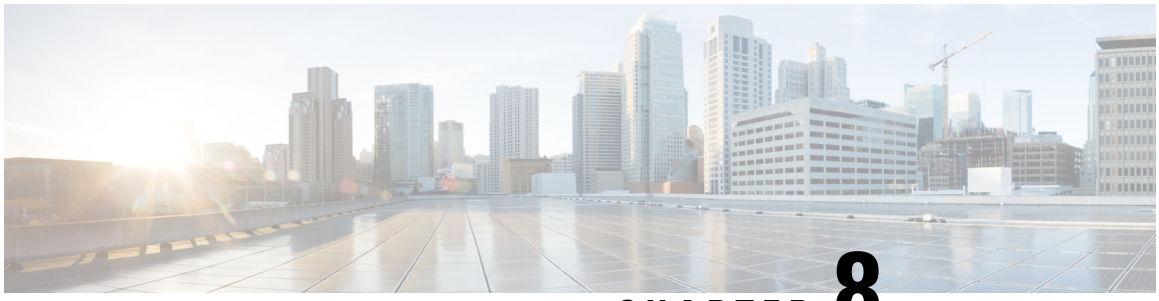
- Export the certificates of all the components imported into the truststore.

  The command to export the certificates is *keytool -export -keystore <JRE path>\lib\security\cacerts -alias <alias of the component> -file <filepath>.cer*
- Enter the truststore password when prompted.

Import the certificate to the custom truststore:

- Run the command at the command prompt: `cd %CCE_JAVA_HOME%\bin`.
- Import the certificates for all the components that you exported from the Java truststore.

  The command to import certificates is *keytool -import -keystore <ICM install directory>\ssl\cacerts -file <filepath>.cer -alias <alias>*.
- Enter the truststore password when prompted.
- Enter 'yes' when prompted to trust the certificate.



CHAPTER 8

Common Ground Upgrade Process

Upgrade Path

The supported upgrade paths to Packaged CCE 12.6(2) are as follows:

- Packaged CCE 12.5(1) to Packaged CCE 12.6(2). EDMT is not required during this upgrade process. If Windows and SQL platform upgrade is involved during this upgrade process, refer to the Technology Refresh Upgrade Process section for details on using EDMT.
- Packaged CCE 12.5(2) to Packaged CCE 12.6(2). EDMT is not required during this upgrade process.
- Packaged CCE 12.6(1) to Packaged CCE 12.6(2). EDMT is not required during this upgrade process.
- Packaged CCE 12.0(1) to Packaged CCE 12.5(1) with inline upgrade to Packaged CCE 12.6(2) using Common Ground or Technology Refresh upgrade. Use EDMT during this upgrade process.

Note Use 12.5(x) EDMT to upgrade from Packaged CCE 12.0(1) to Packaged CCE 12.5(1).

Prerequisites and Important Considerations

- After you begin the migration and upgrade process, you cannot back out of it. If you want to go back to the previous release, you must restore your VMs from your backup.
- You can upgrade only to Cisco Packaged CCE 2000 Agents deployment, Release 12.0(1) from Release 11.5(x), or 11.6(x) directly. To upgrade from the releases 11.0(x), you must first upgrade to 11.5 and then upgrade to 12.0. To upgrade from releases earlier than 11.0(1), you must first upgrade to 11.0(1) and then upgrade to 11.5(1).

- You can upgrade to Cisco Packaged CCE 2000, 4000, and 12000 Agent deployments as per the supported upgrade path.
- Before you upgrade the Cisco VOS-based servers such as the Live Data server, check the **Check and upgrade VMware Tools before each power on** box in the VM's **Options** > **Edit Settings**.

  For more information on VMware Tools upgrade, see the VMware documentation.
- Before upgrading, close all the open Microsoft Windows Event Viewer instances. This prevents an installation failure with an error that the following DLLs are locked:
  - icrcat.dll
  - icrmsgs.dll
  - snmpeventcats.dll
  - snmpeventmsgs.dll

  If the failure occurs, close the Event Viewer and retry the installation. If the failure persists, restart the Microsoft Windows Event Log service.
- This release contains an updated database schema. During the upgrade process, perform a schema upgrade using the Enhanced Database Migration Tool (EDMT).

  For the upgrade utilities, see https://software.cisco.com/download/type.html?mdfid=268439622
- Make sure that you have backups of all components in both Side A and Side B before you begin your upgrade. You can take a snapshot of the virtual machines on which you are performing the upgrade.
- After you configure the servers, you can move the VMs to the servers and complete the common ground upgrade.
- Optionally, you can stage the Unified CCE Rogger off box before you begin the migration and upgrade to lessen your downtime.
- If you already have a Customer Collaboration Platform added in the remote site, delete Customer Collaboration Platform from the remote site and add it as an External Machine in the main site. For more information on how to delete and add an external machine, see the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.
- Make sure that you are running the minimum supported version of ESXi. For information about supported ESXi versions, see the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html.
- In the Unified CCE Administration console, departments cannot be named `Global` or `Service`. If you have already created departments with these names, update the department names before upgrading ECE.
- Following the upgrade of Packaged CCE, wait for a few minutes for the system to finish loading before logging in to the Unified CCE Administration console.

NTP Configuration Requirements

Packaged CCE relies on time synchronization. Properly configuring NTP is critical for reliability of reporting data and cross-component communication. It's important to implement the requirements outlined in NTP and Time Synchronization, on page 7.

Upgrade Considerations

Update VM Properties

Rather than re-create the VMs in the new version of the OVA, you can manually update the VM properties to match the new OVA. Before you upgrade the CCE or Cloud Connect components, update the properties of each VM to match the appropriate OVA, as follows:

1. Stop the VM.
2. Update the properties of each VM to match the properties of the appropriate OVA. Check the *Virtualization for Packaged Cisco Contact Center Enterprise* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html for descriptions of each OVA. Save your changes.

   See https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-cloud-connect.html for details on Cloud Connect.
3. Restart the VM.

Caution Be careful when you upgrade the virtual machine network adapters. Done incorrectly, this upgrade can compromise the fault tolerance of your Cisco Contact Center.

For version-specific information on the VM properties in an OVA, Check the *Virtualization for Packaged Cisco Contact Center Enterprise* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html for descriptions of each OVA.

SQL Security Hardening

You can optionally apply SQL security hardening when running the installer. If your company employs custom security policies, bypass this option. Most other deployments benefit from SQL security hardening.

Note During Unified CCE installation on to Windows Server 2019 and SQL Server 2019, you should not select SQL Server Security Hardening optional configuration as a part of the installation. You can apply the SQL Security Hardening post installation using the Security Wizard tool.

For more information about SQL security hardening, see the *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Self-signed Certificate for Unified CCE Web Application

Note As part of the upgrade of Unified CCE servers, self-signed certificates employed by Unified CCE web applications such as Unified CCE web administration tool and Websetup, may get regenerated. You must add the new certificates to the trust list on the appropriate end devices.

Upgrade Tools

During the upgrade process, use the following tools as required:

- ICM12.6.2.exe—The Unified CCE patch installer. It copies all files into relevant folders, updates the registries, and installs needed third-party software such as JRE, Apache Tomcat, and Microsoft .NET Framework.
- Enhanced Database Migration Tool (EDMT)—A wizard application that is used for all upgrades to migrate the HDS, Logger, and BA databases during the upgrade process.

  You can download the EDMT from Cisco.com by clicking **Cisco Enhanced Data Migration Tool Software Releases**.

  The prerequisites for running EDMT are:

  - EDMT requires Microsoft® ODBC Driver 17 for SQL Server® and Visual C++ Redistributable for Visual Studio 2015 (or higher). The latest version of these packages can be downloaded from the Microsoft website. However, a copy of the same is also available in the **Prerequisites** folder of EDMT.

  The EDMT displays status messages during the migration process, including warnings and errors. Warnings are displayed for informational purposes only and do not stop the migration. On the other hand, errors stop the migration process and leave the database in a corrupt state. If an error occurs, restore the database from your backup, fix the error, and run the tool again.

Note

- You can select either **SQL Server Authentication** or **Windows Authentication** during database migration. In certain scenarios, for example, where the source and destination machines are in different domains, **SQL Server Authentication** can be used.
- If you are configuring SQL services to run as Virtual account (NT SERVICE) or Network Service account (NT AUTHORITY\NETWORK SERVICE), you must run EDMT as an administrator.
- The installer, not the EDMT, upgrades the AW database for the Administration & Data Server.

Packaged CCE 2000 Agents Deployment

Common Ground Upgrade Process

Redundant Upgrade Workflow

Note The redundant upgrade workflow is applicable to the solution deployments with Main site only.

Important The upgrade requires four maintenance windows:

- First maintenance window to shut down services on Side A and upgrade Side A
- Second maintenance window in the middle of the upgrade to cut over from Side B to Side A. You must bring down Side B before you bring up Side A.
- Third maintenance window after you upgrade Side B to synchronize Side A to Side B.
- Fourth maintenance window to upgrade Cisco Unified Communications Manager (CUCM).

Common Preupgrade Tasks

Perform the tasks in the following table in the order that they are listed.

Task
During upgrades, when the system first migrates your existing ECC variables to the Default payload, it does not check the CTI message size limit. The member names might exceed the extra 500 bytes that is allocated for ECC payloads to a CTI client. Manually check the CTI Message Size counter in the Expanded Call Variable Payload List tool to ensure that the Default payload does not exceed the limit. If the Default payload exceeds the limit, modify it to meet the limit.
Take a snapshot of each virtual machine you are upgrading from the VMware vSphere Client.

Preupgrade of Side A

Task
Disable configuration changes on the Unified CCE. Change the following registry key to 1: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance`
Reverse the Cisco IOS Enterprise Ingress Voice Gateway dial-peer priority configuration so that calls are sent to the Side B Unified CVP server.

Task
Using **Unified CCE Service Control**, stop all Unified CCE services on the Unified CCE servers that you are upgrading, and set the startup type to **Manual**. **1.** Side A Unified CCE Rogger **2.** Side A Unified CCE AW-HDS-DDS **3.** Side A PG **4.** External HDS with Side A as the Central Controller preferred side (if used) Verify that the services are stopped.

Upgrade Side A

Before you begin, check the following to confirm that call activity has ended on Side A:

- On the Unified CVP Statistics portal, make sure that no Side A ports are in use.
  1. Navigate to **Unified CCE Administration** > **Infrastructure** > **Inventory**.
  2. Click the **Statistics** icon to view the statistics for CVP machine.

     The **Infrastructure** tab for Call Server displays the port usage information.
- In the Unified Communications Manager RTMT tool, check that phones have migrated to Side B.

Place upgrade media ISOs on local data stores. Make sure to remove them when the upgrade is complete.

Task
Upgrade to a supported version of ESXi version, if needed. For the supported ESXi versions for this release, see the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html. If you are using a supported ESXi version and want to upgrade to different supported ESXi version, you can upgrade now, or after the Packaged CCE upgrade is complete. See Upgrade VMware vSphere ESXi, on page 207.
Upgrade Unified CVP Server. For more details, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html. After upgrading the Unified CVP server, add the CVP machine to the domain. For more information, see Add Machine to Domain, on page 179.

Task
Upgrade all the Cisco Voice Gateways one after another. See Upgrade Cisco Voice Gateway IOS Version, on page 207. The IOS version of the Cisco Voice Gateways must be upgraded to the minimum version required by Packaged CCE 12.0(1). For more details, see the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for IOS support information.
Upgrade all the Cisco Virtualized Voice Browsers one after another. For more details, see the *Installation and Upgrade Guide for Cisco Virtualized Voice Browser* at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-installation-guides-list.html .
Upgrade the publishers/primary nodes of Cisco Finesse. For details, see the *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html
Upgrade the publishers/primary nodes of Cisco Unified Intelligence Center with Live Data and Identity Service (IdS). For details, see the *Installation and Upgrade Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html
Back up and export the Side A SQL database and the Outbound Option (if used) in Rogger VM. • Use Microsoft SQL Server Backup and Restore utilities for the back up. • Note the HDS customizable values. • Copy the backup files to a shared location.
Run the Enhanced Database Migration Tool on rogger, external HDS (if used), and non-external HDS to perform a schema upgrade during the upgrade process. See Run EDMT , on page 206.
If you use Outbound Option High Availablity, for the enhancements in Outbound Option High Availability to work effectively, disable Outbound Option High Availablity before the logger upgrade and then enable it after the upgrade. For details, see Disable Outbound Options High Availability (If Applicable), on page 210
Run the Unified CCE Release installer on the Side A Unified CCE Rogger. See Install Cisco Unified Contact Center Enterprise, on page 183.
Run the Unified CCE Release installer on the Side A Unified CCE AW-HDS-DDS. See Install Cisco Unified Contact Center Enterprise, on page 183.
Run the Unified CCE installer on the Side A PG. See Install Cisco Unified Contact Center Enterprise, on page 183.

Task
(Optional) Upgrade the External HDS associated with Side A (if used) Run the Unified CCE Release installer the External HDS associated with Side A. See Install Cisco Unified Contact Center Enterprise, on page 183.
(Optional) Upgrade ECE. See *Enterprise Chat and Email Installation Guide (for Packaged Contact Center Enterprise)* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html

Side A Postupgrade Tasks

You must bring down Side B before you bring up Side A. Perform these tasks during maintenance window to cut over from Side B to Side A.

Task
Reverse the Cisco IOS Enterprise Ingress Voice Gateway dial-peer priority configuration so that calls are sent to the Side A Unified CVP server first and then to Side B.
(Optional) If you use Outbound Option High Availablity, enable Outbound Option High Availablity in the Web Setup tool. For details, see the *Configure the Logger for Outbound Option* topic in the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html
Using Unified CCE Service Control, stop all Unified CCE services on the Side B Unified CCE servers that you are upgrading, and set the startup type to **Manual**. **1.** Side B Unified CCE Rogger **2.** Side B Unified CCE AW-HDS-DDS **3.** Side B PG **4.** External HDS with Side B as the Central Controller preferred side (if used) Verify that the services have stopped.
Perform Database Performance Enhancement of TempDB, Logger Database, and AW-HDS Database. For more information, see Database Performance Enhancement, on page 210.
Using Unified CCE Service Control, start all Unified CCE services on the Side A Unified CCE servers that you are upgrading, and set the startup type to **Automatic**. **1.** Side A Unified CCE Rogger **2.** Side A Unified CCE AW-HDS-DDS **3.** Side A PG **4.** External HDS with Side A as the Central Controller preferred side (if used) Verify that the services have started.

Task
Set the following registry key to 0 on Side A Unified CCE Rogger: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance`
Direct agents to sign into the Side A Finesse Primary node.

Preupgrade of Side B

Task
Disable configuration changes on the Side B Unified CCE Rogger. Change the following registry key to 1: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterB\Router\CurrentVersion\Configuration\Global\DBMaintenance`

Upgrade Side B

Before you begin, check the following to confirm that call activity has ended on Side B:

- On the Unified CVP Statistics portal, make sure that no Side B ports are in use.
  1. Navigate to **Unified CCE Administration** > **Infrastructure** > **Inventory**.
  2. Click the **Statistics** icon to view the statistics for CVP machine.

     The **Infrastructure** tab for Call Server displays the port usage information.
- In the Unified Communications Manager RTMT tool, check that phones have migrated to Side A.

Place the upgrade media ISOs on local data stores. Ensure that you remove the media ISOs when the upgrade is complete.

Task
Upgrade to a supported version of ESXi version, if needed. For the supported ESXi versions for this release, see the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html. If you are using a supported ESXi version and want to upgrade to different supported ESXi version, you can upgrade now, or after the Packaged CCE upgrade is complete. See Upgrade VMware vSphere ESXi, on page 207.
Upgrade the Unified CVP Reporting Server See Upgrade Unified CVP Reporting Server, on page 207 After upgrading the Unified CVP Reporting server, add the CVP Reporting server to the domain. For more information, see Add Machine to Domain, on page 179.

Task
Upgrade Unified CVP Server. For more details, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html . After upgrading the Unified CVP server, add the CVP machine to the domain. For more information, see Add Machine to Domain, on page 179.
Upgrade the subscribers/secondary nodes of Cisco Finesse. For details, see the *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html
Upgrade the subscribers/secondary nodes of Cisco Unified Intelligence Center with Live Data and Identity Service (IdS). For details, see the *Installation and Upgrade Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html
Back up and export the Side B SQL database and the Outbound Option (if used) database in the Rogger VM. • Use Microsoft SQL Server Backup and Restore utilities for the back up. • Note the HDS customizable values. • Copy the backup files to a shared location.
Run the Enhanced Database Migration Tool on rogger, external HDS (if used), and non-external HDS to perform a schema upgrade during the upgrade process. See Run EDMT , on page 206.
If you use Outbound Option High Availablity, for the enhancements in Outbound Option High Availability to work effectively, disable Outbound Option High Availablity before the logger upgrade and then enable it after the upgrade. For details, see Disable Outbound Options High Availability (If Applicable), on page 210
Run the Unified CCE installer on the Side B Unified CCE Rogger. See Install Cisco Unified Contact Center Enterprise, on page 183
Run the Unified CCE installer on the Side B Unified CCE AW-HDS-DDS. See Install Cisco Unified Contact Center Enterprise, on page 183
Run the Unified CCE installer on the Side B PG. See Install Cisco Unified Contact Center Enterprise, on page 183
(Optional) Upgrade the External HDS associated with Side B (if used) See Install Cisco Unified Contact Center Enterprise, on page 183

Task
(Optional) Upgrade ECE. See *Enterprise Chat and Email Installation Guide (for Packaged Contact Center Enterprise)* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html.

Sync Side A to Side B

Perform these tasks during the third maintenance window to sync Side A and Side B.

Task
Set the following registry key to 0 on either the Side B Unified CCE Rogger: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router B\Router\CurrentVersion\Configuration\Global\DBMaintenance`
(Optional) If you use Outbound Option High Availability, enable Outbound Option High Availability in the Web Setup tool. For details, see the *Configure the Logger for Outbound Option* topic in the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html
On each of the following VMs, select **Unified CCE Service Control** on the desktop. Start the Unified CCE services and change Startup to Automatic, in this order: **1.** Side B Unified CCE Rogger **2.** Side B Unified CCE AW-HDS-DDS **3.** Side B PG **4.** External HDS with Side B as the Central Controller preferred side (if used) Verify that the services are started.
Perform Database Performance Enhancement of TempDB, Logger Database, and AW-HDS Database for Side B. For more information, see Database Performance Enhancement, on page 210.
Run the **UserRoleUpdate.PS1** tool in Powershell in any one of the distributor machines. This ensures that the User Role is updated in the database for the existing users. To download **UserRoleUpdate.PS1** script, go to the link https://software.cisco.com/download/home/268439622/type and select **User Role Update Bulk Tool** from the list. Download the file **UserRoleUpdateScript_1201.zip** and extract the script.

Postupgrade Tasks

Task
Bring back Side A and Side B to call flow
Change the Cisco IOS Enterprise Voice Gateway dial-peer configuration to point to both Side A and Side B Unified CVP Servers.

Upgrade UCM in Side A and Side B

Perform these tasks to upgrade UCM in both Side A and Side B.

Important Upgrade of CUCM requires a minimal maintenance window.

Step	Task
1	Upgrade the Side A CUCM Publisher and Subscriber. For detailed upgrade steps, see the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.
2	Upgrade JTAPI on the Side A PG. See Upgrade Cisco JTAPI Client on PG, on page 209. **Important** If you are installing CUCM 12.5 and above, download the Cisco JTAPI Client from CUCM and install it on the PG machine. See Install Cisco JTAPI Client on PG, on page 208.
Side B	
3	Upgrade the Side B CUCM Subscriber. For detailed upgrade steps, see the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html. **Important** The CUCM Publisher upgrade must be complete and the 12.5 software must be active before you upgrade the CUCM Subscriber.
4	Upgrade JTAPI on the Side B PG. See Upgrade Cisco JTAPI Client on PG, on page 209. **Important** If you are installing CUCM 12.5 and above, download the Cisco JTAPI Client from CUCM and install it on the PG machine. For more information, see Install Cisco JTAPI Client on PG, on page 208.

Cisco Unified Communications Manager 12.5 - Steps After Upgrade

Perform the following tasks if Cisco Unified Communications Manager (CUCM) is on-box and if you have upgraded to CUCM 12.5 and above on the Cisco UCS C240 M4SX server. This procedure is performed on the main site.

Note Do not change the IP address of both CUCM Publisher and Subscriber.

Step	Task
1	Move CUCM Publisher and Subscriber from Side A host to a different host.

Step	Task
2	Move CUCM Subscriber from Side B host to a different host.
3	Delete CUCM references from all the location configurations.
4	Add CUCM Publisher as an external machine to the main site of the **Packaged CCE Inventory**.

Multistage Upgrade Workflow

Note The multistage upgrade workflow is applicable for solution deployments with both main site and remote site (if available).

A Unified CCE solution upgrade likely involves a multistage process; components are grouped in several stages for upgrading. At each stage in the upgrade, the upgraded components must interoperate with components that haven't yet been upgraded to ensure the overall operation of the contact center. Therefore, it's important to verify this interoperability during the planning stages of the upgrade.

Before upgrading a production system, perform the upgrade on a lab system that mirrors your production system to identify potential problems safely.

The following table details the required sequence for upgrading Packaged CCE 2000 Agent Deployments components, and the minimum component groupings that must occur together within each stage. Follow each stage to completion within each maintenance window. Each maintenance window must accommodate any testing required to ensure system integrity and contact center operation.

You can combine more than one complete stage into a single maintenance window, but you can't break any one stage into multiple maintenance windows.

The sequence of upgrade is as per the Upgrade Flowcharts for 2000 Agent Deployments, on page 39. Upgrade the Unified CCE components as follows:

Note

- Upgrade Agent Desktop, CUIC, Live Data, and IdS server along with the Unified CCE Central Controller upgrade.
- After upgrading Finesse, IdS, and CUIC, import the IdS certificates to the Finesse and CUIC servers.
- Run Stage 3 and Stage 4 upgrades in the same maintenance window.

Note Components of the same type within a particular stage of the upgrade sequence should be on the same application and operating system version before proceeding to the next stage in upgrade sequence.

Stage	Component Group	Components	Notes
1	Platform Orchestration, Hybrid Features	Cloud Connect	In 12.6(2), the RAM requirement for Cloud Connect has changed. See the **Update VM Properties** section in the Upgrade Considerations, on page 61 for instructions on increasing hard disk and RAM before upgrading Cloud Connect. If you don't have Cloud Connect in your environment, and you use any Hybrid feature or Orchestration, fresh install Cloud Connect. For fresh install instructions, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
2	Queuing and self-service	Cisco Unified Customer Voice Portal (CVP) (Reporting Server, Call Server/VXMLServer, Unified Call Studio)	You must upgrade all sites before proceeding to the next stage. For more information, see *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.
3	Gateways	• IOS Gateways (If used for ingress access only. If used for Outbound Option Dialer, see Stage 5.) • IOS VXML Gateways • Cisco Virtualized Voice Browser	

Stage	Component Group	Components	Notes
4	Agent/Supervisor Desktop, Central Controller, and Reporting	• ECE • Cisco Finesse • Unified CCE Rogger • Admin & Data server (AW/HDS/DDS) • CUIC-LD-IDS • CUIC Reporting Templates • CCMP	

Stage	Component Group	Components	Notes
			• In 12.6(2), the RAM requirement for Live Data VM has changed. Refer to the **Update VM Properties** section in Upgrade Considerations, on page 61 to update the Live Data VM properties before you upgrade the component. • After you upgrade AW, import the self-signed certificate of all solution components (if applicable) to all AWs. • If you are using AppDynamics for performance monitoring on 12.6(1), then before upgrading the Distributor node from 12.6(1) to 12.6(2), disable AppDynamics performance monitoring on 12.6(1) and re-enable it after upgrading to 12.6(2). If AppDynamics performance monitoring is not disabled before the Distributor node is upgraded to 12.6(2), then post upgrade, restart the Distributor node. • After you upgrade Finesse to Release 12.6(x) , to load any gadgets to Finesse, you must first import all self-signed certificates (if applicable) to Finesse. After upgrading Finesse to 12.6(2), ensure that both ECDSA and RSA valid certificates are available in the certificate store in PG. If not, you must export the Finesse Tomcat certificates and import them to CTI Gateway (CG) and Peripheral Gateway (PG) systems. For more information, refer to the *Add Certificate for HTTPS Gadget* section in the Cisco Finesse Administration Guide. **Note** After upgrading cuic-ld-ids to 12.6, run the **utils finesse layout updateCuicGadgetUrl** command to update the gadget URL. For more information about Finesse, see *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html. For more information about ECE, see https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html • Cisco IdS 12.6(2) upgrade requires all SSO clients to log out from SSO, before any of the upgraded nodes is brought online. To avoid this requirement, it's recommended that you install 12.6(2) ES02 on the upgraded node and wait for the access token to expire before commencing the secondary node upgrade.

Stage	Component Group	Components	Notes
			Without installing the 12.6(2) ES02, graceful shutdown feature will not be available for Cisco IdS 12.6(2) upgrade. You can view the duration of access token expiry in the IdS administration portal under **Settings** > **Security** > **Tokens** > **Access Token Expiry**. Deployments using VPN-less access to Finesse desktop should also upgrade the reverse proxy to 12.6(2) before Cisco IdS is upgraded to 12.6(2). • After you upgrade Live Data (LD), you must enable CORS on the LD box for Finesse and CUIC. For more information, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html. • After you upgrade LD, you must import the Finesse certificate to LD.
5	Peripherals	• Agent (Unified Communications Manager) PG • CTI Server • Outbound Option Dialer and SIP IOS Gateway	You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window.
6	Peripherals	• MR PG, VRU PG • CRM connector	You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window.
7	Call Processing	• Cisco Unified Communications Manager (Unified Communications Manager) • JTAPI on Agent (Unified Communications Manager) PG	You must install JTAPI client only when you upgrade to UCM 12.5. If you upgrade to CUCM 12.5 on the M4 servers, ensure that you deploy CUCM off-box. For more information, refer to *Virtualization for Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html.

Hardware Refresh with Common Ground Upgrade

If you are performing a hardware refresh as part of the upgrade process, you must first prepare the target servers as described in the following documents:

- *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html

After you configure the servers, you can move the VMs to the servers and complete the Common Ground Upgrade Process, on page 63.

As a part of hardware refresh, if you are migrating from existing Cisco UCS C240 M3S/Cisco UCS C240 M4SX to Cisco UCS C240 M5SX or Cisco UCS C240 M6SX or Cisco HX220c-M5SX or Cisco HX220c-M6S hardware, perform the following migration steps:

Pre-migration Steps

Step	Task
1	Upgrade to the latest release with the latest ES on old hardware. For upgrade procedure, refer the *Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide Release* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html.
2	Update the annotation of the core VMs as per requirement for Specification Based hardware. See Installation Tasks, on page 15.

Migration Steps

Steps	Task
1	Move the VMs to the target hardware
2	Log in to the Packaged CCE Administration and open the Inventory.
3	Perform the following in the Packaged CCE Inventory: **1.** Click Update Hosts. **2.** Provide ESXI details of the target hardware. **3.** Select the hardware type as **M5 or HX M5 Tested Reference Configuration / Specification Based Configuration**, to migrate to Cisco UCS C240 M5SX or Cisco UCS C240 M6SX or Cisco HX220c-M5SX or Cisco HX220c-M6S hardware. **4.** Complete the wizard. **Note** If CUCM and CVP Reporting Server were on-box in the old hardware, you must add them back as external machines after completing the deployment.

Post-migration Step

Step	Task
1	Complete the common ground hardware upgrade process. See Common Ground Upgrade Process, on page 63.

Packaged CCE 4000 Agents and above Deployment

Common Ground Upgrade Process

Multistage Upgrade Workflow

Note A CCE solution upgrade likely involves a multistage process; components are grouped in several stages for upgrading. At each stage in the upgrade, the upgraded components must interoperate with components that have not yet been upgraded to ensure the overall operation of the contact center. Therefore, it is important to verify this interoperability during the planning stages of the upgrade.

Before upgrading a production system, perform the upgrade on a lab system that mirrors your productionsystem to identify potential problems safely.

The following table details the required sequence for upgrading Packaged CCE 4000 Agent Deployments components, and the minimum component groupings that must occur together within each stage. Follow each stage to completion within each maintenance window. Each maintenance window must accommodate any testing required to ensure system integrity and contact center operation.

You can combine more than one complete stage into a single maintenance window, but you cannot break any one stage into multiple maintenance windows.

The sequence of upgrade is as per the Upgrade Flowcharts for 4000 Agents and above Deployments, on page 47. Upgrade the CCE components as follows:

Note In case of 4K deployment the CCE components consists of Rogger VM instead of Router and Logger VMs.

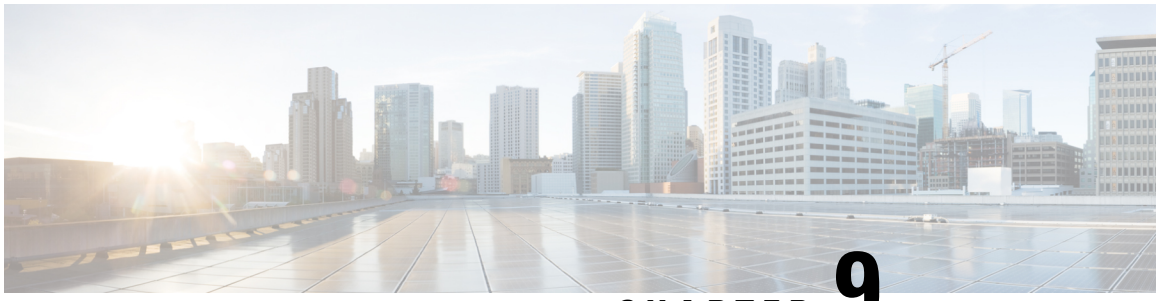
Stage	Component Group	Components	Notes
1	Platform Orchestration, Hybrid Features	Cloud Connect	In 12.6(2), the RAM requirement for Cloud Connect has changed. See the **Update VM Properties** section in the Upgrade Considerations, on page 61 for instructions on increasing hard disk and RAM before upgrading Cloud Connect. If you don't have Cloud Connect in your environment, and you use any Hybrid feature or Orchestration, fresh install Cloud Connect. For fresh install instructions, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html

Stage	Component Group	Components	Notes
2	Queuing and self-service	Cisco Unified Customer Voice Portal (CVP) (Reporting Server, Call Server/VXMLServer, Unified Call Studio)	You must upgrade all sites before proceeding to the next stage. Before you upgrade to Unified CVP 12.6, you must apply the latest ES of Packaged CCE 12.5 . For more information, see *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.
3	Gateways	• IOS Gateways (If used for ingress access only. If used for Outbound Option Dialer, see Stage 8.) • IOS VXML Gateways • Cisco Virtualized Voice Browser	
4	Identity Service	IdS Server	Cisco IdS 12.6(2) upgrade requires all SSO clients to log out from SSO, before any of the upgraded nodes is brought online. To avoid this requirement, it's recommended that you install 12.6(2) ES02 on the upgraded node and wait for the access token to expire before commencing the secondary node upgrade. Without installing 12.6(2) ES02, graceful shutdown feature will not be available for Cisco IdS 12.6(2) upgrade. You can view the duration of access token expiry in the IdS administration portal under **Settings** > **Security** > **Tokens** > **Access Token Expiry**. Deployments using VPN-less access to Finesse desktop should also upgrade the reverse proxy to 12.6(2) before Cisco IdS is upgraded to 12.6(2). For IdS upgrade, see the procedure as documented in the *Upgrades* section of *Unified Intelligence Center Installation and Upgrade Guide* at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html

Stage	Component Group	Components	Notes
5	Agent and supervisor desktops	ECE Cisco Finesse	After you upgrade Finesse to Release 12.6, to load any gadgets to Finesse, you must first import all self-signed certificates (if applicable) to Finesse. For more information about Finesse, see *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html. After upgrading Finesse to 12.6(2), ensure that both ECDSA and RSA valid certificates are available in the certificate store in PG. If not, you must export the Finesse Tomcat certificates and import them to CTI Gateway (CG) and Peripheral Gateway (PG) systems. For more information, refer to the *Add Certificate for HTTPS Gadget* section in the Cisco Finesse Administration Guide. For more information about ECE, see https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html
6	Reporting server	CUIC server	After you upgrade Cisco Unified Intelligence Center (CUIC), you must: • Enable CORS on the CUIC server, and add **`cors allowed_origin`** with the Finesse hostname. • Import LD and Finesse certificates to CUIC. For more information, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html.

Stage	Component Group	Components	Notes
7	Central Controller	• Unified CCE Rogger • Admin & Data server (AW/HDS/DDS) • Standalone Live Data • CUIC Reporting Templates • Administration Client	• After you upgrade AW, import the self-signed certificate of all solution components (if applicable) to all AWs. • If you are using AppDynamics for performance monitoring on 12.6(1), then before upgrading the Distributor node from 12.6(1) to 12.6(2), disable AppDynamics performance monitoring on 12.6(1) and re-enable it after upgrading to 12.6(2). If AppDynamics performance monitoring is not disabled before the Distributor node is upgraded to 12.6(2), then post upgrade, restart the Distributor node. • After you upgrade Live Data (LD), you must enable CORS on the LD box for Finesse and CUIC. For more information, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html. • After you upgrade LD, you must import the Finesse certificate to LD. **Note** For Live Data VM, you have to increase the RAM before upgrading. See https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html
8	Peripherals	• Agent (Unified Communications Manager) PG • CTI Server • CTI OS Server • Outbound Option Dialer and SIP IOS Gateway	• CTI OS Server is applicable only if Avaya PG is used. • You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window.
9	Peripherals	• MR PG, VRU PG • CRM connector	You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window.
10	Agent desktop client software	CTI OS (Agent/Supervisor Desktops)	• CTI OS is applicable only if Avaya PG is used. • You can have many desktops located in many different sites. You can upgrade CTI OS desktops in multiple maintenance windows; the later upgrade stages are not dependent on the completion of this stage.

Stage	Component Group	Components	Notes
11	Call Processing	• Cisco Unified Communications Manager (Unified Communications Manager) • JTAPI on Agent (Unified Communications Manager) PG	You must install JTAPI client only when you upgrade to UCM 12.5. If you upgrade to CUCM 12.5 on the M4 servers, ensure that you deploy CUCM off-box. CUCM 12.5 on-box deployment are only supported for M5 servers. For more information, refer to *Virtualization for Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html.



CHAPTER 9

Technology Refresh Upgrade Process

You can perform Technology Refresh Upgrade as a single-stage upgrade or a multistage upgrade.

- Single-stage upgrade: set up all virtual machines (VMs) required for a Packaged CCE solution (rebuild) on a different hardware.
- Multistage upgrade: set up or upgrade the required set of components on a different hardware.

The tasks involved in the Technology Refresh upgrade are:

- Deploy components as per your requirements.
- Migrate CCE databases using the Enhanced Database Migration Tool (EDMT) and upgrade the CCE components. You can upgrade the other solution components also.
- Update the IP address or hostname of components.
- Synchronize components and complete the upgrade on the destination server.

Upgrade Path

The supported upgrade paths to Packaged CCE 12.6(2) are as follows:

- Packaged CCE 12.5(1) to Packaged CCE 12.6(2). EDMT is not required during this upgrade process. If Windows and SQL platform upgrade is involved during this upgrade process, refer to the Technology Refresh Upgrade Process section for details on using EDMT.
- Packaged CCE 12.5(2) to Packaged CCE 12.6(2). EDMT is not required during this upgrade process.
- Packaged CCE 12.6(1) to Packaged CCE 12.6(2). EDMT is not required during this upgrade process.
- Packaged CCE 12.0(1) to Packaged CCE 12.5(1) with inline upgrade to Packaged CCE 12.6(2) using Common Ground or Technology Refresh upgrade. Use 12.6(x) EDMT during this upgrade process.

Prerequisites and Important Considerations

- You can upgrade to Cisco Packaged CCE 2000, 4000, and 12000 Agent deployments as per the supported upgrade path.
- Components must be upgraded as per the supported versions detailed in the *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.
- Before upgrading the Unified CCE Central Controller, do the following:
  - In the Unified CCE Router of the source server, Disable Configuration Changes, on page 91.
  - Disable Outbound Option High Availability (if applicable) before the logger upgrade. For details, see Disable Outbound Options High Availability (If Applicable), on page 210
- In the Unified CCE Rogger, AW-HDS-DDS, and Peripheral Gateways of the source server, Export the Server Registry, on page 92.
- Before you upgrade the Live Data server, check the **Check and upgrade VMware Tools before each power on** box in the VM's **Options** > **Edit Settings**.

  For more information on VMware Tools upgrade, see the VMware documentation.
- In Technology Refresh upgrade, both source and destination servers must be on the same domain.
- This release contains an updated database schema. During the upgrade process, perform a schema upgrade using the Enhanced Database Migration Tool (EDMT).

  For the upgrade utilities, see https://software.cisco.com/download/type.html?mdfid=268439622
- If you are moving the existing VMs, take the required backups of components on both Side A and Side B before you begin your upgrade. You can take a snapshot of the virtual machines on which you are performing an upgrade.
- If you already have a Customer Collaboration Platform added in the remote site, it is recommended to delete the Customer Collaboration Platform from the remote site and add it as an external machine in the Main site, before upgrade. For more information on how to delete and add an external machine, see the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.
- Make sure that you are running the minimum supported version of ESXi. For information about supported ESXi versions, see the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html.
- In the Unified CCE Administration, departments cannot be named `Global` or `Service`. If you already have departments created with these names, update the department names before upgrading Email and Chat.

NTP Configuration Requirements

Packaged CCE relies on time synchronization. Properly configuring NTP is critical for reliability of reporting data and cross-component communication. It's important to implement the requirements outlined in NTP and Time Synchronization, on page 7.

Upgrade Tools

Note During Unified CCE installation on to Windows Server 2019 and SQL Server 2019, SQL Server Security Hardening optional configuration should not be selected as part of installation. SQL Security Hardening should be applied post Unified CCE installation using Security Wizard tool.

During the upgrade process, use the following tools:

- ICM-CCE-Installer—The main Unified CCE Installer. It copies all files into relevant folders, creates the base registries, and installs needed third-party software such as JRE, Apache Tomcat, and Microsoft .NET Framework.

  You cannot run the installer remotely. Mount the installer ISO file only to a local machine.

- ICM12.6.2.exe—The Unified CCE patch installer. It copies all files into relevant folders, updates the registries, and installs needed third-party software such as JRE, Apache Tomcat, and Microsoft .NET Framework.

- Enhanced Database Migration Tool (EDMT)—A wizard application that is used for upgrades to migrate the Logger, BA, AW, and HDS databases.

  You can download the EDMT from Cisco.com by clicking **Cisco Enhanced Data Migration Tool Software Releases**.

  The EDMT displays status messages during the migration process, including warnings and errors. Warnings are displayed for informational purposes only and do not stop the migration. On the other hand, errors stop the migration process and leave the database in a corrupt state. If an error occurs, fix the error, and run the tool again.

- Regutil Tool—Used in Technology Refresh upgrades, the tool exports the Cisco Systems, Inc. registry from the source machine during the preupgrade process. The output of the tool is required on the destination machine when running the Unified CCE Installer during the upgrade process.

  You can download the Regutil Tool from Cisco.com by clicking **Contact Center Enterprise Tools**.

Packaged CCE 2000 Agents Deployment

Packaged CCE solution upgrade for 2000 Agent deployments can be done in single-stage on both main site and remote sites (if applicable). In a single-stage upgrade, all components are upgraded and taken to completion. For more information, see Single-stage Upgrade, on page 86.

Single-stage Upgrade

For single-stage upgrades, perform the tasks detailed in the following table.

Task
Upgrade Tasks
Technology Refresh Upgrade Task Flow, on page 86
Postupgrade Tasks
See *Post Technology Refresh Configurations* section in the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

Technology Refresh Upgrade Task Flow

For single-stage upgrades, perform the tasks detailed in the following table. You can either:

- set up all virtual machines required for a Packaged CCE solution (rebuild) on a different hardware or
- upgrade the existing components which have been moved (from the source server) to the destination server on a different hardware

Note

- On the destination server, follow the VM Layouts for 2000 Agent deployments as specified in the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html.
- The VM validations of hardware are turned off during Central Controller upgrade and are activated when cutover is initiated.
- For co-resident configurations, upgrade CUIC-LD-IDS along with the Unified CCE Central Controller upgrade.

Component Group	Components	Notes
Platform Orchestration, Hybrid Features	Cloud Connect	If you have Cloud Connect in your environment, refer the **Update VM Properties** section in Upgrade Considerations, on page 61 for Cloud connect upgrade prerequisite to increase the hard disk and RAM before you upgrade the component. If you don't have Cloud Connect in your environment, and you use any Hybrid feature or Orchestration, fresh install Cloud Connect. For fresh install instructions, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html

Component Group	Components	Notes
Queuing and self-service	Cisco Unified Customer Voice Portal (CVP) (Reporting Server, Call Server/VXMLServer, Unified Call Studio)	For CVP installation or upgrade instructions, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html After upgrading the Unified CVP servers, add the CVP machines to the domain. For more information, see Add Machine to Domain, on page 179.
Gateways	Cisco Virtualized Voice Browser (VVB)	For more information, see the *Installation and Upgrade Guide for Cisco Virtualized Voice Browser* at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-installation-guides-list.html.
	• IOS Gateways (If used for ingress access only) • IOS VXML Gateways	Upgrade Cisco Voice Gateway IOS Version, on page 207

Component Group	Components	Notes
Agent and supervisor desktops and Reporting	ECE	For ECE installation or upgrade instructions, see the *Enterprise Chat and Email Installation and Configuration Guide for Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html
	Cisco Finesse	For Finesse installation or upgrade instructions, see the *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html. After upgrading Finesse to 12.6(2), ensure that both ECDSA and RSA valid certificates are available in the certificate store in PG. If not, you must export the Finesse Tomcat certificates and import them to CTI Gateway (CG) and Peripheral Gateway (PG) systems. For more information, refer to the *Add Certificate for HTTPS Gadget* section in the Cisco Finesse Administration Guide.
	CUIC-LD-IDS CUIC (Reporting Templates)	

Component Group	Components	Notes
		Install or upgrade Cisco Unified Intelligence Center with Live Data and Identity Service (IdS). **Note** Cisco IdS 12.6(2) upgrade requires all SSO clients to log out from SSO, before any of the upgraded nodes is brought online. To avoid this requirement, it's recommended that you install 12.6(2) ES02 on the upgraded node and wait for the access token to expire before commencing the secondary node upgrade. Without installing 12.6(2) ES02, graceful shutdown feature will not be available for Cisco IdS 12.6(2) upgrade. You can view the duration of access token expiry in the IdS administration portal under **Settings** > **Security** > **Tokens** > **Access Token Expiry**. Deployments using VPN-less access to Finesse desktop should also upgrade the reverse proxy to 12.6(2) before Cisco IdS is upgraded to 12.6(2). For CUIC upgrade instructions, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html. After you upgrade Cisco Unified Intelligence Center (CUIC), you must: • Enable CORS on the CUIC server, and add **`cors allowed_origin`** with the Finesse hostname. For more information, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html. • After you upgrade Live Data (LD), you must enable CORS on the LD box for Finesse and CUIC. • Import LD and Finesse certificates to CUIC.

Component Group	Components	Notes
Unified CCE Controller	Unified CCE Rogger and AW-HDS-DDS	The CCE components upgrade requires the following maintenance windows on the source server: • First maintenance window to shut down services on Side A of source components. • Second maintenance window in the middle of the upgrade to cutover from Side B to Side A. You must bring down Side B before you bring up Side A.
	Unified CCE Rogger Side A	Migrate the Logger database and upgrade Side A Rogger Migrate the Logger Database and Upgrade the Rogger, on page 92
	Unified CCE AW-HDS-DDS Side A	Migrate AW-HDS-DDS and then upgrade Side A Unified CCE Administration & Data Server Migrate the AW and HDS Database and Upgrade the Unified CCE Administration & Data Server, on page 94 If you are using AppDynamics for performance monitoring on 12.6(1), then before upgrading the Distributor node from 12.6(1) to 12.6(2), disable AppDynamics performance monitoring on 12.6(1) and re-enable it after upgrading to 12.6(2). If AppDynamics performance monitoring is not disabled before the Distributor node is upgraded to 12.6(2), then post upgrade, restart the Distributor node.
	Unified CCE Rogger Side B	Migrate the Logger database and upgrade Side B Rogger Migrate the Logger Database and Upgrade the Rogger, on page 92
	Unified CCE AW-HDS-DDS Side B	Migrate AW-HDS-DDS and then upgrade Side B Unified CCE Administration & Data Server Migrate the AW and HDS Database and Upgrade the Unified CCE Administration & Data Server, on page 94 After you upgrade AW, import the certificate of all solution components (if applicable) to all AWs. If you are using AppDynamics for performance monitoring on 12.6(1), then before upgrading the Distributor node from 12.6(1) to 12.6(2), disable AppDynamics performance monitoring on 12.6(1) and re-enable it after upgrading to 12.6(2). If AppDynamics performance monitoring is not disabled before the Distributor node is upgraded to 12.6(2), then post upgrade, restart the Distributor node.
	External HDS	Migrate the AW and HDS Database & Upgrade the External HDS, on page 97

Component Group	Components	Notes
	Unified CCE Router	Enable Configuration Changes, on page 99
	Database Performance Enhancement	Database Performance Enhancement, on page 210
Unified CCE Peripheral Gateways and associated components	Peripheral Gateways	Upgrade Peripheral Gateways, on page 99 You can have many PGs located on different virtual machines. Upgrade both Side A and Side B PGs.
	Outbound Option Dialer	Upgrade the Outbound Option Dialer: Upgrade Outbound Option Dialer, on page 100 To enable Outbound Option High Availability in the Web Setup tool, see *Configure the Logger for Outbound Option* section in the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.
	Customer Collaboration Platform	For Customer Collaboration Platform installation or upgrade instructions, see the *Cisco SocialMiner Installation and Upgrade Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/products-installation-guides-list.html.
Call Processing Components	Cisco Unified Communications Manager (Unified Communications Manager)	For installation or upgrade instructions, see the *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service* or *Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html

Disable Configuration Changes

Procedure

To disable configuration changes during the upgrade, set the following registry key to 1 on the Side A Call Router: **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router A\Router\CurrentVersion\Configuration\Global\DBMaintenance**.

Caution Make sure that you do not perform inventory[1] and configuration[2] changes on the source server before the cutover is complete. Else, you will have to do these updates manually in the inventory on the destination server.

Export the Server Registry

Export the Cisco registry on each source machine that is involved in a Technology Refresh upgrade.

During the upgrade process, you are prompted for the path to the exported registry file location. Perform the following procedure and note the location of the resulting file for later in the upgrade process.

Each time you run the RegUtil with the export option, if a RegUtil_<hostname>.dat file exists, the utility renames that file to RegUtil_<hostname>.dat.bak<number>.

Procedure

Step 1 Open a command prompt and change the directory to the location where the RegUtil.exe resides.

Step 2 Run the RegUtil tool to export the Cisco Systems, Inc. registry using the following command: **RegUtil -export [target directory]** , for example, `<ICM install directory>:\icm\bin>RegUtil -export C:\RegUtil`

The target directory must have write access. Therefore, you cannot select the install media on a DVD. The target directory is optional. If it is not specified, the tool outputs the result of the Registry export to the current directory. The output filename is of the format RegUtil_<hostname>.dat, where hostname is the name of the source machine.

Migrate the Logger Database and Upgrade the Rogger

Before you begin

- EDMT requires Microsoft® ODBC Driver 17 for SQL Server® and Visual C++ Redistributable for Visual Studio 2015 (or higher). The latest version of these packages can be downloaded from the Microsoft website. However, a copy of the same is also available in the **Prerequisites** folder of EDMT.
- If you are configuring SQL services to run as Virtual account (NT SERVICE) or Network Service account (NT AUTHORITY\NETWORK SERVICE), you must run EDMT as an administrator.
- Create a shared folder in any desired location. Ensure that:
  - In the **Properties** window > **Sharing** tab > **Advanced Sharing,** the **Share this folder** check box is checked.
  - In the **Properties** window > **Security** tab > **Advanced Sharing** > **Permission**, the permission level is set as **Full control** for the user group **everyone**.

[1] Addition, modification, or deletion of machines.
[2] Cloud Connect integration, Default Media Server settings, Courtesy Callback, SIP Server Group, Route Pattern, and Locations.

Note If the user group **everyone** is not available, add it using the **Add** button.

Procedure

Step 1 Use **Unified CCE Service Control** to stop all Unified CCE services on the Router and Logger, on the source server.

Step 2 (Optional) If Outbound Option High Availability is deployed, disable Outbound Options High Availability. For details, see Disable Outbound Options High Availability (If Applicable), on page 100.

Step 3 Download the EDMT tool from Cisco.com, and ensure pre-requisites for the same have been installed on the target/destination system, prior to launching EDMT. These include the ODBC Driver 17 for SQL Server, and Visual C++ Redistributable for Visual Studio 2015.

Step 4 Run the **EDMT** from the server that will host the destination Logger and click **Next**.

Step 5 Select **Technology Refresh** and click **Next**.

Step 6 Under **Source Database Connection**, complete the following fields:

- From the **Authentication** drop-down list, select **SQL Server Authentication** or **Windows Authentication** (default).
- In the **HostName/IP Address** field, enter the IP address or hostname of the source server with the Logger database.
- In the **SQL Server Port Number** field, enter the TCP or IP port in which the source SQL Server runs. This field defaults to1433, the standard SQL Server port.
- Enter the values in **Domain Name**, **Username**, and **Password** fields.

  Note
  - For SQL Server Authentication, enter the SQL Server credentials and the domain name (if applicable) for the selected database.
  - For Windows Authentication, the Domain Name, Username, and Password fields are disabled. Windows Single Sign-On (SSO) uses your Windows authentication cached credentials to connect to the selected database.

- Click **Refresh Database List** to refresh the list of available Unified ICM databases on the server.
- In the **Database Name**, select the Logger database.

Step 7 Under **Destination Database Connection**, complete the following fields:

- In the **Authentication** drop-down list, use **Windows Authentication** (default).
- In the **SQL Server Port Number** field, enter the TCP or IP port in which the destination SQL Server runs. This field defaults to1433, the standard SQL Server port.

  Note The rest of the fields are disabled (read-only) and the default values are displayed.

- Click **Next**.

Step 8 Under **Backup Connection**, complete the following fields:

- In the **HostName/IP Address** field, enter the backup server's IP address or hostname.
- In the **Windows Share Name** field, enter the name of the shared folder where the backup database file is.
- In the **Windows Share Domain** field, enter the domain name (if applicable).
- In the **Windows Share Username** and **Windows Share Password** fields, enter the Windows credentials that has read or write access to the specified Windows share.

Step 9 In the **Destination Restore Location**, browse to select the folder where the system creates the database data files (.mdf) and translation log files (.ldf). The destination is prepopulated with the default location for database file storage for the running SQL Server.

Step 10 Click **Next**.

Step 11 Click **Start Migration**.

Step 12 Click **Yes** on the warning pop-up to start the data migration.

Step 13 Upon completion of the migration, click **Exit** to close the tool.

Step 14 (Optional) If Outbound Option High Availability is deployed, repeat steps 1 through 13 to migrate the BA database.

Step 15 Launch the ICM-CCE-Installer and click **Next**.

Step 16 Select **Technology Refresh** and click **Next**.

Step 17 Click **Browse** and specify the path for the RegUtil file you exported from the source machine during the preupgrade process.

Step 18 (Optional) To apply any Minor/Maintenance Releases, click **Browse** and navigate to the Minor/Maintenance Release software. Click **Next**.

Note During Unified CCE installation on to Windows Server 2019 and SQL Server 2019, you should not select SQL Server Security Hardening optional configuration as a part of the installation. You can apply the SQL Security Hardening post installation using the Security Wizard tool.

Step 19 (Optional) Select **SQL Server Security Hardening** and click **Next**.

Step 20 Click **OK** on any informational messages that display.

Step 21 Click **Install**.

Step 22 Reboot the system after the upgrade completes.

Migrate the AW and HDS Database and Upgrade the Unified CCE Administration & Data Server

To upgrade the Administration & Data Server, migrate the AW database and then the HDS database (if applicable). After successful migration, install the new software and import the Cisco registry information.

Before you begin

- EDMT requires Microsoft® ODBC Driver 17 for SQL Server® and Visual C++ Redistributable for Visual Studio 2015 (or higher). The latest version of these packages can be downloaded from the Microsoft website. However, a copy of the same is also available in the **Prerequisites** folder of EDMT.

- If you are configuring SQL services to run as Virtual account (NT SERVICE) or Network Service account (NT AUTHORITY\NETWORK SERVICE), you must run EDMT as an administrator.
- Create a shared folder in any desired location. Ensure that:
  - In the **Properties** window > **Sharing** tab > **Advanced Sharing,** the **Share this folder** check box is checked.
  - In the **Properties** window > **Security** tab > **Advanced Sharing** > **Permission**, the permission level is set as **Full control** for the user group **everyone**.

Note If the user group **everyone** is not available, add it using the **Add** button.

Procedure

Step 1 Use **Unified CCE Service Control** to stop all Unified CCE services on the source server.

Step 2 Download the EDMT tool from Cisco.com, and ensure pre-requisites for the same have been installed on the target/destination system, prior to launching EDMT. These include the ODBC Driver 17 for SQL Server, and Visual C++ Redistributable for Visual Studio 2015.

Step 3 Launch the EDMT tool on the destination server that hosts the **Administration and Data Server with AW and HDS database** and click **Next**.

Step 4 Select **Technology Refresh** and click **Next**.

Step 5 Under **Source Database Connection**, complete the following fields:

- From the **Authentication** drop-down list, select **SQL Server Authentication** or **Windows Authentication** (default).
- In the **HostName/IP Address** field, enter the IP address or hostname of the source server with the database.
- In the **SQL Server Port Number** field, enter the TCP or IP port in which the source SQL Server runs. This field defaults to1433, the standard SQL Server port.
- Enter the values in **Domain Name**, **Username**, and **Password** fields.

  Note
  - For SQL Server Authentication, enter the SQL Server credentials and the domain name (if applicable) for the selected database.
  - For Windows Authentication, the Domain Name, Username, and Password fields are disabled. Windows Single Sign-On (SSO) uses your Windows authentication cached credentials to connect to the selected database.

- Click **Refresh Database List** to refresh the list of available Unified ICM databases on the server.
- In the **Database Name**, select the AW database.

Step 6 Under **Destination Database Connection**, complete the following fields:

- In the **Authentication** drop-down list, use **Windows Authentication** (default).

- In the **SQL Server Port Number** field, enter the TCP or IP port in which the destination SQL Server runs. This field defaults to1433, the standard SQL Server port.

  Note The rest of the fields are disabled (read-only) and the default values are displayed.

- Click **Next**.

Step 7 Under **Backup Connection**, complete the following fields:

- In the **HostName/IP Address** field, enter the backup server's IP address or hostname.
- In the **Windows Share Name** field, enter the name of the shared folder where the backup database file is.
- In the **Windows Share Domain** field, enter the domain name (if applicable).
- In the **Windows Share Username** and **Windows Share Password** fields, enter the Windows credentials that has read or write access to the specified Windows share.

Step 8 In the **Destination Restore Location**, browse to select the folder where the system creates the database data files (.mdf) and translation log files (.ldf). The destination is prepopulated with the default location for database file storage for the running SQL Server.

Step 9 Click **Next**.

Step 10 Click **Start Migration**.

Step 11 Click **Yes** on the warning pop-up to start the data migration.

Step 12 Upon completion of the migration, click **Exit** to close the tool.

Step 13 To migrate the HDS database, repeat steps 1 to 12.

Under Source Database Connection, in **Database Name**, select the HDS database.

Step 14 Launch the ICM-CCE-Installer and click **Next**.

Step 15 Select **Technology Refresh** and click **Next**.

Step 16 Click **Browse** and specify the path for the `RegUtil` file you exported from the source machine during the preupgrade process.

Step 17 To apply any Minor/Maintenance Releases, click **Browse** and navigate to the Minor/Maintenance Release software. Click **Next**.

Step 18 (Optional) Select **SQL Server Security Hardening** and click **Next**.

Step 19 Click **OK** on any informational messages that display.

Step 20 Click **Install**.

Step 21 Select **`Yes`** for the system to restart and complete the installation automatically or select **`No`** to restart the system manually after installing Unified ICM 12.5(1).

Note
- If you have selected Unified ICM 12.6(2) previously, you must select **`Yes`** for the system to restart automatically.
- After installing Unified ICM 12.5(1), you must restart the system manually before launching the Unified ICM 12.6(2) installation wizard.

Step 22 Log in to your system using domain credentials with administrative privileges.

Step 23 Wait for the Unified CCE 12.6(2) installation wizard to launch. Click **Next** to proceed.

Step 24 Select the radio button to accept the license agreement and click **Next**.

Step 25 Click **Install** to begin the installation.

Step 26 Select the radio button to restart the system and click **Finish**.

Migrate the AW and HDS Database & Upgrade the External HDS

To upgrade the external HDS, migrate the AW database, and then the HDS database. After successful migration, install the new software and import the Cisco registry information.

Before you begin

- EDMT requires Microsoft® ODBC Driver 17 for SQL Server® and Visual C++ Redistributable for Visual Studio 2015 (or higher). The latest version of these packages can be downloaded from the Microsoft website. However, a copy of the same is also available in the **Prerequisites** folder of EDMT.
- If you are configuring SQL services to run as Virtual account (NT SERVICE) or Network Service account (NT AUTHORITY\NETWORK SERVICE), you must run EDMT as an administrator.
- Create a shared folder in any desired location. Ensure that:
  - In the **Properties** window > **Sharing** tab > **Advanced Sharing,** the **Share this folder** check box is checked.
  - In the **Properties** window > **Security** tab > **Advanced Sharing** > **Permission**, the permission level is set as **Full control** for the user group **everyone**.

Note If the user group **everyone** is not available, add it using the **Add** button.

Procedure

Step 1 Use **Unified CCE Service Control** to stop all Unified CCE services on the source server.

Step 2 Download the EDMT tool from Cisco.com, and ensure pre-requisites for the same have been installed on the target/destination system, prior to launching EDMT. These include the ODBC Driver 17 for SQL Server, and Visual C++ Redistributable for Visual Studio 2015.

Step 3 Launch the EDMT tool on the destination server that hosts the **Administration and Data Server with AW and HDS database** and click **Next**.

Step 4 Select **Technology Refresh** and click **Next**.

Step 5 Under **Source Database Connection**, complete the following fields:

- From the **Authentication** drop-down list, select **SQL Server Authentication** or **Windows Authentication** (default).
- In the **HostName/IP Address** field, enter the IP address or hostname of the source server with the database.
- In the **SQL Server Port Number** field, enter the TCP or IP port in which the source SQL Server runs. This field defaults to1433, the standard SQL Server port.

- Enter the values in **Domain Name**, **Username**, and **Password** fields.

  Note
  - For SQL Server Authentication, enter the SQL Server credentials and the domain name (if applicable) for the selected database.
  - For Windows Authentication, the Domain Name, Username, and Password fields are disabled. Windows Single Sign-On (SSO) uses your Windows authentication cached credentials to connect to the selected database.

- Click **Refresh Database List** to refresh the list of available Unified ICM databases on the server.
- In the **Database Name**, select the AW database.

Step 6 Under **Destination Database Connection**, complete the following fields:

- In the **Authentication** drop-down list, use **Windows Authentication** (default).
- In the **SQL Server Port Number** field, enter the TCP or IP port in which the destination SQL Server runs. This field defaults to1433, the standard SQL Server port.

  Note The rest of the fields are disabled (read-only) and the default values are displayed.

- Click **Next**.

Step 7 Under **Backup Connection**, complete the following fields:

- In the **HostName/IP Address** field, enter the backup server's IP address or hostname.
- In the **Windows Share Name** field, enter the name of the shared folder where the backup database file is.
- In the **Windows Share Domain** field, enter the domain name (if applicable).
- In the **Windows Share Username** and **Windows Share Password** fields, enter the Windows credentials that has read or write access to the specified Windows share.

Step 8 In the **Destination Restore Location**, browse to select the folder where the system creates the database data files (.mdf) and translation log files (.ldf). The destination is prepopulated with the default location for database file storage for the running SQL Server.

Step 9 Click **Next**.

Step 10 Click **Start Migration**.

Step 11 Click **Yes** on the warning pop-up to start the data migration.

Step 12 Upon completion of the migration, click **Exit** to close the tool.

Step 13 To migrate the HDS database, repeat steps 1 to 12.

Under Source Database Connection, in **Database Name**, select the HDS database.

Step 14 Launch the ICM-CCE-Installer and click **Next**.

Step 15 Select **Technology Refresh** and click **Next**.

Step 16 Click **Browse** and specify the path for the `RegUtil` file you exported from the source machine during the preupgrade process.

Step 17 (Optional) To apply any Minor/Maintenance Releases, click **Browse** and navigate to the Minor/Maintenance Release software. Click **Next**.

Note SQL Security Hardening should not be applied during installation of Windows Server 2019 and SQL Server 2019. SQL Security Hardening can be applied post installation using the Security Wizard tool.

Step 18 (Optional) Select **SQL Server Security Hardening** and click **Next**.

Step 19 Click **OK** on any informational messages that display.

Step 20 Click **Install**.

Step 21 Reboot the server when the upgrade completes.

Enable Configuration Changes

Procedure

Step 1 To enable configuration changes during the upgrade, set the following registry key to 0 on the Side A Call Router: **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router A\Router\CurrentVersion\Configuration\Global\DBMaintenance**.

Step 2 To confirm that configuration changes are enabled, save a configuration change.

Save your changes.

Upgrade Peripheral Gateways

You can upgrade different Peripheral Gateways (PG) within a contact center at different times within different maintenance windows. However, upgrade all PGs that reside on the same virtual machine and redundant PGs (Side A and corresponding Side B) during the same maintenance window.

The following dependencies occur when upgrading the PG:

- If your contact center uses the CTI OS component, upgrade the CTI OS server at the same time as the associated Avaya PG[3].
- If your contact center uses Outbound Option, upgrade any Outbound Option Dialers associated with Unified Communications Manager PGs at the same time.
- If the Unified Communications Manager application is upgraded, upgrade the JTAPI client associated with the Unified Communications Manager PG at the same time.

To upgrade the Peripheral Gateways, install the new software and import the Cisco registry information.

Procedure

Step 1 Use Unified CCE Service Control to stop all Unified CCE and CTI OS (if applicable when upgrading the Avaya PG) services on the PG server. Change the services to Manual Start.

Step 2 Launch the ICM-CCE-Installer and click **Next**.

Step 3 Select **Technology Refresh** and click **Next**.

[3] Applicable only in 4000 and 12000 Agent deployments.

Step 4 Click **Browse** and specify the path for the RegUtil file you exported from the source machine during the preupgrade process.

The registry information for the Avaya PG also contains information for the CTI OS server (if applicable).

Step 5 (Optional) To apply any Minor/Maintenance Releases, click **Browse** and navigate to the Minor/Maintenance Release software. Click **Next**.

Step 6 Click **OK** on any informational messages that display.

Step 7 Click **Install**.

Step 8 Reboot the system after the upgrade completes.

Step 9 If Avaya PG is configured, after reboot, open the Peripheral Gateway Setup tool, and edit the Avaya PG as required.

Step 10 If CTI OS component is configured, after reboot, open the CTI OS Server setup tool, and edit the CTI OS component as required.

Disable Outbound Options High Availability (If Applicable)

Before you begin

If Outbound Options High Availability is enabled, you must disable it on source machines before you perform the upgrade.

Before proceeding with the following steps, ensure that Outbound Options feature is in maintenance mode. There must not be any customer records getting imported to Outbound database. The outbound campaigns must not be active and outbound callflow must not be in progress.

Perform the following steps on Side A:

Procedure

Step 1 Launch **Websetup**. Navigate to **Component Management** > **Loggers**.

Step 2 Edit the **Logger** and navigate to **Additional Options**. Uncheck **Enable High Availability** under **Outbound Option**. Enter the SQL Server Admin credentials and click **Next**.

Step 3 Enable **Stop and then start(cycle) the Logger Service for this instance (if it is running)** checkbox . Click **Next** to complete the setup.

Step 4 Repeat similar steps (steps 1, 2, and 3) for side B.

What to do next

You can enable Outbound Options High Availability after the upgrade is successful.

Upgrade Outbound Option Dialer

To upgrade the Outbound Option Dialer, install the new software and import the Cisco registry information.

Before you begin

You must have previously migrated the Outbound Option database during the Logger upgrade.

Procedure

Step 1 Launch the ICM-CCE-Installer and click **Next**.

Step 2 Select **Technology Refresh** and click **Next**.

Step 3 Click **Browse** and specify the path for the RegUtil file you exported from the source machine during the preupgrade process.

Step 4 (Optional) To apply any Maintenance Releases, click **Browse** and navigate to the Maintenance Release software. Click **Next**.

Step 5 Click **OK** on any informational messages that display.

Step 6 Click **Install**.

Step 7 Reboot the system after the upgrade completes.

Step 8 Open the Peripheral Gateway Setup tool from the Installer dialog box or desktop shortcut and edit the Dialer as required.

Step 9 Use Unified CCE Service Control to set all Unified CCE services to Automatic Start.

Packaged CCE 4000 Agents and above Deployment

Packaged CCE solution upgrade for 4000 Agents and above deployments can be done in single-stage or in multiple stages (multistage) on both main site and remote sites (if applicable).

In a single-stage upgrade, all components are upgraded and taken to completion. For more information, see Single-stage Upgrade, on page 101.

In a multistage upgrade, components are grouped into several stages for upgrading. You must follow the upgrade sequence and the minimum component groupings that must occur together within each stage. At each stage in the upgrade, the upgraded components must interoperate with components that have not yet been upgraded to ensure the overall operation of the contact center. Therefore, it is important to verify this interoperability during the planning stages of the upgrade. For more information, see Multistage Upgrade, on page 106.

Single-stage Upgrade

For single-stage upgrades, perform the tasks detailed in the following table.

Task
Upgrade Tasks
Technology Refresh Upgrade Task Flow, on page 102
Postupgrade Tasks
See *Post Technology Refresh Configurations* section in the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

Technology Refresh Upgrade Task Flow

For single-stage upgrades, perform the tasks detailed in the following table. You can either:

- set up all virtual machines required for a Packaged CCE solution (rebuild) on a different hardware or
- upgrade the existing components which have been moved (from the source server) to the destination server on a different hardware

Component Group	Components	Notes
Platform Orchestration, Hybrid Features	Cloud Connect	If you have Cloud Connect in your environment, refer the **Update VM Properties** section in Upgrade Considerations, on page 61 for Cloud connect upgrade prerequisite to increase the hard disk and RAM before you upgrade the component. If you don't have Cloud Connect in your environment, and you use any Hybrid feature or Orchestration, fresh install Cloud Connect. For fresh install instructions, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
Queuing and self-service	Cisco Unified Customer Voice Portal (CVP) (Reporting Server, Call Server/VXMLServer, Unified Call Studio)	For CVP installation or upgrade instructions, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html
Gateways	Cisco Virtualized Voice Browser	For VVB installation or upgrade instructions, see the *Installation and Upgrade Guide for Cisco Virtualized Voice Browser* at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-installation-guides-list.html.
	• IOS Gateways (If used for ingress access only.) • IOS VXML Gateways	Upgrade Cisco Voice Gateway IOS Version, on page 207

Component Group	Components	Notes
Identity Service (IdS)/SSO	IdS Server	SSO is an optional feature. It exchanges authentication and authorization details between an identity provider (IdP) and an identity service (IdS). For IdS installation or upgrade instructions, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html **Note** Cisco IdS 12.6(2) upgrade requires all SSO clients to log out from SSO, before any of the upgraded nodes is brought online. To avoid this requirement, it's recommended that you install 12.6(2) ES?? on the upgraded node and wait for the access token to expire before commencing the secondary node upgrade. Without using the 12.6(2) ES??, graceful shutdown feature will not be available for Cisco IdS 12.6(2) upgrade. You can view the duration of access token expiry in the IdS administration portal under **Settings** > **Security** > **Tokens** > **Access Token Expiry**. Deployments using VPN-less access to Finesse desktop should also upgrade the reverse proxy to 12.6(2) before Cisco IdS is upgraded to 12.6(2).
Agent and supervisor desktops	ECE	For ECE installation or upgrade instructions, see the *Enterprise Chat and Email Installation and Configuration Guide for Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html
	Cisco Finesse	For Finesse installation or upgrade instructions, see the *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html. After upgrading Finesse to 12.6(2), ensure that both ECDSA and RSA valid certificates are available in the certificate store in PG. If not, you must export the Finesse Tomcat certificates and import them to CTI Gateway (CG) and Peripheral Gateway (PG) systems. For more information, refer to the *Add Certificate for HTTPS Gadget* section in the Cisco Finesse Administration Guide.
Reporting Management	Cisco Unified Intelligence Center (CUIC) Reporting Server	For CUIC installation or upgrade instructions, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html. After you upgrade Cisco Unified Intelligence Center (CUIC), you must: • Enable CORS on the CUIC server, and add **`cors allowed_origin`** with the Finesse hostname. • Import LD and Finesse certificates to CUIC.

Component Group	Components	Notes
Unified CCE Central Controller	Unified CCE Rogger and AW-HDS-DDS	The CCE components upgrade requires the following maintenance windows on the source server: • First maintenance window to shut down services on Side A of source components. • Second maintenance window in the middle of the upgrade to cut over from Side B to Side A. You must bring down Side B before you bring up Side A.
	Unified CCE Rogger Side A	Migrate the Logger database and upgrade Side A Rogger Migrate the Logger Database and Upgrade the Rogger, on page 92
	Unified CCE AW-HDS-DDS Side A	Migrate AW-HDS-DDS and then upgrade Side A Unified CCE Administration & Data Server Migrate the AW and HDS Database and Upgrade the Unified CCE Administration & Data Server, on page 94 If you are using AppDynamics for performance monitoring on 12.6(1), then before upgrading the Distributor node from 12.6(1) to 12.6(2), disable AppDynamics performance monitoring on 12.6(1) and re-enable it after upgrading to 12.6(2). If AppDynamics performance monitoring is not disabled before the Distributor node is upgraded to 12.6(2), then post upgrade, restart the Distributor node.
	Unified CCE Rogger Side B	Migrate the Logger database and upgrade Side B Rogger Migrate the Logger Database and Upgrade the Rogger, on page 92
	Unified CCE AW-HDS-DDS Side B	Migrate AW-HDS-DDS and then upgrade Side B Unified CCE Administration & Data Server Migrate the AW and HDS Database and Upgrade the Unified CCE Administration & Data Server, on page 94 After you upgrade AW, import the certificate of all solution components (if applicable) to all AWs. If you are using AppDynamics for performance monitoring on 12.6(1), then before upgrading the Distributor node from 12.6(1) to 12.6(2), disable AppDynamics performance monitoring on 12.6(1) and re-enable it after upgrading to 12.6(2). If AppDynamics performance monitoring is not disabled before the Distributor node is upgraded to 12.6(2), then post upgrade, restart the Distributor node.
	External HDS	Migrate the AW and HDS Database & Upgrade the External HDS, on page 97
	Unified CCE Router	Enable Configuration Changes, on page 99
	CUIC (Reporting Templates)	

Component Group	Components	Notes
		For CUIC installation or upgrade instructions, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html.
	Standalone Live Data	To install or upgrade Live Data, see the *Installation and Upgrade Guide for Cisco Unified Intelligence Center Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html. After you upgrade Live Data (LD), you must enable CORS on the LD server, and add **`cors allowed_origin`** with Finesse hostname.
	Database Performance Enhancement	Database Performance Enhancement, on page 210
Collocated Peripheral Gateways and associated components	Peripheral Gateways[4]	Upgrade Peripheral Gateways, on page 99 You can have many PGs located on different virtual machines. Upgrade both Side A and Side B PGs.
	Outbound Option Dialer	Upgrade Outbound Option Dialer, on page 100 To enable Outbound Option High Availability in the Web Setup tool, see *Configure the Logger for Outbound Option* section in the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.
	• CTI Server • CTI OS Server	CTI OS Server is applicable only if Avaya PG is used. For installation instructions, see the *CTI OS System Manager Guide for Cisco Unified ICM* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.
Peripheral Gateways and associated components not collocated	Customer Collaboration Platform	For Customer Collaboration Platform installation or upgrade instructions, see the *Cisco SocialMiner Installation and Upgrade Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/products-installation-guides-list.html.
Agent and Supervisor Desktops	CTI OS Desktops	For CTI OS Desktop client installation instructions, see the *CTI OS System Manager Guide for Cisco Unified ICM* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html .

Component Group	Components	Notes
Call Processing Components	Cisco Unified Communications Manager (Unified Communications Manager)	For installation or upgrade instructions, see the *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service* or *Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html
	JTAPI client on Agent (Cisco Unified Communications Manager) PG	Upgrade Cisco JTAPI Client on PG, on page 209

[4] After upgrading the Central Controller to 12.6(2), if you intend to keep the PGs in 12.0(1), you must install ICM_12.0(1)_ES49 on the PG machines for an inventory update.

Multistage Upgrade

For multistage upgrades, perform the tasks detailed in the following table.

Task
Upgrade Tasks
Technology Refresh Upgrade Task Flow, on page 106
Postupgrade Tasks
Follow the post upgrade tasks after each stage of upgrade. For more information, see *Post Technology Refresh Configurations* section in the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

Technology Refresh Upgrade Task Flow

For multistage upgrades, perform the upgrade tasks detailed in the following table. The upgrade tasks are as per the Upgrade Flowcharts for 4000 Agents and above Deployments, on page 47. You can either:

- set up the required virtual machines (rebuild) on a different hardware or
- upgrade the existing components which have been moved (from the source server) to the destination server on a different hardware

Note Maintenance window is applicable for each component until the inventory update and configurations are complete.

Stage	Component Group	Components	Notes
1	Platform Orchestration, Hybrid Features	Cloud Connect	If you have Cloud Connect in your environment, refer the **Update VM Properties** section in Upgrade Considerations, on page 61 for Cloud connect upgrade prerequisite to increase the hard disk and RAM before you upgrade the component. If you don't have Cloud Connect in your environment, and you use any Hybrid feature or Orchestration, fresh install Cloud Connect. For fresh install instructions, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
2	Queuing and self-service	Cisco Unified Customer Voice Portal (CVP) (Reporting Server, Call Server/VXMLServer, Unified Call Studio)	For CVP installation or upgrade instructions, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html
3	Gateways	Cisco Virtualized Voice Browser	For VVB installation or upgrade instructions, see the *Installation and Upgrade Guide for Cisco Virtualized Voice Browser* at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-installation-guides-list.html.
		• IOS Gateways (If used for ingress access only. If used for Outbound Option Dialer, see stage 6 in Upgrade Flowcharts for 4000 Agents and above Deployments, on page 47.) • IOS VXML Gateways	Upgrade Cisco Voice Gateway IOS Version, on page 207

Stage	Component Group	Components	Notes
4	Identity Service (IdS)/SSO	IdS Server	SSO is an optional feature. It exchanges authentication and authorization details between an identity provider (IdP) and an identity service (IdS). **Note** Cisco IdS 12.6(2) upgrade requires all SSO clients to log out from SSO, before any of the upgraded nodes is brought online. To avoid this requirement, it's recommended that you install 12.6(2) ES02 on the upgraded node and wait for the access token to expire before commencing the secondary node upgrade. Without installing 12.6(2) ES02, graceful shutdown feature will not be available for Cisco IdS 12.6(2) upgrade. You can view the duration of access token expiry in the IdS administration portal under **Settings** > **Security** > **Tokens** > **Access Token Expiry**. Deployments using VPN-less access to Finesse desktop should also upgrade the reverse proxy to 12.6(2) before Cisco IdS is upgraded to 12.6(2). For IdS installation or upgrade instructions, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html
5	Agent and supervisor desktops	ECE	For ECE installation or upgrade instructions, see the *Enterprise Chat and Email Installation and Configuration Guide for Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html
		Cisco Finesse	For Finesse installation or upgrade instructions, see the *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html. After upgrading Finesse to 12.6(2), ensure that both ECDSA and RSA valid certificates are available in the certificate store in PG. If not, you must export the Finesse Tomcat certificates and import them to CTI Gateway (CG) and Peripheral Gateway (PG) systems. For more information, refer to the *Add Certificate for HTTPS Gadget* section in the Cisco Finesse Administration Guide.

Stage	Component Group	Components	Notes
6	Reporting Management	Cisco Unified Intelligence Center (CUIC) Reporting Server	For CUIC installation or upgrade instructions, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html. After you upgrade Cisco Unified Intelligence Center (CUIC), you must: • Enable CORS on the CUIC server, and add **`cors allowed_origin`** with the Finesse hostname. • Import LD and Finesse certificates to CUIC.

Stage	Component Group	Components	Notes
7	Unified CCE Central Controller	Unified CCE Rogger and AW-HDS-DDS	The CCE components upgrade requires the following maintenance windows on the source server: • First maintenance window to shut down services on Side A of source components. • Second maintenance window in the middle of the upgrade to cut over from Side B to Side A. You must bring down Side B before you bring up Side A.
		Unified CCE Rogger Side A	Migrate the Logger database and upgrade Side A Rogger Migrate the Logger Database and Upgrade the Rogger, on page 92
		Unified CCE AW-HDS-DDS Side A	Migrate AW-HDS-DDS and then upgrade Side A Unified CCE Administration & Data Server Migrate the AW and HDS Database and Upgrade the Unified CCE Administration & Data Server, on page 94 If you are using AppDynamics for performance monitoring on 12.6(1), then before upgrading the Distributor node from 12.6(1) to 12.6(2), disable AppDynamics performance monitoring on 12.6(1) and re-enable it after upgrading to 12.6(2). If AppDynamics performance monitoring is not disabled before the Distributor node is upgraded to 12.6(2), then post upgrade, restart the Distributor node.
		Unified CCE Rogger Side B	Migrate the Logger database and upgrade Side B Rogger Migrate the Logger Database and Upgrade the Rogger, on page 92
		Unified CCE AW-HDS-DDS Side B	Migrate AW-HDS-DDS and then upgrade Side B Unified CCE Administration & Data Server Migrate the AW and HDS Database and Upgrade the Unified CCE Administration & Data Server, on page 94 After you upgrade AW, import the certificate of all solution components (if applicable) to all AWs. If you are using AppDynamics for performance monitoring on 12.6(1), then before upgrading the Distributor node from 12.6(1) to 12.6(2), disable AppDynamics performance monitoring on 12.6(1) and re-enable it after upgrading to 12.6(2). If AppDynamics performance monitoring is not disabled before the Distributor node is upgraded to 12.6(2), then post upgrade, restart the Distributor node.
		External HDS	Migrate the AW and HDS Database & Upgrade the External HDS, on page 97
		Unified CCE Router	Enable Configuration Changes, on page 99
		CUIC (Reporting Templates)	

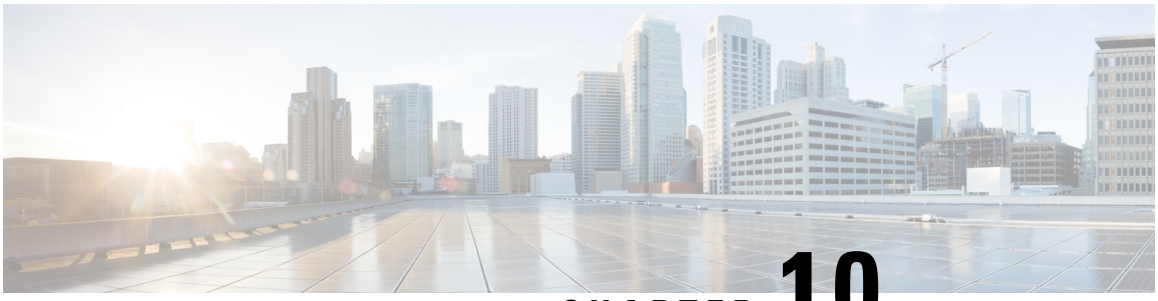
Stage	Component Group	Components	Notes
			For CUIC installation or upgrade instructions, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html.
		Standalone Live Data	To install or upgrade Live Data, see the *Installation and Upgrade Guide for Cisco Unified Intelligence Center Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html. After you upgrade Live Data (LD), you must enable CORS on the LD server, and add **`cors allowed_origin`** with Finesse hostname.
		Database Performance Enhancement	Database Performance Enhancement, on page 210
8	Collocated Peripheral Gateways and associated components	Peripheral Gateways[5]	Upgrade Peripheral Gateways, on page 99 You can have many PGs located on different virtual machines. Upgrade both Side A and Side B PGs.
		Outbound Option Dialer	Upgrade Outbound Option Dialer, on page 100 To enable Outbound Option High Availability in the Web Setup tool, see *Configure the Logger for Outbound Option* section in the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.
		• CTI Server • CTI OS Server	CTI OS Server is applicable only if Avaya PG is used. For installation instructions, see the *CTI OS System Manager Guide for Cisco Unified ICM* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.
9	Peripheral Gateways and associated components not collocated	Customer Collaboration Platform	For Customer Collaboration Platform installation or upgrade instructions, see the *Cisco SocialMiner Installation and Upgrade Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/products-installation-guides-list.html.
10	Agent and Supervisor Desktops	CTI OS Desktops	For CTI OS Desktop client installation instructions, see the *CTI OS System Manager Guide for Cisco Unified ICM* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html .

Stage	Component Group	Components	Notes
11	Call Processing Components	Cisco Unified Communications Manager (Unified Communications Manager)	For installation or upgrade instructions, see the *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service* or *Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html
		JTAPI client on Agent (Cisco Unified Communications Manager) PG	Upgrade Cisco JTAPI Client on PG, on page 209

[5] After upgrading the Central Controller to 12.6(2), if you intend to keep the PGs in 12.0(1), you must install ICM_12.0(1)_ES49 on the PG machines for an inventory update.

PART IV

Uninstallation



CHAPTER 10

Uninstallation

Uninstallation of Unified ICM/CCE base version 12.5(1)

Uninstallation of Unified ICM/CCE base of 12.5(1) is not supported for Unified CCE components that are deployed on Windows Server using the ICM-CCE-Installer. However, support for uninstallation and re-installation of client installer packages like Administration Client and Internet Script Editor continues.

Note The option to roll back to previous versions is only available with minor and maintenance releases.

Prerequisite for Uninstallation of CCE 12.6(2) Maintenance Release

If you have enabled the optional feature Outbound Option High Availability, you must disable it before you uninstall Unified ICM 12.6(2). From Unified CCE Web Setup, choose **Component Management** > **Loggers**. Select a logger that is enabled for High Availability, and click **Next** until the **Additional Options** page appears. Uncheck the **Enable High Availability** check box. Perform this action for each logger enabled for Outbound Option High Availability.

If you are planning to roll back to previous version of CCE Release 12.6(2), do the following:

1. Export the certificates of all the components imported into the truststore. To export the certificate, use the command:

   ```
   keytool -export -keystore <ICM install Dir>\ssl\cacerts -alias <alias of the component>
    -file <filepath>.cer
   ```

2. Enter the truststore password when prompted.

After the roll back, do the following:

1. Import the certificates exported in step 1 above, into the JRE keystore. To import the certificate, use the command:

   ```
   keytool -import -keystore <Oracle/OpenJDK JRE path>\lib\security\cacerts -file
   <filepath>.cer -alias <alias>
   ```

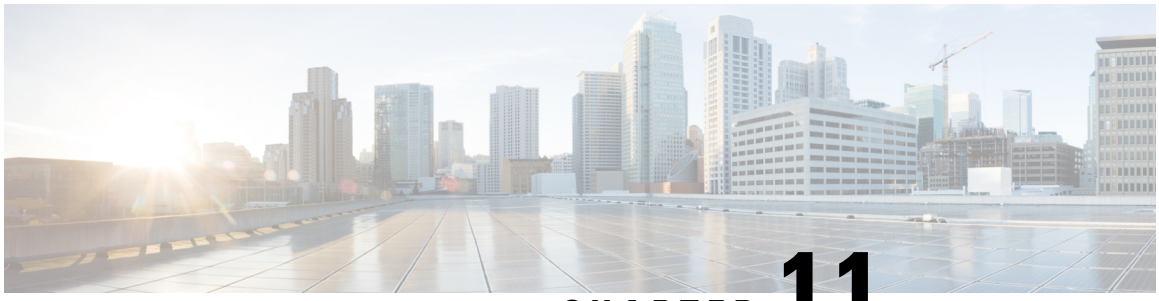
2. Enter the keystore password when prompted.

3. Enter **yes** when prompted to trust the certificate.

Note You don't need to reimport the certificates if you are rolling back to CCE 12.5(1a) or 12.6(1). Also, if you have already installed ES55 (mandatory OpenJDK ES), you don't need to reimport the certificate when you roll back to CCE 12.5(1).

PART V

Orchestration



CHAPTER 11

CCE Orchestration

Overview

The Orchestration feature provides partners and administrators an option to automatically download software updates and simplify the installation and rollback processes. The Orchestration framework is built within the Cloud Connect server that connects to the Cisco hosted cloud software repository. This framework provides the ability to check and download new software updates as and when they are available and notify the administrators via email about the new updates along with the release notes. Orchestration currently supports installation and rollback of Cisco Engineering Specials (ES), Service Updates (SU), Minor Releases (MR), and Microsoft Patches.

Email Notification

The Cloud Connect server checks for new software updates daily at a predefined time. When the new software updates are available, an email notification is sent. This email notification consists of available software updates details along with the release notes and is triggered to the administrators who have subscribed for it.

Email notifications are also sent to provide updates on the success and failure of any upgrade, rollback, or switch forward procedure. These notifications include details such as:

- Specific nodes on which the upgrade, rollback, or switch forward is initiated.
- Cloud Connect server name from where the procedure is triggered.
- Time (Cloud Connect server time) at which the procedure is started.
- Details about build versions of the respective nodes. For example, for an upgrade procedure, it shows both the version from which it is upgraded (FromVersion) and the version to which it is upgraded (ToVersion).
- Status of the procedure for respective nodes to indicate whether the procedure is successful or has failed; the subject line of the email indicates the overall status: success, failure, or partial success.

Cloud Connect server downloads the available software from Cisco software repository every day at the configured time. Email notification is triggered from Cloud Connect server to subscribed users with software download failure details. Also, Cisco software artifactory will trigger an email notification with entitlement or compliance failure details to the email address mapped to CCO ID that is used to generate the Artifactory API key.

Note

- If the option "All nodes" is selected during the upgrade, an email notification is sent about the success or failure at each stage of upgrade.
- The name of the deployment is shown in the subject line of the email, depending on the configuration in the inventory file.
- For patch install or rollback, email notifications are not sent to indicate whether the procedure is successful or if it is a failure.

Orchestration in CCE Deployment

The Orchestration feature is part of the Cloud Connect node that is configured in the CCE deployment.

To access this feature, Cloud Connect must be added to the inventory in the Unified CCE Administration console.

For more information, see *Configure Cloud Connect* section in the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

System Requirements

Cloud Connect 12.5(x) is obsolete. Cloud Connect 12.6(x) is required.

VOS Component Upgrade

Refer below for the minimum software version required to enable this feature for the following components:

- Finesse
- CUIC/LD/IDS/Co-resident
- VVB

Apply the ES **ucos.orchestration.enable-12.5.1.cop.sgn** on the above-mentioned components with 12.5(1) version to on-board and orchestrate VOS nodes from Cloud Connect server.

Note The ES **ucos.orchestration.enable-12.5.1.cop.sgn** must be applied on both the publisher and subscriber target nodes. This mandatory ES is not required for onboarding the above-mentioned components with 12.6(x) version. After you install this ES on target VOS node, you will not be able to run commands in the same session. You must restart the session on target nodes to use the Orchestration CLI commands.

Note

- Before you begin the VOS node upgrade from 12.6(1) to 12.6(2), check if the **ucos.keymanagement.v02.cop.sgn** is applied on the base version. If not, you must install it; else the upgrade will fail. Restart the VOS node after installing **ucos.keymanagement.v02.cop.sgn**.
- Before you begin the VOS node upgrade from 12.5(1) to 12.6(2), check if the **ucos.keymanagement.v01.cop.sgn** is applied on the base version. If not, you must install it; else the upgrade will fail. Restart the VOS node after installing **ucos.keymanagement.v01.cop.sgn**

Windows Component Upgrade

Manually install mandatory ES23 on Unified CVP 12.5 (1) and ES66 on Unified ICM 12.5 (1) to onboard and orchestrate Windows nodes from Cloud Connect server.

Note For 12.5(1) Windows and VOS nodes, ES is required to onboard and orchestrate from Cloud Connect server. mandatory ES is not required for onboarding target Windows and VOS components with 12.6(x) version.

Orchestration Support using Cloud Connect Server

Cloud Connect 12.6(x) supports orchestration in the following scenarios:

- Unified CCE 12.5(x) ES, Unified CCE 12.6(x) ES and Windows Updates can be orchestrated from Cloud Connect 12.6(x)
- Unified CCE 12.5(x) to Unified CCE 12.6(x), software upgrade can be orchestrated from Cloud Connect 12.6(x)

See System Requirements, on page 120 for minimum software requirement to enable orchestration for the above supported model.

Parallel Running of CLI

Parallel running of same or different CLIs on Cloud Connect server is disabled for Orchestration. However, parallel running of CLIs is allowed for the following commands:

- set cloudconnect orchestration config
- show cloudconnect orchestration config
- utils image-repository show
- utils deployment compatibility-check
- utils deployment show in-progress
- utils system inventory export
- utils system inventory import
- utils deployment show progress-HA

- email configuration-related commands, see Configure Email Notification.
- utils set software-download time
- utils set software-download bandwidth

Orchestration Deployment Task Flow

CLI to configure artifactory URL and API key, on page 125
Generate the Artifactory API Key, on page 123
CLI to configure proxy for orchestration, on page 124
Onboard VOS Nodes to Orchestration Control Node, on page 129
Onboard Windows nodes to orchestration control node, on page 130
Add Deployment Type and Deployment Name, on page 132
Validate Onboarded Nodes for Orchestration, on page 132
Configure Email Notification, on page 133
Configure Windows Server for Updates (Optional), on page 135

Administration Task Flow

Check Installed Software Version and Patches, on page 135
Install or Rollback Patch or Upgrade Cloud Connect Server , on page 135
List Available Patches for Specific Node or Group of Nodes, on page 137
Install Patch to Specific Node or Group of Nodes, on page 137
Roll Back Patch from Specific Node or Group of Nodes, on page 138
Install Windows Updates to Specific Node or Group of Nodes, on page 139
Roll Back Windows Update from Specific Node or Group of Nodes, on page 141
Enable or Disable Compatibility Enforcement, on page 142
Initiate maintenance mode for a specific node(s), on page 143
List Available Upgrade Options , on page 144
Upgrade a Specific Node or Group of Nodes or All Nodes , on page 144
Perform Switch Forward on Specific VOS Node or Group of Nodes , on page 146
Roll Back Upgrade from Specific Node or Group of Nodes, on page 146
Check Last Known Orchestration Operation Status on Remote Node, on page 148
Check Status, on page 147
Start Unified ICM Services, on page 148

Maintenance Task Flow

CLI to configure software download schedule, on page 149
CLI to configure the bandwidth for Orchestration software download, on page 149
Enforce software download from Cisco hosted software artifactory, on page 151
Update VOS Nodes Onboarded to Orchestration Control Node, on page 151
Remove VOS Nodes from Orchestration Control Node, on page 151
Update Windows Nodes Onboarded to Orchestration Control Node, on page 152
Validate Updated Nodes Onboarded for Orchestration, on page 152
Configure Email Configuration, on page 152
Delete Configuration for Email Notification, on page 153
Unsubscribe Email Notification, on page 154
Export and Import of Nodes Managed by Orchestration Control Node, on page 154
Export Current Patch Level Details, on page 155
Serviceability, on page 156
Enable and View Windows Open SSH Logs, on page 157

Deployment Tasks

Generate the Artifactory API Key

To generate the Artifactory API Key, follow the steps below:

Note It is mandatory for the CCO ID used to generate API keys to have necessary software upgrade entitlements. The CCO ID used by the partner or customer should have a valid SWSS (service contract) or Flex subscription in order to have the necessary entitlement.

- Login to https://devhub-download.cisco.com/console/ using your CCO Username and Password.
- Navigate to '**Manage Download Key** page.
- Click Generate Key option to Generate the API key. Option to **View** and **Revoke** Key is available in **Manage Download Key** page.
- Click on the Copy option to copy the API key to the clipboard.

Note You must log into https://devhub-download.cisco.com/console once every six months to extend the validity of the API key.

Note Cisco recommends not to use the same Artifactory API key generated by a single CCO ID across multiple deployments. For multiple deployments such as test, pre-production, production, and so on, generate the Artifactory API key for each deployment using different CCO IDs. Artifactory API key generated by a single CCO ID can be used in both publisher and subscriber of Cloud Connect in a single deployment.

CLI to configure proxy for orchestration

You can enable proxy configuration for orchestration to check and fetch updates from the Cisco-hosted cloud artifactory.

To configure the proxy for orchestration, run the **set cloudconnect orchestration config** command. To view the proxy configured for orchestration, run the **show cloudconnect orchestration config** command.

Table 4: Set Command Table

Command	**set cloudconnect orchestration config**
Description	This command enables the proxy configuration for orchestration to check and fetch updates from the Cisco-hosted cloud artifactory.
Expected Inputs	In the *Proxy Configured* prompt, enter **Yes** to enable the proxy or **No** to turn-off the proxy. If you choose to enable the proxy, you will be prompted to enter the Proxy Host and Proxy Port details. **Note** • Proxy Host should be the proxy server FQDN or IP address. • Proxy is turned off by default. • Orchestration supports only HTTPS proxy.
Expected Outcome	This CLI enables or turns-off the proxy for orchestration based on user input.

Note You can run this command only from the publisher node of the Cloud Connect server. The proxy configuration replicates automatically from the publisher node to the subscriber node when the **set cloudconnect orchestration config** command is run successfully on the publisher node.

Table 5: Show Command Table

Command	**show cloudconnect orchestration config**
Description	This command displays the proxy configuration for orchestration to check and fetch updates from the Cisco-hosted cloud artifactory.
Expected Inputs	NA

Expected Outcome	Proxy Host and Proxy Port details will be displayed if proxy is enabled.

CLI to configure artifactory URL and API key

Cisco hosts all the software artifacts in a cloud-based artifactory. The Cloud Connect server uses this artifactory to download and notify new updates.

Configure the Cloud Connect server with Cisco-hosted software Artifactory URL, Repository Name, and API Key. Run the command **utils image-repository set**. Refer to the **Set Command** table.

To view the configured Artifactory URL, Repository Name, and API Key in the Cloud Connect server, run the command **utils image-repository show**. Refer to the **Show Command** table.

Note You can run the **utils image-repository set** command only in the publisher node of the Cloud Connect server. The replication of image repository configuration occurs automatically from the publisher node to the subscriber node when you run this command with successful results on the publisher node.

Note Before running the command **utils image-repository set** on the CLI, access the link https://software.cisco.com/download/eula and accept the End User License Agreement (EULA)

Table 6: Set Command Table

Command	**utils image-repository set**

Description	

	This command allows you to configure the Cisco hosted software Artifactory URL, Artifactory Repository Name, and API Key. For information on API Key, refer to the Generate the Artifactory API Key section. This command validates the below:
	• If the Cisco.com ID used to generate the API key has entitlement to download the Cisco Contact Center software.
	• If the EULA is signed by the Cisco.com ID that generates the API key.
	• If the Cisco.com ID that generates the API key has the customer company's full address that is updated in the Cisco.com profile and validated by Cisco.
	• If the Cloud Connect server is deployed in embargoed countries where software download is restricted.
	• If the user has valid authentication token that is associated with the API key.
	If the user doesn't have a valid authentication token associated with the API key, then the user has to sign in to https://devhub-download.cisco.com/console/ to extend the validity of the API key.
	If compliance validation fails, the Cisco.com ID user must perform the below-mentioned actions:
	• For EULA compliance failure, confirm that you have read and agreed to be bound by the terms of Cisco EULA. Access the link https://software.cisco.com/download/eula to view and accept the agreement.
	• For customer company's address verification failure, access the link https://rpfa.cloudapps.cisco.com/rpfa/profile/profile_management.do to update the address.
	• For Entitlement failure, where Cisco service contract information indicates that you're not authorized to download the Contact Center software, perform one or more of the following actions:
	  • Identify the product name and MDFID of the Contact Center product for which the entitlement failed. To find the product name and corresponding MDFID of the product, check the CLI log for the keyword **Entitlement check failed for MDFID**. Refer to the Serviceability section for the command to retrieve the CLI log.
	  • The service contract or subscription containing coverage for the product may not be associated to the Cisco.com user ID. To associate the relevant service contract to the Cisco user ID, use the **Cisco Profile Manager**, and select **Add Access** to request access to the contract (which can now be done using the Serial Number of the product).

	• If your software is covered by a Smart License subscription, go to Cisco Software Central to request access to your company's Smart Account in the **Administration** section. Contact your Cisco representative, partner, or reseller to ensure that the product is covered by a service contract or subscription that is associated with your Cisco.com user ID. Use the Partner Locator link to locate your nearest partner. For assistance, contact your Cisco Accounts Manager or Partner. To expedite your request, include the following information: • User ID (Cisco.com ID used to generate the API key) • Contact Name • Company Name • Contract Number • Product ID or MDFID, Product Name, and Release • You can obtain access to U.S. export-restricted software by completing the K9 agreement form. **Note** Upon successful configuration of artifactory details, artifacts are downloaded locally to the Cloud Connect server periodically at the configured time. During artifact download, the compliance validation is done. The Cisco.com ID user performs the above-mentioned actions for any compliance failure during artifact download.
Expected Inputs	User should input Artifactory URL, Artifactory Repository Name, and API Key. The Cisco-hosted software Artifactory URL is https://devhub-download.cisco.com/binaries and Artifactory Repository Name is `ent-platform-release-external`. **Note** Cisco recommends not to use the same Artifactory API key generated by a single CCO ID across multiple deployments. For multiple deployments such as test, pre-production, production, and so on, generate the Artifactory API key for each deployment using different CCO IDs. Artifactory API key generated by a single CCO ID can be used in both publisher and subscriber of Cloud Connect in a single deployment. CLI provides an option to the customer to choose between using export-restricted and unrestricted software, based on the entitlement associated with the Cisco.com ID. For example, VVB has export-restricted and unrestricted software.

Expected Outcome	This CLI validates the entitlement associated with the Cisco.com ID and connection to the Cisco-hosted software artifactory using the given configuration. Based on successful validation, the artifactory details are configured in the Cloud Connect server.

Note Use the command **utils image-repository set** to change export-restricted or unrestricted software in the deployment. Use the CLI **utils initiate software-download** to enforce the cleanup and download the restricted vs unrestricted software.

Note On the successful configuration of artifactory details, artifacts are downloaded locally to the Cloud Connect server at the scheduled or default time. Orchestration operations such as patch install, rollback, or upgrade can be performed only after the artifacts are downloaded. If you need to download the artifacts immediately after the configuration, use the **utils initiate software-download** CLI. Usage of orchestration-related CLI is blocked during download, and this duration depends on the number of artifacts to be downloaded.

Note Before you configure the bandwidth using the **utils set software-download bandwidth** command, make sure the software is downloaded locally for the first time after the artifactory is successfully configured using the **utils image-repository set** command. To download the artifacts immediately after the configuration, use the **utils initiate software-download** command.

Table 7: Show Command Table

Command	**utils image-repository show**
Description	This command displays the configured Cisco-hosted software Artifactory URL, Repository Name, and the API Key (the mix of hash and last 4 characters of key) in the Cloud Connect server.
Expected Inputs	NA
Expected Outcome	Displays the configured Artifactory URL, Repository Name, and the API Key.

Onboard VOS Nodes to Orchestration Control Node

The onboarding process helps to establish a password-less connection between the Cloud Connect node and the VOS nodes.

Prerequisites:

- Ensure that the Cloud Connect server and target nodes maintain the minimum software versions that are required as outlined in System Requirements.
- If you are using self-signed certificates, import the self-signed Tomcat certificate of the Cloud Connect server into the VOS nodes which you have to onboard. Ensure to import both Cloud Connect publisher

and subscriber node certificates on all VOS publisher and subscriber nodes. For details, see Self-Signed Certificate, on page 158.

To onboard Finesse, CUIC, VVB, IDS, LD to a Cloud Connect server, run the **utils system onboard initiate** command from the publisher node of the respective VOS cluster that you wish to onboard. The publisher node of the Cloud Connect server must be up and running when onboarding is initiated from VOS node. When the onboarding is initiated from VOS node, FQDN of the Cloud Connect server must be used.

Command	**utils system onboard initiate**
Description	This command is used to onboard a VOS node such as Finesse, CUIC, VVB, etc., to a Cloud Connect server.
Expected Inputs	When run, the command prompts for: • Cloud Connect server FQDN • Cloud Connect application username • Password
Expected Outcome	The nodes are onboarded to the Cloud Connect server orchestration inventory. A message is displayed indicating the status.

Note If the system (cluster) onboards to the Cloud Connect server with partial error, check the reason for the error and correct it. Then, run the **utils system onboard update** command instead of running the **utils system onboard initiate** command.

Note Onboarding is allowed only when all the publisher and subscriber nodes in the Cloud Connect server are reachable.

Note If the Cloud Connect server is corrupted and redeployed by doing fresh install, the administrator has to run **utils system onboard remove** from the VOS node and then run **utils system onboard initiate** to onboard the VOS nodes again.

Onboard Windows nodes to orchestration control node

The onboarding process helps to establish a password-less connection between the Cloud Connect node and the Windows nodes. To onboard the Windows-based nodes to orchestration control node, perform the following steps:

Procedure

Step 1 Configure SSH public key on the Windows nodes by following the steps in the section Configure SSH public key on Windows nodes, on page 157.

Step 2 From the cloud connect server, run the **utils system inventory export** command to download the inventory to an SFTP server. For details, see Export and Import of Nodes Managed by Orchestration Control Node, on page 154.

Step 3 Edit the inventory file to include the Windows components. Refer to the default template section in the inventory file.

Note
- The syntax, alignment, and indentation must be exactly the same as mentioned in the inventory file.
- Ensure the CRLF line endings are of UNIX-Style. Use a Linux-based or a Mac OS-based editor to create the Windows inventory file.

The following fields in the inventory file are mandatory.

Field	Description
ProductName	The **ProductName** mentioned in the inventory file must be in uppercase and cannot be changed. For example, CVPREPORTING, CVPSERVER, CVPOAMP, DISTRIBUTOR, LOGGER, PG, ROGGER or ROUTER.
Pair under product	This is a user-defined pair name.
Hostname	This can be a valid IP, or hostname, or FQDN name of the target node.
Side of the deployment	It can either be A or B.
User configured on host	This is the username for which the SSH keys are configured in Step 1. **Note** The user must have either domain admin or local administrator privilege. **Note** User name can be in User Principal Name (UPN) format or Domain username (domain\username) format for domain administrator or local administrator user name. Example: UPN format : administrator@stooges.icm Domain Administrator: stooges\administrator Local Administrator: administrator

Step 4 Import the inventory back from the SFTP server by running the command **utils system inventory import** on the Cloud Connect publisher node. For details, see Export and Import of Nodes Managed by Orchestration Control Node, on page 154.

Add Deployment Type and Deployment Name

An administrator can edit the inventory file to add the details of the deployment.

Procedure

Step 1 Download the inventory to an SFTP server by running the utils system inventory export command. For details, see Export and Import of Nodes Managed by Orchestration Control Node, on page 154.

Step 2 Edit the following strings in the inventory file, if required.

- **deploymentType**: This field is used for compatibility check during an upgrade or rollback or switch forward procedure. The supported deployment types are:
  - UCCE-2000-Agents
  - UCCE-4000-Agents
  - PCCE-2000-Agents
  - PCCE-4000-Agents

  Note Orchestration is not supported for 12000, 24000 and 36000 agent deployment models.

  Ensure that the values entered in this field conform to the above format. The deployment type is case sensitive.

- **deploymentName**: Provide a unique name for the deployment.

  This name appears in the subject line of the email notification. If it is not configured, the subject line of the email notification contains only the type of procedure and the overall status.

Note The administrator can update or edit the default values, if required, based on their deployment type and preferred deployment name.

Step 3 Import the inventory back from the SFTP server by running the utils system inventory import command on the Cloud Connect publisher node. For details, see Export and Import of Nodes Managed by Orchestration Control Node, on page 154.

Validate Onboarded Nodes for Orchestration

To validate the onboarding of VOS and Windows nodes, and to check whether the Orchestration feature is ready to be used, run the **utils deployment test-connection** command.

Command	**utils deployment test-connection**
Description	This command is used to validate whether password-less SSH connection is successful between the onboarded nodes and the Cloud Connect server. You can test the connection to all nodes on the deployment or to a specific group or individual nodes.
Expected Inputs	NA

Expected Outcome	Shows whether the inventory is accurate and the Cloud Connect node is able to connect to the managed hosts.

Configure Email Notification

If an email notification is configured, the Cloud Connect server checks the Cisco-hosted artifact repository periodically at scheduled times and sends email notifications along with the release notes when new software updates are available. Administrators can decide when to apply a patch or perform an upgrade. Email notifications are not triggered if no new software updates are available.

Note The SMTP server referred to in this section is the mail server that is used within the customer organization for their internal email communication.

Perform the following procedures in the same sequence as given here.

1	Set up Email Notification, on page 133
2	Validate Email Configuration, on page 134
3	Subscribe to Email Notification, on page 134
4	Configure Email Notification, on page 133

Set up Email Notification

Configure the email notification by running the following set of commands:

- Set the IP address or hostname of the SMTP server by running the **set smtp-host** command.

Command	**set smtp-host**
Description	This command is used to set the IP address or hostname of the SMTP server.
Expected Inputs	SMTP server IP Address/HostName
Expected Outcome	The SMTP address is updated.

- Set the email address from which emails are triggered by running the **set smtp-from-email** command.

Command	**set smtp-from-email**
Description	This command is used to set the email address from which the emails are triggered. This email address is not monitored and therefore not used for replying to any emails.
Expected Inputs	When run, this command takes an input for a complete email address.
Expected Outcome	Configures the email address from which email notifications are triggered.

- Enable or disable SMTP authentication by running the **set smtp-use-auth** command.

Command	**set smtp-use-auth**

Description	This command is used to enable or disable SMTP authentication. By default, this is disabled.
Expected Inputs	The command takes an input for the values Enable or Disable.
Expected Outcome	SMTP authentication type is updated.

- Set the username to be used for SMTP server connection by running the **set smtp-user** command. This is an optional configuration that needs to be set only when the SMTP authentication is enabled.

Command	**set smtp-user**
Description	This command is used to set the username to be used for SMTP server connection.
Expected Inputs	The command takes an input for the username to be used for SMTP authentication.
Expected Outcome	Configures the SMTP username.

- Set the password for SMTP server connection by running the **set smtp-pswd** command. This is an optional configuration that needs to be set only when the SMTP authentication is enabled.

Command	**set smtp-pswd**
Description	This command is used to set the password for SMTP server connection. The password is stored in an encrypted format. To change the password, run this command again.
Expected Inputs	The command prompts for a password for the SMTP connection.
Expected Outcome	Configures the SMTP password.

Validate Email Configuration

Validate the configuration by running the **utils smtp test-connection** command.

Command	**utils smtp test-connection**
Description	This command is used to establish a connection to the SMTP server using the given configuration.
Expected Inputs	NA
Expected Outcome	Shows whether SMTP connection is successful or not.

Subscribe to Email Notification

Subscribe to email notifications by running the **utils smtp subscribe** command. Specify the email addresses to which the email notifications must be sent.

Command	**utils smtp subscribe**

Description	This command is used to specify the email addresses that subscribe to the email notifications. For example:
	`utils smtp subscribe`
	`<emailaddress1,emailaddress2,.....emailaddressesN>`

Expected Inputs	Comma-separated list of valid email addresses.
Expected Outcome	Email addresses provided are subscribed for notification.

Configure Windows Server for Updates (Optional)

Microsoft Windows update configuration needs to be done on the target Windows node. Microsoft Windows updates can be downloaded in one of following ways on the target Windows node:

- by directly connecting to the Microsoft server;
- from the Windows update server configured. To deploy or configure Windows server update services, refer to https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/deploy-windows-server-update-services.

Administration Tasks

Note Before upgrade or rollback of nodes managed by Orchestration, make sure to take backup as suggested by respective component documentation. Backup has to be done manually.

Note In case the upgrade or rollback on VOS node fails, then the respective VOS node restart is mandatory before attempting the next upgrade or rollback on the same node. If the administrator does not restart, the next attempt to upgrade or rollback might fail.

Check Installed Software Version and Patches

To check the currently installed software version and patches on a node or group of nodes or all nodes in either Windows or VOS systems, run the **utils deployment show status** command.

Command	**utils deployment show status**
Description	This command is used to check the currently installed software version and patches for the selected Windows or VOS node individually or group of nodes or for all nodes in the inventory by selecting the option 'All Nodes in the inventory'.
Expected Inputs	Select the node or group of nodes or all nodes from the inventory.
Expected Outcome	Displays information about the installed software version and the patches for the selected node or group of nodes or all nodes from the inventory. If there is no patch installed, a message "No patch installed" is displayed to indicate that along with software version.

Install or Rollback Patch or Upgrade Cloud Connect Server

To install a patch or to roll back a previously installed patch on Cloud Connect server or to upgrade Cloud Connect Server to next available version, run the **utils system upgrade initiate** command. The **Local**

Repository option in this command lists the patches and upgrade options available from Cisco artifactory for patch install or rollback or upgrade on Cloud Connect server. This command can be run separately on the Cloud Connect publisher and subscriber nodes.

Note The Cloud Connect publisher should be upgraded before upgrading the subscriber. The switch version on publisher should be done first before doing switch version on subscriber, use **utils system switch version** command to switch between versions.

Note The **Local Repository** option is also available on the Cisco Unified OS Administration web page of Cloud Connect server. Select this option to install a patch or to roll back a previously installed patch on Cloud Connect server or to upgrade Cloud Connect Server to next available version.

Command	**utils system upgrade initiate**
Description	This command is used to initiate the patch install or to roll back the previously installed patch on Cloud Connect server or to upgrade Cloud Connect Server to the next available version. The patches and upgrade options available for patch install or rollback or upgrade are listed from Cisco artifactory.
Expected Inputs	Select the **Local Repository** option to list the patches and upgrade options available for patch install or rollback or upgrade. Select the patch to install or roll back or upgrade option to upgrade Cloud Connect server.
Expected Outcome	The selected patch for install or rollback is installed on Cloud Connect server or selected upgrade option is used to upgrade the Cloud Connect server.

Note The **Local Repository** option is used only after the Cisco Artifactory is successfully configured on Cloud Connect server. See CLI to configure artifactory URL and API key, on page 125 for configuring Cisco artifactory.

Note Optionally, to receive email notification about the status of the patch installation or rollback or upgrade for Cloud Connect server, provide the SMTP host server details when prompted by the CLI.

Note Patch install or roll back or upgrade on Cloud Connect server initiated using **utils system upgrade initiate** command can be canceled using **utils system upgrade cancel** command. The **utils system upgrade status** command can be used to check the status.

List Available Patches for Specific Node or Group of Nodes

To get a list of available patches for a specific node or group of nodes in the inventory, run the **utils patch-manager list** command.

Command	**utils patch-manager list**
Description	This command is used to get a list of patches available for installation for a specific node or group of nodes based on the selected option.
Expected Inputs	Select a node or group of nodes based on the inventory.
Expected Outcome	Displays information about available patches for the selected node or group of nodes.

Install Patch to Specific Node or Group of Nodes

To install patch to a specific node or group of nodes, run the **utils patch-manager install** command.

Command	**utils patch-manager install**
Description	This command is used to install patches on a specific node or group of nodes onboarded to the Cloud Connect inventory.
Expected Inputs	From the list of Windows/VOS nodes displayed, select the node or group of Windows/VOS nodes on which the patch needs to be installed. Once you select the nodes, only the nodes for which patches are available will be displayed. For example, if you select 3 nodes and Windows/VOS patches are available for only 1 of them, you are asked to proceed with only one node. Confirm to proceed. You are also asked to confirm whether the target node needs to be rebooted after installing the patch. Selection of components such as Finesse, CVP Call Server, IdS, and PG with software version 12.6(x) will provide the options "With maintenance mode” and “Without maintenance mode”.. If you select a group of nodes with some nodes on 12.6(x) and some nodes below 12.6(x), then "With maintenance mode” or “Without maintenance mode” option will not be available. In this case if "With maintenance mode” option is required, then the individual node with 12.6(x) can be selected separately. If you select “With maintenance mode” option, the maintenance mode is initiated for the selected node to failover active traffic gracefully or shutdown the services gracefully without interrupting the active traffic or causing outage for new traffic before installing the patch and automatically rebooting. If you select, “Without maintenance mode” option, you are initially asked to confirm to proceed. Next, you are asked to provide confirmation on rebooting the node after installing the patch.
Expected Outcome	The selected patch is installed on the selected node or group of nodes.

Note To start Unified ICM services, post the successful completion of patch install with reboot on Unified ICM nodes. See Start Unified ICM Services.

Note You can check the status of the patch install which is currently in-progress. For more information, see Check Status, on page 147.

Note Maintenance mode for IDS co-resident in 2000 Agents Deployment model is not supported

Roll Back Patch from Specific Node or Group of Nodes

To roll back a previously installed patch on a specific node or a group of nodes, run the **utils patch-manager rollback** command.

Command	**utils patch-manager rollback**
Description	This command is used to roll back previously installed patches on a specific node or group of nodes. In case of Windows-based nodes, the latest applied patch is allowed to roll back. In case of VOS-based nodes, the latest applied ES is rolled back.

Expected Inputs	From the list of Windows/VOS nodes displayed, select the node or group of Windows/VOS nodes on which the patch needs to be rolled back. Once you select the nodes, only the nodes for which Windows/VOS patch rollback is available will be displayed. For example, if you select 3 nodes and Windows/VOS patch rollback is available for only 1 of them, you are asked to proceed with only one node. There is also a message displayed indicating that the machine would restart after the patch is rolled back. Confirm to proceed. Selection of components such as Finesse, CVP Call Server, IdS, and PG with software version 12.6(x) will provide the options "With maintenance mode" and "Without maintenance mode". If you select a group of nodes with some nodes on 12.6(x) and some nodes below 12.6(x), then "With maintenance mode" or "Without maintenance mode" option will not be available. In this case if "With maintenance mode" option is required, then the individual node with 12.6(x) can be selected separately. If you select "With maintenance mode" option, the maintenance mode is initiated for the selected node to failover active traffic gracefully or shutdown the services gracefully without interrupting the active traffic or causing outage for new traffic before rollback and automatically rebooting. If you select, "Without maintenance mode" option, you are initially asked to confirm to proceed. Next, you are asked to provide confirmation on rebooting the node after rollback.
Expected Outcome	The previously installed patch is rolled back on the selected node or group of nodes.

Note To start Unified ICM services, post the successful completion of patch roll back with reboot on Unified ICM nodes. See Start Unified ICM Services

Note You can check the status of patch rollback which is currently in-progress. For more information, see Check Status, on page 147.

Install Windows Updates to Specific Node or Group of Nodes

To install Windows updates to a node or group of nodes or all Windows nodes, run the **utils patch-manager ms-patches install** command.

Note Before running this command, refer to the recommended guidelines in the *Microsoft Security Updates* section of the *SecurityGuide for CiscoUnified ICM/Contact Center Enterprise* at:https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Microsoft Windows updates are NOT hosted on Cisco-hosted Software Artifactory. You must configure the target Windows node to fetch the Microsoft Windows updates, either by directly connecting to the Microsoft Server via Internet or from the Windows Update Server. For more details, refer to the Configure Windows Server for Updates (Optional) section. The **utils patch-manager ms-patches install** command will not list the available Windows updates for the administrator to choose for the target node. Instead, it will check the available updates for the below listed Windows update categories and install all the available updates:

- Application
- Connectors
- DefinitionUpdates
- DeveloperKits
- FeaturePacks
- Guidance
- ServicePacks
- Tools
- UpdateRollups
- CriticalUpdates
- SecurityUpdates
- Updates

The administrator can control the installation of Windows updates using Windows Update Server, instead of directly connecting to the Microsoft Server via Internet. Ansible log, generated during the running of **utils patch-manager ms-patches install** CLI, captures the details of the Windows updates, along with the Knowledge Base (KB) number of the updates that were installed on the target node. Refer to the Serviceability section for the command to retrieve the Ansible log.

Command	**utils patch-manager ms-patches install**
Description	This command is used to install the latest Windows updates to a node or a group of Windows nodes or all Windows nodes.

Expected Inputs	From the list of Windows nodes displayed, select the node or group of Windows nodes or all Windows nodes to which the updates need to be applied. You can also select all the Windows nodes in the inventory. Once you select the nodes, only the nodes for which Windows updates are available will be displayed. For example, if you select 3 nodes and Windows updates are available for only 1 of them, you are asked to proceed with only one node. Confirm to proceed. You are asked to confirm whether the target nodes needs to be rebooted after installing the updates. Selection of components such as CVP Call Server and PG with software version 12.6(x) will provide the options "With maintenance mode" and "Without maintenance mode". If you select a group of nodes with some nodes on 12.6(x) and some nodes below 12.6(x), then "With maintenance mode" or "Without maintenance mode" option will not be available. In this case if "With maintenance mode" option is required, then the individual node with 12.6(x) can be selected separately. If you select "With maintenance mode" option, the maintenance mode is initiated for the selected node to failover active traffic gracefully or shutdown the services gracefully without interrupting the active traffic or causing outage for new traffic before installing the update and automatically rebooting. If you select, "Without maintenance mode" option, you are initially asked to confirm to proceed. Next, you are asked to provide confirmation on rebooting the node after installing the patch.
Expected Outcome	The selected Windows updates are installed on the selected node or group of nodes or all Windows nodes.

Roll Back Windows Update from Specific Node or Group of Nodes

To roll back Windows update from a specific node or group of nodes or all Windows nodes, run the **utils patch-manager ms-patches rollback** command.

Note

- Before running this command, refer to the recommended guidelines in the *Microsoft Security Updates* section of the *SecurityGuide for CiscoUnified ICM/Contact Center Enterprise* at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html
- Listing of Windows updates available for rollback is not supported.

Command	**utils patch-manager ms-patches rollback**
Description	This command is used to roll back a specific Windows update from a specific node or group of nodes or all Windows nodes.

Expected Inputs	Select the node or group of Windows nodes or all Windows nodes on which the rollback needs to be performed. You can also select all the Windows nodes in the inventory for rollback. Provide the Knowledge Base (KB) number you want to rollback. You are asked to confirm whether the target nodes need to be rebooted after rollback. Selection of components such as CVP Call Server and PG with software version 12.6(x) will provide the options "With maintenance mode" and "Without maintenance mode". If you select a group of nodes with some nodes on 12.6(x) and some nodes below 12.6(x), then "With maintenance mode" or "Without maintenance mode" option will not be available. In this case if "With maintenance mode" option is required, then the individual node with 12.6(x) can be selected separately. If you select "With maintenance mode" option, the maintenance mode is initiated for the selected node to failover active traffic gracefully or shutdown the services gracefully without interrupting the active traffic or causing outage for new traffic after rollback and automatically rebooting. If you select, "Without maintenance mode" option, you are initially asked to confirm to proceed. Next, you are asked to provide confirmation on rebooting the node after rollback.
Expected Outcome	The selected Windows updates are rolled back.

Enable or Disable Compatibility Enforcement

You can enable or disable compatibility enforcement. When the compatibility enforcement is enabled, it ensures that the upgrade, rollback, or switch forward is as per the compatibility matrix published by Cisco for reference design-based deployment. To enable or disable compatibility enforcement, run the **utils deployment compatibility-check** command.

Note By default, the compatibility enforcement is enabled.

When the compatibility enforcement is disabled, the Orchestration framework does not enforce upgrade, rollback, or switch forward as per the compatibility matrix published by Cisco.

Command	**utils deployment compatibility-check**
Description	This command is used to enable or disable compatibility enforcement.
Expected Inputs	User confirmation to proceed with enabling or disabling compatibility enforcement.
Expected Outcome	Message about the success or failure of enabling or disabling compatibility enforcement.

Note You can run this command only from the publisher node of the Cloud Connect server. The compatibility configuration replicates automatically from the publisher node to the subscriber node when the **utils deployment compatibility-check** command is run with successful results on the publisher node.

Initiate maintenance mode for a specific node(s)

Initiating maintenance mode allows the components to failover gracefully or shutdown the services gracefully (depending on the selected components) without interrupting the active traffic or causing outage to new traffic. This ensures that the system can be taken down for maintenance activity such as installing new software updates, restarting services etc. Currently, maintenance mode is supported for PG, CVP server, IdS, and Finesse.

Note Ensure that not all CVP servers are put into maintenance mode at same time, so that incoming call traffic can be distributed.

To initiate maintenance mode for a specific node in the inventory, run the **utils system maintenance initiate** command.

Command	**utils system maintenance initiate**
Description	This command is used to initiate maintenance mode for a specific node based on the selected option. Currently, the initiate maintenance command is available for Finesse, CVP Call Server, IdS, and PG components.
Expected Inputs	When run, this command prompts you to select a node based on the inventory.
Expected Outcome	Information about success or failure of the initiate maintenance command for a selected node is displayed.

Note The **utils system maintenance initiate** is applicable for target nodes on CCE 12.6(1) and above.

Note If either the Publisher or Subcriber or the active/inactive node is already in maintenance mode in any of the components, the other server cannot be initiated for maintenance.

Note You can check the status of system maintenance initiate which is currently in-progress. For more information, see Check Status, on page 147.

Note Maintenance mode for IDS co-resident in 2000 Agents Deployment model is not supported

List Available Upgrade Options

To get a list of available upgrade options for VOS and Windows nodes individually or for group of nodes or for all nodes in the inventory, run the **utils upgrade-manager list** command.

Command	**utils upgrade-manager list**
Description	This command is used to get a list of upgrade options available for the selected VOS or Windows node or group of nodes or all nodes in the inventory by selecting the option "All nodes in the inventory"..
Expected Inputs	Select a node or group of nodes or all nodes based on the inventory.
Expected Outcome	Displays information about available upgrade options for selected VOS or Windows nodes or group of nodes or all nodes in the inventory. If the selected node or group of nodes or all nodes are already running the latest software version, a message is displayed to indicate that.

Upgrade a Specific Node or Group of Nodes or All Nodes

To perform software version upgrades on VOS or Windows nodes or All nodes in the deployment (VOS and Windows nodes together), run the **utils upgrade-manager upgrade** command from the Cloud Connect server. It is recommended to run this command during a maintenance window as the procedure involves system restart that will cause service outage.

For the selected VOS or Windows component for upgrade, a compatibility check is performed in the background based on the configured deployment type to ensure that all the associated components are onboarded. If the components are onboarded and the required dependent components are either in same target upgrade version or backward compatible version, the upgrade procedure begins. However, if the components are not onboarded, you have to onboard them first or if the versions are not compatible, upgrade them to the required version. For example, if you select to upgrade the Rogger nodes to 12.6(1) version, the inter-component compatibility check is run for the Rogger dependent components such as Finesse, CVP, VVB, CUIC. These must already be in 12.6(1) version and PG must be backward compatible version, that is, 12.5(1) .

Note The sub-components sequence dependencies are not validated as part of the upgrade compatibility. Refer to the upgrade guides of the respective components for the correct sequence. For example, in case of CVP, we have sub-components such as Operations Console, Unified CVP Reporting Server and Unified CVP Server. These must be upgraded in the required sequence.

For VOS node/cluster, switch forward is optional at the end of upgrade. If administrators opt for switch forward, the target node is restarted and the active/inactive partition is switched. If they decide not to switch forward, the upgraded version remains in the inactive partition of the target node. Switch forward for these nodes can be performed later. For details, see Perform Switch Forward on Specific VOS Node or Group of Nodes , on page 146.

For VOS cluster, the upgrade or the switch forward procedure is performed first on the publisher and then on the subscriber nodes. If switch forward is performed immediately after an upgrade, the overall procedure takes a significant amount of time; hence plan the maintenance window accordingly.

For selecting "All nodes" option during upgrade, make sure that all the VOS and Windows nodes onboarded are on the same software version. Stage-wise upgrade is performed for the solution components as per the *CCE Installation and Upgrade guide*. In case of any component upgrade failure during the process, the upgrade does not proceed to the next stage. The administrator has to upgrade individual components by selecting the respective individual VOS or Windows nodes.

Command	**utils upgrade-manager upgrade**
Description	This command is used to upgrade VOS or Windows nodes or group of nodes or All nodes in the deployment (VOS and Windows nodes together) in the inventory.
Expected Inputs	Select the Windows or VOS node or group of nodes or all nodes in the deployment (VOS and Windows nodes together) that you want to upgrade. From the list of upgrade options available for the selected node or group of nodes or all nodes, select the appropriate option and confirm. A compatibility check is then run in the background. To select "All nodes" upgrade option, make sure that all the VOS and Windows nodes onboarded and the components are on the same software version. Once the upgrade procedure begins, you can see the progress details for each of the machines. You can also see the elapsed time since the procedure started.
Expected Outcome	The selected node or group of nodes or all nodes is upgraded.

Note

- For faster upgrades, the Cloud Connect server downloads locally all the new software updates from the Cisco hosted repository at a predefined time.
- To start the Unified ICM services, post the successful completion of upgrade with reboot on Unified ICM nodes. See Start Unified ICM Services.
- Upgrade of all nodes to CCE 12.6(2) will be supported for the following scenarios:
  - All CCE components are on 12.6(1)
  - All CCE components are on 12.5(1)
  - All ICM and VOS components are on 12.5(2) and all CVP components are on 12.5(1)

Note You can check the status of upgrade which is currently in-progress. For more information, see Check Status, on page 147.

Perform Switch Forward on Specific VOS Node or Group of Nodes

Administrators can perform switch forward on target VOS nodes independently. When the active partition is on lower version and the inactive partition is on higher version, run the **utils upgrade-manager switch-forward** command to perform a switch forward. It is recommended to run this command during a maintenance window as the procedure involves system restart that will cause service outage.

Command	**utils upgrade-manager switch-forward**
Description	This command is used to switch forward on target VOS node/cluster from Cloud Connect server.
Expected Inputs	Select the VOS node/cluster on which you want to perform the switch forward. You will see the details of the current active/inactive versions. Confirm to proceed with the switch forward. A compatibility check is then run in the background. • If there are components whose versions are not compatible or the components are not onboarded as per the compatibility requirements, a list of those components is displayed. Upgrade or switch forward the listed components to the required software versions and re-run this command. • If the versions of the associated components are compatible with the node's inactive version, then the switch forward procedure continues. Once the switch-forward procedure begins, you can see the progress details for each of the machines. You can also see the elapsed time since the procedure started.
Expected Outcome	The system restarts and the current version of the system is on a higher version.

Note You can check the status of switch forward which is currently in-progress. For more information, see Check Status, on page 147.

Roll Back Upgrade from Specific Node or Group of Nodes

To roll back an upgrade on VOS or Windows nodes, run the **utils upgrade-manager rollback** command from the Cloud Connect server. It is recommended to run this command during a maintenance window as the procedure involves system restart that will cause service outage.

For the selected VOS or Windows component for rollback, a compatibility check is performed in the background to ensure that all the associated components are onboarded and the versions are compatible. If the components are onboarded and the versions are compatible with each other, the rollback procedure begins. However, if the components are not onboarded, you have to onboard them first or if the versions are not compatible, roll them back to the required version.

For VOS nodes/cluster, the rollback (switch backward) must be initiated from an active higher version to an inactive lower version of the node. Also, the publisher node of the managed cluster must be rolled back before the subscriber node of the cluster.

Command	utils upgrade-manager rollback
Description	This command is used to roll back an upgrade on VOS or Windows nodes.
Expected Inputs	Select the Windows node or VOS node/cluster on which you want to perform the rollback. The rollback option is listed for the selected node or group of nodes. Select the appropriate option and confirm. A compatibility check is then run in the background. • If there are components whose versions are not compatible or if the components are not onboarded as per the compatibility requirements, a list of these components is displayed. Roll back the listed components to the required software versions and then re-run this command. • If the versions of the associated components are compatible with the selected node's rollback version, then the rollback procedure begins. Once the rollback procedure begins, you can see the progress details for each of the machines. You can also see the elapsed time since the procedure started.
Expected Outcome	The selected node or group of nodes is rolled back.

Note To start Unified ICM services, post the successful completion of roll back upgrade with reboot on Unified ICM nodes. See Start Unified ICM Services.

Note You can check the status of rollback which is currently in-progress. For more information, see Check Status, on page 147.

Check Status

To check the current status of patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forward, or system maintenance initiate, run the **utils deployment show in-progress** command. You can run this command if connectivity to CLI is lost after initiating any of above procedures.

Command	utils deployment show in-progress
Description	This command is used to check the current status of any patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forward or system maintenance initiate. It also shows the subsequent progress, if applicable, for each node on which the procedure is initiated. If there is no procedure in progress, this command gives the last successful/failed procedure status.

Expected Inputs	NA
Expected Outcome	Shows the current status of the patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forwardor system maintenance initiate for each node. If there is no patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forward, or system maintenance initiate, then you see the status of the previous upgrade, rollback, or maintenance.

Check Last Known Orchestration Operation Status on Remote Node

To check the last known orchestration operation status (last completed state or last known state when the operation is in progress or when the remote node is not reachable) on the remote node, run the **utils deployment show progress-HA** command. This command is applicable for patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, ms patch install, ms patch rollback, switch-forward, system maintenance initiate, and Unified ICM services start.

This command can be used only in Cloud Connect High Availability setup

Command	**utils deployment show progress-HA**
Description	This command is used to check the last known operation status run on remote node. This will only display the snapshot of the last known operation status and will not display the continuous status changes for the operation that is currently in progress. This command can be used to check the last known operation status on the remote node when the Cloud Connect node is not reachable.
Expected Inputs	NA
Expected Outcome	The snapshot of the last known operation status is displayed.

Note Last known orchestration operation status will not be synchronized to remote node, in case of communication loss to remote node after initiating the orchestration operation and operation being completed before re-establishing the communication.

Start Unified ICM Services

To start Unified ICM services from Cloud Connect server, run the **utils system icm-services start** command.

Command	**utils system icm-services start**
Description	This command is used to start the Unified ICM services from Cloud Connect server. This CLI will present the user with a list of Unified ICM hosts configured in the inventory, and the admin can select individual or group of Unified ICM hosts.

Expected Inputs	User should choose individual or group of Unified ICM hosts from the list. User should give confirmation yes/no to proceed with start of Unified ICM services
Expected Outcome	As part of CLI output, there are two kinds of messages which displays success as shown below: • When the Unified ICM services are started successfully from stop state, the message "**Services started**" is displayed. • When the Unified ICM services are already up and running, the message "**Services running**" is displayed.

Maintenance Tasks

CLI to configure software download schedule

To change the default schedule for the software download from the Cisco-hosted software artifactory or to change the previously configured software download schedule, run the **utils set software-download time** command.

Command	**utils set software-download time**
Description	This command changes the default or the previously configured schedule for the software download from the Cisco-hosted software artifactory.
Expected inputs	Displays the currently configured software download time and prompts you to enter the new time (HH:MM in 24-hours format).
Expected outcome	Displays the success or failure message for the software download time configuration.

Note

- Cisco recommends that you change the default software download schedule based on your preference.
- Make sure that you configure the time for software download on the publisher and subscriber separately.
- Cisco recommends to set different software download time in Cloud Connect publisher and subscriber, preferably 1 hour apart. For example, if Cloud Connect publisher is set with the download time 3:00 AM, then set Cloud Connect subscriber with the download time 4:00 AM. Avoid using 1:00 AM and 5:00 AM for the software download as this time conflicts with other automatic orchestration operation.
- Default software download time is 2:00 AM Cloud Connect server time.

CLI to configure the bandwidth for Orchestration software download

To configure the bandwidth that the Orchestration feature uses to download the software from Cisco hosted software artifactory to Cloud Connect server, run the **utils set software-download bandwidth** command.

Note Before you configure the bandwidth using the **utils set software-download bandwidth** command, make sure the software is downloaded locally for the first time after the artifactory is successfully configured using the **utils image-repository set** command. To download the artifacts immediately after the configuration, use the **utils initiate software-download** command.

Command	**utils set software-download bandwidth**
Description	This command configures the bandwidth that the Orchestration feature uses to download software.
Expected inputs	When run, this command prompts for the following: • Your confirmation with yes or no for turn-on or turn-off the bandwidth configuration. • Enter a valid bandwidth value if you have chosen to turn-on the bandwidth configuration. **Note** • Make sure to suffix the bandwidth value with M for Mbps, K for Kbps and None for Bytes per second.
Expected outcome	Following are the outcomes: • Displays the success or failure message when you turn-on or turn-off the bandwidth configuration. • If you have turned-on the bandwidth configuration and entered a valid value, this CLI validates and configures the entered bandwidth value.

Note

- Make sure that you configure the bandwidth for software download, on the publisher and subscriber separately.
- Software download bandwidth control is disabled by default. The maximum available bandwidth is used during software download. This might have an impact on the features supported by Cloud Connect only during software download.
- Cisco recommends minimum10-Mbps bandwidth for optimal software download. If you configure the bandwidth to a value that is lesser than 10-Mbps, the duration of the software download increases and the orchestration operations cannot be performed during the software download duration. If you configure the bandwidth to a value that is greater than the maximum available bandwidth, the software download uses only the maximum available bandwidth.
- Proxy configured for orchestration might have an impact on the maximum available bandwidth for software download. Check the proxy configuration and ensure the configured bandwidth will be available for the software download when proxy is used for orchestration.

Enforce software download from Cisco hosted software artifactory

To initiate software download from Cisco hosted software artifactory to cloud connect server, run the **utils initiate software-download** command.

Command	**utils initiate software-download**
Description	This command initiates the software download from Cisco hosted software artifactory to Cloud Connect server.
Expected inputs	User confirmation with yes or no to proceed with software download.
Expected outcome	Displays the CLI message about the success or failure for the software download initiated.

Note

- Software download must be planned during off-peak hours as it consumes network bandwidth and resources. The duration of the download depends on the number of software that needs to be downloaded.
- Periodic software download happens everyday at 2 AM or at the time configured by admin. Use this CLI to initiate software download before the next scheduled download.
- Software download needs to be initiated in the publisher and the subscriber separately. While software download is in progress on the publisher, you can run the orchestration operation from the subscriber, or vice-versa.
- This CLI only initiates the software download and the download starts after prerequisites are met.

Update VOS Nodes Onboarded to Orchestration Control Node

To update VOS based nodes that have been onboarded, run the **utils system onboard update** command from the publisher node in the VOS node/cluster that you want to update.

Command	**utils system onboard update**
Description	This command is used to update a node/cluster on a Cloud Connect node.
Expected Inputs	When run, this command prompts for: • Cloud Connect server FQDN • Cloud Connect application username and password
Expected Outcome	The existing node/cluster is updated in the Cloud Connect node inventory.

Remove VOS Nodes from Orchestration Control Node

To remove any existing VOS-based node or cluster, run the **utils system onboard remove** command from the publisher node in the VOS node/cluster that you want to remove.

Command	**utils system onboard remove**

Description	This command is used to remove a node/cluster from a Cloud Connect node.
Expected Inputs	When run, this command prompts for: • Cloud Connect server FQDN • Cloud Connect application username and password
Expected Outcome	The node/cluster is successfully removed from the Cloud Connect node inventory.

Update Windows Nodes Onboarded to Orchestration Control Node

The update procedure is similar to the onboarding procedure described in Onboard Windows nodes to orchestration control node, on page 130.

Note If SSH connection is already established, skip Step 1 in the above procedure.

Validate Updated Nodes Onboarded for Orchestration

The procedure to validate updated nodes that have been onboarded is the same as described in Validate Onboarded Nodes for Orchestration, on page 132.

Configure Email Configuration

You can check your email configuration details by running the respective commands as described below:

- Get the IP address and hostname of the SMTP server by running the **show smtp-host** command.

Command	**show smtp-host**
Description	This command is used to get the IP address or hostname of the SMTP server.
Expected Inputs	NA
Expected Outcome	Shows the configured IP address or host name of the SMTP server.

- Get the email address from which the emails are triggered by running the **show smtp-from-email** command.

Command	**show smtp-from-email**
Description	This command is used to get the email address from which the emails are triggered. This email address is not monitored and therefore not used for replying to any emails.
Expected Inputs	NA
Expected Outcome	Shows the email address from which the emails are triggered.

- See if SMTP authentication is enabled or not by running the **show smtp-use-auth** command.

Command	show smtp-use-auth
Description	This command is used to know if SMTP authentication is enabled or not.
Expected Inputs	NA
Expected Outcome	SMTP authentication : <enable/disable>

- Get the username for SMTP server connection by running the **show smtp-user** command.

Command	show smtp-user
Description	This command is used to show the user name to be used for SMTP server connection.
Expected Inputs	NA
Expected Outcome	Shows the SMTP username.

- See if the SMTP password is set or not by running the **show smtp-pswd** command.

Command	show smtp-pswd
Description	This command is used to know if the SMTP password is set or not. To reset the password, run the **set smtp-pswd** command.
Expected Inputs	NA
Expected Outcome	Shows whether the SMTP password is set or not.

- See the email addresses subscribed for notification by running the **utils smtp show subscriptions** command.

Command	utils smtp show subscriptions
Description	This command is used to get a list of all the email addresses subscribed for email notification.
Expected Inputs	NA
Expected Outcome	Shows the email addresses that are subscribed for email notification. If there is no email address subscribed, a message is displayed indicating it.

Delete Configuration for Email Notification

To remove the configuration for email notifications, run the **utils smtp remove-config** command.

Command	utils smtp remove-config
Description	This command is used to remove the SMTP configuration from the control node. Email notification will no longer be sent to the subscribed email addresses. This command removes only the SMTP configuration, not the subscribed email addresses.

Expected Inputs	NA
Expected Outcome	SMTP configuration is deleted.

Unsubscribe Email Notification

To unsubscribe from email notifications, run the **utils smtp unsubscribe** command.

Command	**utils smtp unsubscribe**
Description	This command is used to remove one or more email addresses from the existing list of subscribers for email notification. **Note** You can get a list of subscribed email addresses using the **utils smtp show subscriptions** command.
Expected Inputs	Provide a comma-separated list of the email addresses to unsubscribe. For example: **utils smtp unsubscribe <emailaddress1,emailaddress2,.....emailaddressesN>** You can also remove all the subscribed email addresses from the subscription list at once. To do that, run **utils smtp unsubscribe all** and confirm.
Expected Outcome	Removes the email addresses you provided as the input from the subscription list.

Export and Import of Nodes Managed by Orchestration Control Node

To export inventory to an SFTP server, run the **utils system inventory export** command.

Command	**utils system inventory export**
Description	This command is used to export inventory to an SFTP server location. The inventory file can then be viewed and edited as required.
Expected Inputs	When run, this command prompts for: • SFTP Server: IP address of the SFTP remote server • SFTP User • SFTP User's Password • SFTP Directory: Location of the remote server directory where the inventory needs to be exported **Note** Provide the location only; the filename is *inventory.conf* by default.
Expected Outcome	Inventory is exported to the SFTP server location.

To import inventory to Cloud Connect server, run the **utils system inventory import** command.

Command	utils system inventory import
Description	This command is used to import inventory to Cloud Connect server.
Expected Inputs	When run, this command prompts for: • SFTP Server: IP address of the SFTP remote server • SFTP User • SFTP User's Password • SFTP Directory: Location of the remote server directory from where the inventory needs to be imported **Note** • Provide the location only. The filename is *inventory.conf* by default. • During inventory import, the *inventory.conf* filename should have the side information added for each node. For example, side: "A" /side: "B". During inventory import, the cluster information cannot be blank. It should have valid host details or a default value {}. For example, "ROGGER":{}
Expected Outcome	Inventory is imported to Cloud Connect server.

Note For information on adding deployment type and deployment name in the inventory file, see Add Deployment Type and Deployment Name, on page 132.

Export Current Patch Level Details

Available patches for nodes in the deployment can be obtained in either of the following ways:

- Email Notification
- Using the **utils patch-manager list** command.

Current patch levels can be exported in text file format using the **utils patch-manager export status** command.

Command	utils patch-manager export status
Description	This command is used to export the patch level details of a node or a group of nodes in a text file format.
Expected Inputs	Select the node(s) and enter the SFTP server details.
Expected Outcome	A text file with the current patch levels of the selected nodes is exported to the provided location. A success message is displayed along with the location where the file is saved.

Serviceability

Audit Logs

Audit trial for administrative operation that is initiated from Orchestration CLI on Cloud Connect is captured in Orchestration Audit logs. Audit trial captures the user, action and date/time details of the CLI operation.

- **file get activelog orchestration-audit/audit.log***

CLI Logs

Run the following command on the Cloud Connect node to retrieve CLI logs:

- **file get activelog platform/log/cli*.log**

Ansible Logs

Run the following commands on the Cloud Connect node to retrieve ansible-related logs:

- Current transaction logs: **file get activelog ansible/ansible.log**
- Historical logs: **file get activelog ansible/ansible_history.log**

Operation Status HA Synchronization Logs

Run the following command on the Cloud Connect node to retrieve synchronization-related logs:

- **file get activelog ansible/sync_ansible_log_to_remote_cc.log**

Email Notification-related Logs

Run the following commands on the Cloud Connect node to retrieve email-related logs:

- Current transaction logs:**file get activelog ansible/ansible_email_cron.log**

Software Download Logs

Run the following commands on the Cloud Connect node to retrieve software download-related logs:

- Current transaction logs:**file get activelog ansible/software_download_ansible.log**
- Historical logs:**file get activelog ansible/software_download_ansible_history.log**
- Process logs:**file get activelog ansible/software_download_process.log**

Note Software is downloaded separately on Cloud Connect publisher and subscriber.

Orchestration Logs in RTMT

You can also view the below-mentioned logs using the Real-Time Monitoring Tool (RTMT):

- Audit logs by selecting 'Orchestration Audit' as the Cloud Connect service
- Ansible logs by selecting 'Ansible Controller' as the Cloud Connect service

To download RTMT from Cloud Connect, access https://FQDN:8443/plugins/CcmServRtmtPlugin.exe.

For more information, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at:https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

For logs on individual components, refer to the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Enable and View Windows Open SSH Logs

To enable and view open SSH logs, do the following:

- Make sure the sshd_config file *%programdata%\ssh\sshd_config* has the value as 'LogLevel DEBUG' and uncomment the line.
- Restart the service (select service name **OpenSSH SSH Server**).
- In the Windows Event Viewer, select option **`Show Analytic and Debug Logs`** from **View** on the top menu bar.
- Select **`Debug`** channel from OpenSSH folder.
- On the right hand side, under Actions from Debug channel, select **`Enable log`**.

To turn on file-based logging, do the following:

- In the sshd_config file *%programdata%\ssh\sshd_config*, set the value as "SyslogFacility LOCAL0" and uncomment the line.
- Restart the service (select service name **OpenSSH SSH Server**).
- The file based logs are collected at location *%programdata%\ssh\logs*.

Configure SSH public key on Windows nodes

This section describes how to establish password-less Secure Shell (SSH) connection between Cloud Connect server and Windows node (CVP and ICM) using an SSH public key. The Windows node can be in a Workgroup or Domain.

Note If the Windows node (CVP and ICM) version is 12.5, install 12.5 mandatory ES before performing this procedure. Mandatory ES is not applicable for 12.6(x) target nodes. See System Requirements, on page 120 for details.

1. Navigate to *%Users%\<logonUser>\.ssh* and create *authorized_keys* file, if it doesn't exist.

Note

- The *authorized_keys* extension type is **File** and you should not modify it.
- The user must have either domain admin or local administrator privilege.

2. Open the browser and enter the following Cloud Connect publisher URL: **https://<CloudConnectIP>:8445/inventory/controlnode/key**
3. Provide your Cloud Connect application admin credentials. Upon successful authentication, a REST API response fetches the Cloud Connect Public SSH Key.
4. Copy the public key value that appears between quotes in the API response into the *authorized_keys* file in *%Users%\<logonUser>\.ssh*.
5. Repeat steps 2, 3, and 4 to fetch the Cloud Connect subscriber public key (if Cloud Connect is HA setup).

Note You must copy the Cloud Connect publisher and subscriber public keys into a single *authorized_keys* file. The publisher and subscriber entries should be in separate lines and should not use any extra space, comma, or any special characters at the end of the line.

6. Restart the following OpenSSH services:
   - OpenSSH SSH Server
   - OpenSSH Authentication Agent

Note For more information on Windows security hardening, see the *Windows Server Hardening* section in the Security Guide for Cisco Unified ICM/Contact Center Enterprise.

Self-Signed Certificate

You must import the self-signed certificates of both Cloud Connect publisher and subscriber nodes to the VOS publisher and subscriber nodes.

Get Tomcat Certificate from Cloud Connect Server

Procedure

Step 1 Login to the Cloud Connect server using: `https://<cloud connect hostname>:8443/cmplatform`.

Step 2 Navigate to **Security** > **Certificate Management**.

Step 3 Click **Find**.

Step 4 Click on the Tomcat certificate of the Cloud Connect server.

Step 5 Download the *.PEM file* and save the file.

Import Cloud Connect Server Tomcat Certificate to VOS Nodes

Procedure

Step 1 Login to the VOS node server using: `https://<VOS node hostname>:8443/cmplatform`.

Step 2 Navigate to **Security** > **Certificate Management**.

Step 3 Click on Upload Certificate/Certificate Chain.

Step 4 Select 'tomcat-trust' from the drop-down list in the **Certificate Purpose** field.

Step 5 Click **Browse** to upload the Cloud Connect server *.PEM file*.

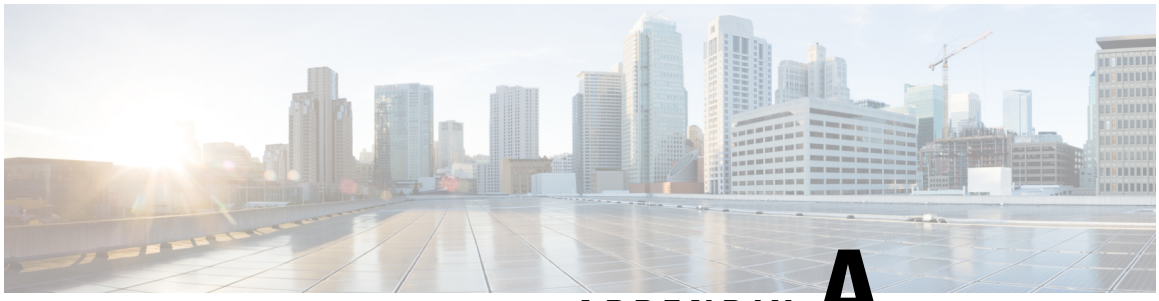
Step 6 Click **Upload**.

Step 7 Restart the specific VOS node by running the **utils system restart** command.

Things to Know

- Orchestration is not supported for CTIOS, Customer Collaboration Platform (CCP), ECE, CCDM, CCMP, and non-Contact Center Cisco products such as UCM, Unity Connection, CUBE gateways, CUSP, IM&P etc. Patches and upgrade operations for these components can be performed in a traditional manner.
- Orchestration is supported only for upgrades and patch install and not for tech refresh or fresh install.
- If any activity is blocked with a message `previous orchestration or upgrade operation is still in progress` even if there is no active operation, then restart Cloud Connect server.
- If one component ES has a dependency on another component ES, then they have to be taken into consideration by the administrator before initiating the patch installation from Cloud Connect server. The administrator should read the release notes that is notified through an email to understand the dependency. The Orchestration framework does not track this aspect automatically. For example, if an ES of Finesse has a dependency on an ES of Live Data and has to be installed in a specific order, then the administrator must consider this before initiating the patch installation from Cloud Connect server.
- Within Upgrade commands 'All Nodes' option for the Roll Back and Switch version commands are not available.
- Only Microsoft Exchange Server is supported for email notification; Office 365 and Gmail are not supported as of now.
- Email notifications are triggered about the available software upgrade from the publisher node of Cloud Connect server. If the publisher node is down at the trigger time, then the Admin will not receive any notification.
- All nodes option in *utils upgrade-manager list* CLI uses an internal cache, which is updated every day at 5 AM. The latest version of components that are upgraded before the cache update scheduled time will not be listed in All nodes option. The latest version of components can be listed by selecting the individual VOS or Windows or group of nodes option in the *utils upgrade-manager list* CLI. The cache update can be enforced by running the *utils system inventory import* CLI.
- For Packaged CCE deployment, only multistage upgrade is supported from Orchestration.

- For Packaged CCE deployment, CVPOAMP is not supported.



APPENDIX A

Security Considerations

Java Upgrades

During installations and upgrades, Unified CCE installs the base required Java version.

You can apply Java updates to your contact center as follows:

- Apply Java updates for the latest 32-bit Java 8 minor version.

  For the most current Java support information, see the 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.

  You can download and install the OpenJDK Java updates from the OpenLogic website.

- Modify the Windows CCE_JAVA_HOME environment variable to point to the new OpenJDK Java Runtime Environment (JRE) location if it has changed.

Note AppDynamics machine agent that is packaged with Unified ICM and Unified CVP uses a separate copy of OpenJDK. Any vulnerability fix for OpenJDK requires an upgrade of the AppDynamics machine agent. This update is delivered through an engineering special (ES) for Unified ICM and Unified CVP.

Upgrade OpenJDKUtility

The Cisco Upgrade OpenJDKUtility:

- Upgrades OpenJDK JRE to latest release.
- Supports upgrade for both MSI and Zip file formats.
- Automatically sets the CCE_JAVA_HOME environment variable to updated version so that Unified CCE applications can employ the latest OpenJDK version as the Java runtime.

Before using the tool:

- Download the OpenJDK installer from the OpenLogic OpenJDK website: https://www.openlogic.com/openjdk. (Both msi and zip formats are supported).
- Copy the downloaded file into the Unified CCE component VMs. *For Example* **C:\UpgradeOpenJDKTool**.
- Download the utility from https://software.cisco.com/download/home/284360381/type/284416107/release/12.6(2) and unzip **OpenJdkUpgradeTool.zip** to any local folder. For example: Download and Unzip under **C:\UpgradeOpenJDKTool**.
- Run **openJDKUtility.exe** from unziped folder For all the supported commands and for more details, refer to the *Readme.html* (which is available as part of the *OpenJdkUpgradeTool.zip*).

  Once the installation is successful, **CCE_JAVA_HOME** is updated and does not trigger the system reboot.

Upgrade Tomcat Utility

Use the optional Cisco Upgrade Tomcat Utility to:

- Upgrade Tomcat to version 9.0 build releases. (That is, only version 9.0 build releases work with this tool.) You may choose to upgrade to newer builds of Tomcat release 9.0 to keep up with the latest security fixes.

  Tomcat uses the following release numbering scheme: Major.minor.build. For example, you can upgrade from 9.0.22 to 9.0.69. You cannot use this tool for major or minor version upgrades.

Before using the tool:

- Download the Tomcat installer (apache-tomcat-version.exe) from the Tomcat website: http://archive.apache.org/dist/tomcat/tomcat-9/. Copy the installer onto the Unified CCE component VMs. For Example C:\UpgradeTomcatTool.
- Download the utility zip file, extract it, and run the batch file to upgrade Tomcat.

  Download link:
- Delete or back up large log files in these directories to reduce upgrade time:

  <ICM install directory>:\icm\tomcat\logs
  <ICM install directory>:\icm\debug.txt

Install Tomcat

For detailed information on the results from each step, see the ../UpgradeTomcatResults/UpgradeTomcat.log file.

Note Stop Unified CCE services on the VM before using the Tomcat Utility.

Procedure

Step 1 From the command line, navigate to the directory where you copied the Upgrade Tomcat Utility.

Step 2 Enter this command to run the tool: **tomcatutility.bat**.

Step 3 When prompted, enter the full pathname of the Tomcat installer version you want to use.

For example:

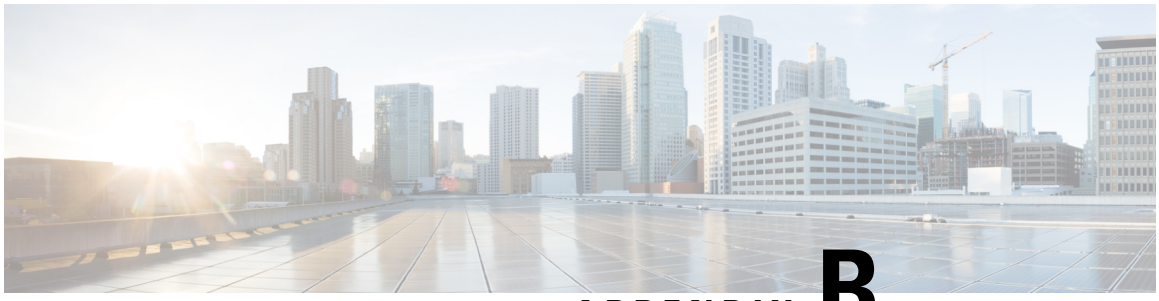
```
c:\tomcatInstaller\apache-tomcat-9.0.69.exe
```

Step 4 When prompted, enter **yes** to continue with the install.

Step 5 Repeat these steps for all unified CCE component VMs.

Note If the latest installed Tomcat does not work properly, install the previous working version using the Tomcat utility by following the above-mentioned steps.

Security Considerations



APPENDIX B

Reference

Tasks Common to Virtual Machines

About Creatings VMs

This chapter explains the sequence of tasks for creating virtual machines on each host server.

The sequence is:

1. Download the OVA files. See Open Virtualization Files, on page 165.
2. Create VMs .
3. After you create all the VMs, perform initial configuration. See the **Post Installation Configuration** section in the *Cisco Packaged Contact Center Enterprise Administration and Configuration* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Open Virtualization Files

Open Virtualization Format files define the basic structure of the VMs that are created—including the CPU, RAM, disk space, reservation for CPU, and reservation for memory.

1. Go to Download Software page on Cisco.com.
2. Select the required product release version.
3. Download and extract the file and save the OVAs to your local drive.

Mount ISO Files

Upload ISO image to data store:

1. Select the host in the vSphere client and click **Configuration**. Then click **Storage** in the left panel.
2. Select the datastore that will hold the ISO file.
3. Right click and select **Browse datastore**.
4. Click the **Upload** icon and select **Upload file**.
5. Browse to the location on your local drive where you saved the ISO file, and upload the ISO to the datastore.

Mount the ISO image:

1. Right-click the VM in the vSphere client and select **Edit virtual machine settings**.
2. Click **Hardware** and select **CD|DVD Drive 1**.
3. Check **Connect at power on** (Device status panel upper right).
4. Click the **Datastore ISO File** radio button and then click **Browse**.
5. Navigate to the data store where you uploaded the file.
6. Select the ISO file and click **OK**.

Unmount ISO File

Procedure

Step 1	Right-click the virtual machine in the vSphere client and select **Edit virtual machine settings**.
Step 2	Click **Hardware** and select **CD/DVD Drive 1**.
Step 3	Select **Client Device** and click **OK**.

Create a Virtual Machine from the OVA

Before you begin

For information on VMs, see the following sections:

- About Creatings VMs, on page 165
- Open Virtualization Files, on page 165
- Mount ISO Files, on page 166

Procedure

Step 1 Select the host in the vSphere client.

Step 2 Right-click the host and select **Deploy OVF Template**.

Step 3 On the **Select an OVF template** page, browse to the location on your local drive where you stored the OVA. Click **Open** to select the file. Click **Next.**

Note For Cisco VVB OVA, an End User License Agreement displays. Click **Agree** and then click **Next**.

Step 4 On the **Select a name and folder** page, enter a name for the virtual machine and then choose the location for the virtual machine.

The name can contain up to 128 characters. Valid characters are period (.), hyphen (-), underscore (_), and alphanumeric. The first character must be alphanumeric.

Step 5 Click **Next**.

Step 6 On the **Select a compute resource** page, select the destination compute resource. Click **Next.**

Step 7 On the **Review details** page, verify the OVF template details.

Step 8 On the **Configuration** page, select the applicable configuration from the available list. Click **Next**.

Note When deploying a CUIC OVF, choose **Co-Resident** for a 2000 Agent Deployment and **Stand-Alone** for a 4000 Agent and 12000 Agent Deployment.

Step 9 On the **Select storage** page, ensure that the virtual disk format is **Thick provision Lazy Zeroed** and then choose a datastore on which you want to deploy the new virtual machine. Click **Next.**

For each datastore, the following tables describe the RAID group, the ESXi Host, and the virtual machines for the Cisco UCS C240 M4SX, Cisco UCS C240 M5SX, and Cisco UCS C240 M6SX servers.

Note If you are on a Cisco UCS C240 M5SX or Cisco UCS C240 M6SX server, remove the following annotations from the non-core component VMs: Cisco, Finesse, CUIC, and CVP.

RAID configuration for the Cisco UCS C240 M4SX, Cisco UCS C240 M5SX, and Cisco UCS C240 M6SX

RAID Group	VM Datastore	ESXi Host	Virtual Machines
VD0	datastore 1	A	ESXi operating system Unified CCE Rogger Side A Unified CCE Router Side A Unified CCE Logger Side A Unified Communications Manager Publisher Cisco Finesse Primary
VD1	datastore 2	A	Unified CCE AW-HDS-DDS Side A

RAID Group	VM Datastore	ESXi Host	Virtual Machines
VD2	datastore 3	A	Unified Communications Manager Subscriber 1 Unified CVP Server Side A
VD3	datastore 4	A	Unified Intelligence Center Server Publisher Unified CCE PG Side A
VD0	datastore 1	B	ESXi operating system Unified CCE Rogger Side B Unified CCE Router Side B Unified CCE Logger Side B Unified Communications Manager Subscriber 2 Cisco Finesse Secondary
VD1	datastore 2	B	Unified CCE AW-HDS-DDS Side B
VD2	datastore 3	B	Unified Customer Voice Portal Reporting Server (optional) Unified CVP Server Side B
VD3	datastore 4	B	Unified Intelligence Center Server Subscriber Unified CCE PG Side B Enterprise Chat and Email Server (optional)

Step 10 On the **Select networks** page, confirm that the network mapping is correct for the Unfied CCE Rogger and PG:

a) For the Unifed CCE Rogger/Router/Logger/PG:

- Map Public to UCCE Public Network
- Map Private to UCCE Private Network

b) For all other servers, map Public to UCCE Public Network.

Step 11 On the **Ready to complete** page, click **Finish** to create the VM.

Configure DNS Server

This procedure is for Windows DNS server.

Note If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data requires FQDNs in order to work properly.

Note If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs in order to work properly.

Procedure

Step 1 Log in to the DNS server.

Step 2 In Windows, navigate to **Administrative Tools** > **DNS**. This opens the DNS Manager.

Step 3 In the Forward lookup zone, navigate to your deployment's domain name.

Step 4 Right-click the domain name and select **New Host (A or AAAA)**.

Step 5 In the New Host dialog box, enter the computer name and IP address (IPv4) of VOS components.

Configure Database Drive

Note Complete this procedure to create a virtual drive, if the virtual drive was not automatically created in the VM.

Procedure

Step 1 Add a virtual drive as follows:

Using Web client:

a) Right-click the virtual machine and click **Edit Settings**.
b) In the **Virtual Hardware** tab, click on **Add New Device**.
c) You can select the type of device you wish to add. Select **Hard Disk**. The new hard disk appears. Assign the desired disk space to the hard disk.
d) Configure the required parameters as specified below:

Note Virtual machine templates for Logger, Rogger, AW, and HDS servers do not have a SQL database drive preprovisioned. The following reference table must be used to assign disk space to the virtual machine based on the type of validation errors will occur:

Virtual Machine Template	Default Second Disk Size
Logger	500 GB
Rogger	150 GB
AW-HDS-DDS	500 GB
AW-HDS	500 GB
HDS-DDS	500 GB

You can custom size the SQL database disk space to meet data retention requirements on an external AW-HDS-DDS server only, as calculated by the Database Estimator tool.

e) On the **Disk Provisioning** section, choose **Thick provision Lazy Zeroed**.
f) In the **VM Options** > **Advanced Options** section, retain the default options.
g) Click **OK** to confirm the changes.

The Recent Tasks window at the bottom of the screen displays the progress.

Step 2 In Windows, navigate to **Disk Management**.

Step 3 Right-click on the **Disk 1** box and select **Online**.

Step 4 Initialize Disk 1 as follows:

a) Right-click on the **Disk 1** box and select **Initialize Disk**.
b) Check the **Disk 1** checkbox.
c) Select the **MBR (Master Boot Record)** radio button.
d) Click **OK**.

Step 5 Create a new disk partition as follows:

a) Right-click the graphic display of **Disk 1** and select **New Simple Volume**.
b) Click **Next** on the first page of the **New Simple Volume Wizard**.
c) On the **Specify Volume Size** page, retain the default volume size. Click **Next**.
d) On the **Assign Drive Letter or Path** page, assign drive letter (E). Click **Next**.
e) On the **Format Partition** page, format the partition as follows:

1. Select the **Format this volume with the following settings** radio button.
2. Click **Format Disk**.
3. Select File System as **NTFS** and click **Start**.
4. Select **Default** from the **Allocation unit size** drop-down menu.
5. Enter a value in the **Volume label** field.
6. Check the **Perform a quick format** checkbox.
7. Click **Next**.

f) Click **Finish**.

A popup window displays a message that you need to format the disk before you can use it.

The format is complete when the status changes to Healthy.

Step 6 Format the disk.

a) Click **Format disk**.
b) Click **Start**.
A popup displays a warning that formatting will erase all data on the disk.
c) Click **OK**.
d) When the format is complete, click **OK** to close the popup window.

Install Antivirus Software

Install one of the supported antivirus software products.

See the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for the list of supported products.

Important Disable automatic updates. Update antivirus software manually.

Important The firewall component of Symantec Endpoint Protection 12.1, the Network Threat Protection feature, must be disabled. If the feature remains enabled, which is the default, both sides of a duplexed router come up in simplex mode, thus blocking communication between each side of a router. This blocking impacts all deployment types.

For more information on security guidelines, refer the **General Antivirus Guidelines** section in the *Security Guide for Cisco Unified ICM/Contact Center Enterprise Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

To allow required access to installation program files or folders, perform file-blocking exclusions in the antivirus product file-and-folder protection rules. To do this in McAfee VirusScan:

Procedure

	Command or Action	Purpose
Step 1	Launch the VirusScan console.	
Step 2	Right-click **Access Protection** and select **Properties**.	

	Command or Action	Purpose
Step 3	In the Anti-virus Standard Protection category, make sure that the rule Prevent IRC communication is unchecked in the Block column.	For more information about changing settings, see the documentation for your antivirus software.

Verification of the Downloaded ISO or Minor Release Installer

Perform the following procedure to validate the downloaded ISO or Minor Release Installer signed by Cisco, to ensure that it is authorized.

Procedure

Step 1 Install **OpenSSL** on Microsoft Windows.

Step 2 Add the OpenSSL installation path to **System variables** in the **Environment Variables** of the system.

Step 3 Add the downloaded ISO Image or Minor Release Installer, ISO Image signature file or Minor Release Installer signature file and the Public key.der file in the same folder for the specific product component.

Step 4 Launch **Command Prompt** on the system.

Step 5 Run the following CLI (Command Line Interface) command to verify the files:

```
openssl dgst -sha512 -keyform der -verify <PUBLIC key.der> -signature
<ISO Image.iso.signature or Minor Release Installer.exe.signature> <ISO
Image or Minor Release Installer exe>
```

The system displays `Verified OK` on successful verification and `Verification failed` on verification failure.

Note If the verification fails do not proceed with the installation, contact Cisco Support for a valid ISO or Minor Release Installer.

Software Installations for Components

This section holds the consolidated list of software installation procedures that are referenced in the following section:

- Packaged CCE 2000 Agents Installation, on page 15
- Packaged CCE 4000 Agents Installation, on page 25
- Packaged CCE 12000 Agents Installation, on page 33

Install Microsoft Windows Server

Complete the following procedure to install Microsoft Windows Server on the virtual machines deployed.

Note Deploying VM with Guest Operating System 'Microsoft Windows Server 2019' on ESXi 7.0 using CCE OVA template displays a warning message "The configured guest OS (Microsoft Windows Server 2016 or later (64-bit)) for this virtual machine does not match the guest that is currently running (Microsoft Windows Server 2019 (64-bit)). You should specify the correct guest OS to allow for guest-specific optimization". This warning message is informational only and has no detrimental effect on the system. This warning message is displayed only once and can be dismissed.

Note Before installing 12.5(1) ICM on SQL Server 2019, make sure to install ODBC Driver 13 for SQL Server® manually.

Procedure

Step 1 Mount the Microsoft Windows Server ISO image to the virtual machine.

Check the **Connect at power on** check box when mounting the ISO.

Step 2 Power on the VM.

Step 3 Enter the Language, Time and Currency Format, and Keyboard settings. Click **Next**.

Step 4 Click **Install Now**.

Step 5 If prompted, enter the product key for Windows Server and click **Next**.

Step 6 Select the Desktop Experience option for the Windows Server and click **Next**.

Step 7 Accept the license terms and click **Next**.

Step 8 Select **Custom: Install Windows only (advanced)**, select **Drive 0** to install Microsoft Windows Server, and then click **Next**.

The installation begins. After the installation is complete, the system restarts without prompting.

Step 9 Enter and confirm the password for the administrator account, and then click **Finish**.

Step 10 Enable Remote Desktop connections as follows:

a) Navigate to **Control Panel** > **System and Security** > **System**.
b) Click **Remote Settings**.
c) Click the **Remote** tab.
d) Select the **Allow remote connections to this computer** radio button. The Remote Desktop Connection dialog displays a notification that the Remote Desktop Firewall exception is enabled. Click **OK**.

Step 11 Install VMWare tools. See Install VMware Tools, on page 179.

Step 12 Open the **Network and Sharing Center**, and in the View your basic network info and set up connections section, click **Ethernet**.

Step 13 In the Ethernet Status window, click **Properties**.

Step 14 In the **Ethernet Properties** dialog box, configure the network settings and the Domain Name System (DNS) data:

a) Uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
b) Select Internet Protocol Version 4 (TCP/IPv4) and click **Properties**.

c) Select **Use the following IP Address**.
d) Enter the IP address, subnet mask, and default gateway.
e) Select **Use the following DNS Server Address**.
f) Enter the preferred DNS server address, and click **OK**.

Edge Chromium (Microsoft Edge) is not installed by default on the Windows server. To install Edge Chromium (Microsoft Edge), see *Microsoft* documentation.

Note If you want to install Unified CCE on a multilingual version of Windows Server, refer to Microsoft documentation for details in installing Microsoft Windows Server Multilingual language packs.

If Unified CCE language pack is applied on Chinese Windows OS machine, set the screen resolution to 1600 x 1200.

Related Topics

Mount ISO Files, on page 166

Install Microsoft SQL Server

Install Microsoft SQL Server and store the SQL Server log and temporary files on the same vDisk as the operating system when using **default** (two) vDisk design. If you choose to use more than two virtual disks, then the tempDB cannot be on the same vDisk as the solution database.

For further information about the database placement and performance tuning the SQL installation, see the Microsoft documentation.

Note For information about supported editions, see the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html.

Before you begin

Note Microsoft SQL Server does not contain SQL Server Management Studio in the default toolkit. To rerun the SQL Server setup to install Management Studio, navigate to: **SQL Selection Center** > **Installation** > **Install SQL Server Management Tools**. If your computer has no internet connection, download and install SQL Server Management Studio manually.

VC++ 2017 `build# 14.12.25810` is not compatible with the Cisco Contact Center Enterprise, ensure that it is not installed.

Add the virtual machine to a domain before installing SQL Server.

Procedure

Step 1 Mount the Microsoft SQL Server ISO image to the virtual machine. For more information, see Mount ISO Files, on page 166.

Step 2 Select **Installation** in the left pane and then click **New SQL Server stand-alone installation or add features to an existing installation**. Click **OK**.

Step 3 On the **Product Key** page, enter the product key and then click **Next**.

Step 4 Accept the **License Terms** and then click **Next**.

Step 5 Optional: On the **Microsoft Update** page, check the **Use Microsoft Update to check for updates** check box, and then click **Next**.

Note If you do not check the **Use Microsoft Update to check for updates** option, click **Next** on the **Product Updates** page.

Step 6 On the **Install Rules** page, click **Next**.

In this step, the installation program checks to see that your system meets the hardware and software requirements. If there are any issues, warnings or errors appear in the **Status** column. Click the links for more information about the issues.

Step 7 On the **Feature Selection** page, select only the following, and click **Next**:

- **Database Engine Services**
- **Client Tools Connectivity**
- **Client Tools SDK**
- **SQL Client Connectivity SDK**

Step 8 On the **Instance Configuration** page, select **Default Instance** and click **Next.**

Step 9 On the **Server Configuration** page, click the **Services Account** tab.

a) Associate the SQL services with the virtual account.

- For the SQL Server Database Engine, in the Account Name field, select **NT Service\MSSQLSERVER**.

Note While you can use the Network or Local Services account instead of the Virtual account, using the Virtual account provides security.

b) For the remaining services, accept the default values.

c) In the **Start Up Type** column, for the **SQL Server Agent service** account, select **Automatic** from the list.

d) Enable **Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service**.

Note Unified ICM Installer automatically enables the **Grant Perform Volume Maintenance Task** for the NT service account.If it is not enabled automatically then you must enable **Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service** manually on the SQL server.

Step 10 On the **Server Configuration** page, click the **Collation** tab.

a) In the Database Engine section, click **Customize**.
b) Select the **Windows Collation designator and sort order** radio button.
c) Select the appropriate collation. Typically, you choose the SQL Server collation that supports the Windows system locale most commonly used by your organization; for example, "Latin1_General" for English.

The database entry is related to the collation that you select. For example, if you set the collation for Latin1_General, but you select Chinese language at sign-in. When you enter field values in Chinese, the application displays the `unsupported character` error, because the database does not support the characters.

Important It is critical to select the correct collation setting for the language display on your system. If you do not select the correct collation during installation, you must uninstall and reinstall Microsoft SQL Server.

d) Check the **Binary** check box.
e) Click **OK**, and then click **Next**.

Step 11 On the **Database Engine Configuration** page:

a) On the Server Configuration tab, click the **Mixed Mode** radio button.
b) Enter the password for the SQL Server system administrator account, and confirm by reentering it.
c) Click **Add Current User** to add the user who is installing the SQL Server as an administrator.
d) On the **TempDB** tab, set the **Initial size** and **Autogrowth** for Rogger, Logger, AW-HDS-DDS, AW-HDS, and HDS-DDS. For information about values for respective components Increase Database and Log File Size for TempDB, on page 178.

For more information about the SQL Server TempDB Database and its use, see the Microsoft SQL Server documentation.

e) On the **MaxDOP** tab, choose the value of MaxDOP as half the value of logical CPU cores detected on the computer which is displayed just above the MaxDOP configuration. For example, if the logical CPU cores are detected as 4, then MaxDOP should be configured as 2.

Note SQL Server installation automatically recommends the MaxDOP server configuration based on the number of processors available. This feature is introduced in SQL Server 2019 and later. In SQL Server 2017, you can configure MaxDOP post installation. To configure MaxDOP, do the following:

1. In **Object Explorer**, right-click the database instance and select **Properties**.
2. Select **Advanced**.
3. In the **Max Degree of Parallelism** box, configure the number of processors as recommended above.

f) Click **Next**.

Step 12 On the **Ready to Install** page, click **Install**.

Step 13 On the **Complete** page, click **Close**.

Step 14 Enable Named Pipes and set the sort order as follows:

a) Open the SQL Server Configuration Manager.
b) In the left pane, navigate to **SQL Native Client 11.0 Configuration (32bit)** > **Client Protocols**.
c) In the right pane, confirm that **Named Pipes** is **Enabled**.
d) Right-click **Client Protocols** and select **Properties**.

e) In the **Enabled Protocols** section of the **Client Protocols Properties** window, use the arrow buttons to arrange the protocols in the following order:

1. Named Pipes
2. TCP/IP

f) Check the **Enable Shared Memory Protocol** and then click **OK**.
g) In the left pane, navigate to **SQL Server Network Configuration** > **Protocols for MSSQLSERVER**.
h) In the right pane, right-click **Named Pipes** and select **Enable**.

Note By default, Microsoft SQL Server dynamically resizes its memory. The SQL Server reserves the memory based on process demand. The SQL Server frees its memory when other processes request it, and it raises alerts about the memory monitoring tool.

Cisco supports the Microsoft validation to dynamically manage the SQL Server memory. If your solution raises too many memory alerts, you can manually limit SQL Server's memory usage. Set the maximum and minimum limit of the SQL memory using the **maximum memory usage** settings in the **SQL Server Properties** menu as shown below:

Component	SQL Server Minimum Memory	SQL Server Maximum Memory
Logger	2GB	4GB
Rogger	2GB	3GB
AWS-HDS	4GB	8GB
AWS-HDS=DDS	4GB	8GB
HDS-DDS	4GB	8GB

For more information about the SQL Server memory settings and its use, see the Microsoft SQL Server documentation.

Step 15 Set the SQL Server's default language to English as follows:

a) Launch SQL Server Management Studio.
b) In the left pane, right-click the server and select **Properties**.
c) Click **Advanced**.
d) In the **Miscellaneous** section, set the **Default Language** to **English**.
e) Click **OK**.

Important Set the SQL Server default language to English because Cisco Unified Contact Center Enterprise requires a US date format (MDY). Many European languages use the European date format (DMY) instead. This mismatch causes queries such as `select * from table where date = '2012-04-08 00:00:00'` to return data for the wrong date. Handle localization in the client application, such as Cisco Unified Intelligence Center.

Step 16 Restart the SQL Server service as follows:

a) Navigate to the **Windows Services** tool.
b) Right-click **SQL Server (MSSQLSERVER)** and click **Stop**.
c) Right-click **SQL Server (MSSQLSERVER)** and click **Start**.

Step 17 Ensure that the SQL Server Browser is started, as follows:

a) Navigate to the **Windows Services** tool.
b) Navigate to the SQL Server Browser.
c) Right-click to open the **Properties** window.
d) Enable the service, change the startup type to **Automatic**, and click **Apply**.
e) To start the service, click **Start**, and then click **OK**.

Related Topics

Mount ISO Files, on page 166

Increase Database and Log File Size for TempDB

To get the benefits of TempDB multiple data files support in CCE components, configure the following values as suggested for respective components.

CCE Component	vCPU	TempDB Data Files			TempDB Transaction Log File	
		Number of Files	Initial Size	Autogrowth	Initial Size	Autogrowth
Rogger	4	4	800MB	100MB	600MB	10MB
Logger	4	4	800MB	100MB	600MB	10MB
AW-HDS-DDS	4	4	800MB	100MB	600MB	10MB
AW-HDS	8	8	400MB	100MB	600MB	10MB
HDS-DDS	8	8	400MB	100MB	600MB	10MB

Collation and Locale Settings for Localization

Microsoft SQL Server Collation Settings for Languages

You select a collation when you install Microsoft SQL Server, and it must be the collation that maps to the customer's language display.

Remember If your initial collation selection is incorrect, you must uninstall Microsoft SQL Server and reinstall it with the correct collation configuration.

For the languages supported by Packaged CCE and the SQL Server Collation setting for each language, see the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html.

Windows System Locale

The Windows system locale must match the display language; otherwise some characters appear incorrectly in the user interface and are saved incorrectly to the database. For example, if the system locale is English and you are working in Spanish, characters such as the *acute a* appear incorrectly.

Perform this procedure at both CCE Roggers, both CCE PGs, both CCE AWs, and any external HDS systems.

1. Open **Control Panel > Clock, Language, and Region > Language**.
2. Add the required language in the **Change your language preferences** page.
3. In the left pane, select **Advanced settings**.
4. Select the language for the **Override for Windows display language** option.
5. Select the language for the **Override for default input method** option.
6. Save your work and restart the virtual machine.

Install VMware Tools

Use this procedure to install and upgrade VMware tools from the VMware vSphere Client.

To install or upgrade VOS for Cisco Finesse, Cisco Unified Intelligence Center, and Cisco Unified Communications Manager:

1. Ensure that your virtual machine is powered on.
2. Right-click the VM in the virtual machine menu. Select **Guest** > **Install / Upgrade VMware tools**
3. Choose the automatic tools update and press **OK**.

The process takes a few minutes. When the process is complete, the tools are listed as Running (Current) on the VM's Summary tab in vSphere.

To install or upgrade VMs with Windows guest operating system:

1. Ensure that your Windows virtual machine is powered on.
2. Right click the VM in the virtual machine menu. Select **Guest** > **Install / Upgrade VMware tools**. Click **OK** on the popup window.
3. Log in to the VM as a user with administrative privileges.
4. Run VMware tools from the DVD drive.

   The installation wizard starts.
5. Follow the prompts in the wizard to complete the VMware Tools installation. Choose the **Typical** installation option.
6. When the VMware Tools installation has finished, restart the virtual machine for the changes to take effect.

When the process is complete, the tools are listed as Running (Current) on the VM's Summary tab in vSphere.

Add Machine to Domain

Procedure

Step 1 Navigate to **Control Panel** > **System and Security** > **System**.

Step 2 Click **Change Settings**.

Step 3 In the **Computer Name** tab, click **Change**.

Step 4 Change the name of the computer from the name randomly generated during Microsoft Windows Server installation. The name does not contain underscores or spaces.

Step 5 Select the **Domain** radio button to change the member from Workgroup to Domain.

Step 6 Enter qualified domain name and click **OK**.

Step 7 In the **Windows Security** dialog, enter the domain credentials and click **OK**.

Step 8 On successful authentication, click **OK**.

Step 9 Reboot the server and sign in with domain credentials.

Configure Network Adapters

The Unified CCE Rogger, Router, Logger and the Unified CCE PG each have two network adapters. You must identify them by MAC address and Network Label, rename them, configure them, and set the interface metric value.

Procedure

Step 1 Identify the MAC addresses and labels for the network adapters as follows:

a) From vSphere, select and right-click the VM.

b) Select **Edit Settings**. In the **Hardware** tab, click **Network adapter 1**. In the right panel, write down the last few digits of MAC addresses and note whether the label is PCCE Public or PCCE Private. For example, Network adapter 1 may have a MAC address that ends in 08:3b and the network label PCCE Public.

c) Repeat for Network adapter 2, noting its MAC address and label.

d) From the VM console, type **ipconfig /all** from the command line. This displays the adapter names and physical addresses.

e) Note the adapter names and physical addresses and match them with the MAC addresses and labels that you noted in VMware. For example, in ipconfig/all, Local Area Connection 2 may have a physical address that ends in 08-3b.

f) Match the MAC address of the network adapter that VMware identified as PCCE Public with the corresponding physical address of Local Area Connector. In this example, the physical address of Local Area Connection 2 (08-3b) matches the MAC address (08-3b) of Network adapter 1. This means that Local Area Connection 2 is PCCE Public.

Note Adapters may have a different name than Local Area Connection.

Step 2 Locate and rename the network adapters in Windows as follows:

a) In Windows, open the **Control Panel** > **Network and Sharing Center** and click **Change adapter settings**.

b) Right-click **Local Area Connection** and select **Rename**. Rename it to **PCCE Public** or **PCCE Private**, based on the matching you did above.

c) Right-click **Local Area Connection 2** and select **Rename**. Rename it to **PCCE Public** or **PCCE Private**, based on the matching you did above. In the example above, **Local Area Connection 2** is renamed to PCCE Public.

Step 3 Set the Properties for PCCE Public as follows:

a) Right-click **PCCE Public** and select **Properties**.

b) In the **Networking** tab, uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
c) Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
d) In the **General** tab for Internet Protocol Version 4, select **Use the following IP address** and enter **IP address**, **Subnet mask**, **Default gateway**, and DNS servers.
e) Click **OK** and **Close** to exit.

Step 4 Set the Properties for PCCE Private as follows:

a) Right-click **PCCE Private** and select **Properties**.
b) In the **Networking** tab, uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
c) Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
d) In the **General** tab for Internet Protocol Version 4, select **Use the following IP address** and enter **IP address** and **Subnet mask**.
e) Click **Advanced**.
f) Click the **DNS** tab and uncheck *Register this connection's addresses in DNS*.
g) In the DNS server, add a new A record that resolves to the private IP address. Also, create an associated pointer record for reverse lookups.

Note For hostnames in A records, append the letter p to indicate that it is a private address.

h) Click **OK** to exit.

Step 5 Assign an interface metric value for the network adapter:

a) Select the network adapter and right-click **Properties**.
b) In the **Networking** tab, select the appropriate Internet Protocol version and click **Properties**.
c) In the **Internet Protocol Version Properties** dialog box, click **Advanced**.
d) In the **IP Settings** tab, uncheck the **Automatic metric** checkbox and type a low value in the **Interface metric** text box.

Note A low value indicates a higher priority. Make sure that the Public Network card should have a lower value compared to the Private Network card.

By default, the value of the Interface Metric property for a network adapter is automatically assigned and is based on the link speed.

e) Click **OK** to save the settings.

Repeat the steps to assign an interface metric value for the internal/private cluster communication network adapter.

Configure Network Adapter for Unified CCE AW-HDS-DDS, AW-HDS, HDS-DDS

Procedure

Step 1 Locate and rename the network adapter in Windows as follows:

a) In Windows, open the **Network and Sharing Center** and click **Change Adapter Settings** .
b) Right-click **Local Area Connection** and select **Rename**. Rename it to **UCCE Public**.

Step 2 Set the Properties for UCCE Public as follows:

a) Right-click **UCCE Public** and select **Properties**.
b) In the Networking dialog box, uncheck Internet Protocol Version 6 (TCP/IPv6).
c) In the Networking dialog box, select Internet Protocol Version 4 (TCP/IPv4) and select **Properties**.
d) In the General dialog box for Internet Protocol Version 4, select **Use the following IP address** and enter the IP address, the Subnet mask, the default gateway, and DNS servers.
e) Click **OK** and **Close** to exit.

Set Persistent Static Routes

For geographically distributed Central Controller sites, redundant Rogger, logger, router, and Peripheral Gateway components typically have a Private IP WAN connection between Side A and Side B. Windows only allows one default gateway for each VM (which sends the Private Network traffic to the Public Network). So, you add a Static Route to all the VMs running the Rogger, logger, router, and PG applications.

To create a persistent static route with the **route add** command, you need the destination subnet, the subnet mask, the local gateway IP, and the interface number of the local Private Network interface:

`route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p`

You must launch the DOS prompt as an administrator to run the commands in this procedure.

Procedure

Step 1 On each Rogger, router, logger, or PG VM, run `ipconfig /all`.
Record the `IPv4 Address`, `Subnet Mask`, and `Physical Address` (MAC address) for the Private Network interface.

Step 2 On each of these VMs, run `route print -4`.
Record the `Interface` for the Private Network. You can identify the correct interface by looking for its `Physical Address` (MAC address).

Step 3 On each of these VMs, run `route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p` to add a persistent static route for the remote Private Network.

On Side A VMs, use the gateway IP for Side B. On Side B VMs, use the gateway IP for Side A.

Run Windows Updates

Procedure

Go to **Settings** > **Update & Security** and run Microsoft Windows Update.

Install Cisco Unified Contact Center Enterprise

Install the Unified Contact Center Release 12.5 software on your Unified CCE virtual machines.

Note Before installing 12.5(1) ICM on SQL Server 2019, make sure to install ODBC Driver 13 for SQL Server® manually.

Procedure

Step 1 Login as a user with administrative privileges.

Step 2 Mount the Cisco Unified CCE ISO image to the virtual machine. See Mount ISO Files, on page 166.

Step 3 Run setup.exe from the D:\ICM-CCE Installer directory.

Step 4 Follow the InstallShield procedures to install Cisco Unified CCE.

Step 5 When the installation completes, restart the computer when prompted.

Step 6 Unmount the ISO image.

Note If the ICM-CCE installer installs JRE on the Windows platform, the system retains only the Cisco approved CA certificates in the java certificate store, and removes all the unapproved certificates.

Silent Installation

In certain situations, such as when a system administrator wants to install or upgrade software silently on multiple systems simultaneously, a silent installation is performed to run an installation wizard.

Silent Installation Prerequisites for Unified CCE Release 12.5(1)

Before running a silent installation, complete the following tasks:

- Stop all applications that are running on the system.
- By default, silent installation assumes the following parameter: **Install on Drive C**.

  To override this default, edit the ICMCCSilentsetup.ini file in the ICM-CCE-Installer directory.
- Mount the ISO image to the target machine, and make the following edits on the target machine:
  - If you are performing a Technology Refresh upgrade, change the **szInstallType** from **0** to **1**. The default value of **0** is for a Fresh Install.
  - If you are performing a Technology Refresh upgrade, provide a path for the **szExportedRegistryPath** parameter where the exported registry from source machine is placed.
  - To change the drive on which you are installing the application, change the **szDrive** parameter. Replace C with the drive where you want to install.
  - If you do not want to apply SQL Security Hardening, change the line that reads **szSQLSecurity=1** to **szSQLSecurity=0**.

Note SQL Security Hardening should not be applied as part of silent installation on Windows Server 2019 and SQL Server 2019 platform. Change the line that reads szSQLSecurity=1 to szSQLSecurity=0. SQL Security Hardening can be applied post installation using Security Wizard tool.

Perform a Silent Installation for Unified CCE Release 12.5(1)

Procedure

Step 1 Mount the Installation ISO image to the target machine. For more information, see Mount ISO Files, on page 166.

Step 2 From a command prompt window, navigate to the ICM-CCE-Installer directory.

Step 3 Enter the command **setup.exe /s**.

Installation starts. Upon successful installation, the server reboots.

Note If the installation is not successful, no error message appears in the command prompt window. You must check the installation log file `<SystemDrive>:\temp\ICMInstall.log` to determine the reason why the installation failed.

Silent Installation Prerequisites for Unified CCE Release 12.6(2)

Before running a silent installation, complete the following tasks:

- Stop all applications that are running on the system.
- The machine on which you create your response file should have a configuration that closely matches the machines on which you will run silent installs. This minimizes the chances of unexpected dialogs being triggered during the installation that could terminate the installation.

  For example, if the response file is created on a machine with Unified CCE services set to Manual and then run on a machine with those services set to Automatic, an additional dialog will open during the install (alerting you that the services have been set from Automatic to Manual). This unexpected dialog will cause the install to terminate, potentially leaving the system in an invalid state that requires manual recovery.

Perform a silent installation for Unified CCE Release 12.6(2)

Procedure

Step 1 Run setup from a command prompt with two command line arguments to create the response file.

Example:

```
"c:\ICM12.6(2).exe" -r -f1 c:\myanswerfilename.iss
```

The -r flag is for recording the response file.

The -f1 flag is the full path and filename for the resulting response file to be created.

Note There is no space between the -f1 and the start of the file path. If no -f1 flag is present, the response file is written to a default location (C:\Windows)".

When you have navigated through the setup process (which completes a full installation of the product on the machine recording the response file) the resulting response file can be copied to any additional machine during a silent installation.

Step 2 Run setup from a command prompt using the same syntax as listed in step 1, with one exception: use **-s** instead of **-r** to indicate the install should run silently using the response file found at -f1filepath.

Example:

```
"c:\ICM12.6(2).exe" -s -f1 c:\myanswerfilename.iss –f2 c:\silentinstall.log
```

The -f2 flag creates a log file.

What to do next

Verify that the silent installation was successful by checking the installer log file to make sure no errors were reported. If your silent installation does not run, check the log file for `ResultCode=-5`. It indicates the installer could not find your response file; recheck your path and file names.

During the creation of the response file, if you chose not to reboot the machine after the installation, ensure that you manually reboot any silently installed system prior to starting the services.

Configure Permissions in the Local Machine

In this release,Unified CCE defaults to providing user privileges by memberships to local user groups on local machines. This technique moves authorization out of Active Directory. However, it requires a one-time task on each local machine to grant the required permissions.

Note You can use the ADSecurityGroupUpdate registry key to choose between the new default behavior and the previous behavior. For more information, see the chapter on solution security in the Solution Design Guide.

Before using the Configuration Manager tool, configure the required registry and folder permissions for the `UcceConfig` group.

Configure Registry Permissions

This procedure only applies to distributor machines. Grant the required registry permissions for the `UcceConfig` group on the local machine.

Procedure

Step 1 Run the `regedit.exe` utility.

Step 2 Select `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM`.

Step 3 Right-click and select **Permissions**.

Step 4 If necessary, add `UcceConfig` in **Group or user names**.

Step 5 Select `UcceConfig` and check **Allow** for the **Full Control** option.

Step 6 Click **OK** to save the change.

Step 7 Repeat the previous steps to grant **Full Control** to the `UcceConfig` group for `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco Systems, Inc.\ICM`.

Step 8 Repeat the previous steps to grant **Full Control** to the `UcceConfig` group for `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2`.

Note If you have configured the Unified CCE Administration Client, open Local security policy and go to **User Rights Assignment**. Right click **Create Global Object**. Go to **properties** and add the local Group `UcceConfig`.

Configure AW-HDS Database Permissions

Follow this procedure to grant access to the AWDB-HDS database to `UcceConfig` group members.

Procedure

In SQL Management Studio, do the following:

a) Go to **Security** > **Logins**.

b) Locate `<Machine netbios name>\UcceConfig`. Right-click and select properties.

c) Go to **User Mappings** and select one AWDB database. Ensure that GeoTelAdmin, GeoTelGroup, and public are selected.

d) Repeat step c for the HDS database.

Note SQL login account `<Machine netbios name>\UcceConfig` is created during CCE installation on the machine. If there is any change in the machine hostname, the SQL login account has to be deleted and re-created with the new **machine netbios name**.

Configure Folder Permissions

Grant the required folder permissions to the `UcceConfig` group on the local machine.

Procedure

Step 1 In Windows Explorer, select `<ICM install directory>\icm`.

Step 2 Right-click and select **Properties**.

Step 3 On the **Security** tab, select `UcceConfig` and check **Allow** for the **Full Control** option.

Step 4 Click **OK** to save the change.

Step 5 Repeat the previous steps to grant **Full Control** to the `UcceConfig` group for `<SystemDrive>:\temp`.

Create Outbound Option Database

Outbound Option uses its own SQL database on the Logger. Perform the following procedure on the Side A Logger or the Side B Logger.

Procedure

Step 1 Open the ICMDBA tool and click **Yes** to any warnings.

Step 2 Navigate to **Servers** > **<Logger Server>** > **Instances** > **<Unified CCE instance>** > **LoggerA** or **LoggerB**. Right-click the instance name and select **Database** > **Create**.

Step 3 On the Stop Server message, click **Yes** to stop the services.

Step 4 In the Create Database dialog box, click **Add** to open the Add Device dialog box.

Step 5 Click **Data**, and choose the drive on which you want to create the database, for example, the E drive. In the database size field, you can choose to retain the default value or enter a required value.

Note Ensure that there is enough free space in the hard disk (at least 20% of database size) to accommodate the log growth.

Step 6 Click **OK** to return to the Create Database dialog box.

Step 7 In the Add Device dialog box, click **Log**. Choose the desired drive. Retain the default value in the log size field and click **OK** to return to the Create Database dialog box.

Step 8 In the Create Database dialog box, click **Create**, and then click **Start**. When you see the successful creation message, click **OK** and then click **Close**.

For more information about configuring Outbound Options, see the *Outbound Option Guide for Unified Contact Center Enterprise* guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

Configure Network Adapters for Cisco Unified CVP

Unified CVP has only one network adapter to configure. You must rename it and set its properties.

Procedure

Step 1 Navigate to **Control Panel** > **Network and Internet** .

Step 2 Click **Network and Sharing Center**, and then click **Change adapter settings** in the left panel.

Step 3 Right-click the adapter and select **Rename**. Change the name to UCCE Public.

Step 4 Right-click UCCE Public and select **Properties**.

Step 5 In the Networking dialog box, de-select Internet Protocol Version 6 (TCP/IPv6).

Step 6 In the Networking dialog box, select Internet Protocol Version 4 (TCP/IPv4) and select **Properties**.

Step 7 In the General dialog box for Internet Protocol Version 4 , select **Use the following IP address** and enter the IP address, the Subnet mask, the default gateway and DNS servers.

Step 8 Click **OK** and **Close** to exit.

Install Cisco Unified CVP Server

Procedure

Step 1 Log in to your system as a user with administrative privileges.

Step 2 Mount the Unified CVP ISO image to the virtual machine. For more information, see Mount ISO Files, on page 166.

Step 3 Run setup.exe from the D:\ CVP\Installer_Windows directory.

Step 4 Follow the InstallShield wizard to Run setup.exe from the D:\CVP\Installer_Windows directory:

a) Accept the license agreement.
b) In the **Select Packages** screen, check the type you are adding.
c) Click **Next**.
d) On the **Voice Prompt Encode Format** screen, select the codec according to your requirement.
e) In the **Choose Destination Location** screen, accept the default. Click **Next**.
f) In the **X.509 certificate** screen, enter the information that you want to include in the certificate.
g) In the **Ready to Install** screen, click **Install**.
h) Select the option to restart the computer after installation. Click **Finish**.

Step 5 If Unified CVP Engineering Specials are available, copy them to the local drive. Follow the InstallShield wizard to install them.

Step 6 Unmount the ISO image.

Unified Customer Voice Portal Licenses

Generate a License

For instructions on generating Unified CVP licences, see the *Smart Licensing* section in *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Setup Unified CVP Media Server IIS

Procedure

Step 1 Navigate to **Start** > **Administrative Tools**.

Step 2 Choose **Server Manager** option navigate to **Manage** > **Add Roles and Features**.

Step 3 Goto **Installation Type** tab, choose **Role based or featue based installation** option and click **Next**.

Step 4 On **Server Selection** window, select server from the list and click **Next**.

Step 5 Check **Web Sever(IIS)** check box to enable IIS and click **Next**.

Step 6 No additional features are necessary to install Web Adaptor, click **Next**.
Displays **Web Server Role(IIS)** tab.

Step 7 Click **Next**.
Displays **Select Role Services** tab.

Step 8 Ensure that the web server components listed below are enabled.

- Web Server
  - Common HTTP Features
    - Default Document
    - Static Content
  - Security
    - Request Filtering
    - Basic Authentication
    - Windows Authentication
  - Application development
    - .NET Extensibility 4.6
    - ASP.NET 4.6
    - ISAPI Extensions
    - ISAPI Filters
- Management Tools
  - IIS Management Console
  - IIS Management Compatibility
    - IIS6 Metabase Compatibility
  - IIS Management Scripts and tools
  - Management Service

Step 9 Click **Next**.

Step 10 Ensure that your settings are correct and click **Install**.

Step 11 After installation click **Close**.

Related Topics

Install FTP Server, on page 190
Enable FTP Server, on page 190

Install FTP Server

Procedure

Step 1 Select **Start** > **Administrative Tools**.

Step 2 Select **Server Manager** and click **Manage**.

Step 3 Select **Add Roles and Features** and click **Next**.

Step 4 In the **Installation Type** tab, select **Role-based or feature-based Installation** and click **Next**.

Step 5 Select required server from the list and click **Next**.

Step 6 On the **Server Roles** page, expand **Web Server (IIS)**.

Step 7 Check **FTP Server** and click **Next**.

Step 8 On the **Features** page, click **Next**.

Step 9 On the **Configuration** page, click **Install**.

Enable FTP Server

Procedure

Step 1 Go to **Start** > **Programs** > **Administrative Tools**> **Server Manager**.

Step 2 Expand **Roles** in the left panel of the **Server Manager** window.

Step 3 Expand **Web Server (IIS)** and select **Internet Information Services (IIS) Manager**.

Step 4 In the **Connections** panel:

a) Expand the CVP server to which you are adding the FTP site.

b) Right-click on **Site** and choose **Add FTP Site**.

Step 5 Enter the **FTP Site Name**.

Step 6 From the **Physical Path** field, browse to `C:\Inetpub\wwwroot` and click **Next**.

Step 7 Choose **IP Address of CVP** from the drop-down list.

Step 8 Enter the port number.

Step 9 Select the **No SSL** check box and click **Next**.

Step 10 Select the **Anonymus** and **Basic** check boxes in **Authentication** panel.

Step 11 Choose **All Users from Allow Access To** from the drop-down list.

Step 12 Select the **Read and Write** check box and click **Finish**.

Configure Basic Settings for FTP Server

Procedure

Step 1 Navigate to the FTP server.

Step 2 In the **Actions** tab, select **Basic Settings**.

Step 3 Click **Connect As**.

Step 4 Choose the **Application User (pass-through authentication)** option and click **OK**.

Step 5 Click **OK** in **Edit Site** window.

Install Cisco Unified CVP Reporting Server

This task is required for the installation of the optional Unified CVP Reporting server.

The IBM Informix database server is installed as part of the Unified CVP Reporting Server.

Before installing the Unified CVP Reporting Server, you must configure a database drive.

Complete the following procedure to install the Unified CVP Reporting server:

Before you begin

IBM Informix database server 12.10 FC3 is installed as part of the Unified CVP Reporting Server.

- Only the actual Local Administrator (should not be renamed) of this system can install CVP Reporting Server.
- Ensure that Unified CVP Reporting Server is not part of any domain and is part of a work group.

Procedure

Step 1 Log in to your system as a user with administrative privileges.

Step 2 Mount the Unified CVP ISO image to the virtual machine. For more information, see Mount ISO Files, on page 166.

Step 3 Run setup.exe from the DVD drive located at the `CVP\Installer_Windows` directory.

Step 4 Follow the InstallShield wizard to Run setup.exe from the `D:\CVP\Installer_Windows` directory:

a) Accept the license agreement.
b) In the **Select Packages** screen, check **Reporting Server**.
c) In the **Choose Destination Folder** screen, select the folder location for the CVP installation folder.
d) In the **X.509 certificate** screen, enter the information that you want to include in the certificate.

e) In the **Choose the database data and backup drive** screen, enter the drive letter (typically, E).
f) In the **Database size selection** screen, select Premium (438 GB).
g) In the **Ready to Install** screen, click **Install**.
h) Enter the Reporting Server password when prompted.
i) Select the option to restart the computer after installation. Click **Finish**.

Step 5 If Unified CVP Engineering Specials are available, copy them to the local drive. Follow the InstallShield wizard to install them.

Step 6 Unmount the ISO image.

What to do next

Repeat this procedure if your deployment requires a second, external Unified CVP Reporting Server.

Install Publishers/Primary Nodes of VOS-Based Contact Center Applications

This task is required for the publisher/primary nodes of the three VOS-based contact center applications: Cisco Cloud Connect, Cisco Finesse, Cisco Unified Communications Manager, and Cisco Unified Intelligence Center.

Before you begin

DNS Configuration is mandatory for installation of Cisco Cloud Connect, Cisco Unified Communications Manager, Cisco Unified Intelligence Center, Cisco Finesse and Cisco Identity Service (IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Procedure

Step 1 Create a virtual machine for your VOS-based contact center application using the OVA.

Step 2 Mount the ISO image for the software to the virtual machine.

Step 3 Select the virtual machine, power it on, and open the console.

Step 4 Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen:

- If you are installing Finesse or Unified Communications Manager, select **OK**.
- If you are installing Unified Intelligence Center, select **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center with Live Data, and Cisco Identity Service (IdS) on the same server.
- If you are installing Cloud Connect, select **Cisco Contact Center Cloud Connect**, and then select **OK**.

d) In the **Proceed with Install** screen, select **Yes**.
e) In the **Platform Installation Wizard** screen, select **Proceed**.

f) In the **Apply Patch** screen, select **No**.

Finesse does not have this step.

g) In the **Basic Install** screen, select **Continue**.

h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

Note For Live Data servers, use the same timezone for all the nodes.

i) In the **Auto Negotiation Configuration** screen, select **Continue**.

j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.

k) In the **DHCP Configuration** screen, select **No**.

Finesse does not have this step.

l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.

m) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.

n) Enter your DNS client configuration. Select **OK**.

Important DNS client configuration is mandatory for Finesse. If you do not perform this step, agents cannot sign in to the desktop and you must reinstall Finesse.

o) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.

p) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.

q) In the **First Node Configuration** screen, select **Yes**.

r) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.

Important Proper NTP configuration is essential.

s) In the **Security Configuration** screen, enter the security password and select **OK**.

t) In the **SMTP Host Configuration** screen, select **No**.

Finesse does not have this step.

u) Unified Communications Manager only: On the **Smart Call Home Enable** screen, select **Disable All Call Home on System Start**.

v) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.

w) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

Step 5 Unmount the ISO image.

Note After successful installation of Cisco Unified Intelligence Center, import the stock templates.

Configure the Cluster for Cisco Unified Intelligence Center

Procedure

Step 1 Direct a browser to the URL `https://<hostmame>:8443/oamp`, where <*hostname*> is the hostname of your Cisco Unified Intelligence Center publisher.

Step 2 Sign in using the system application user ID and password that you defined during installation.

Step 3 From the section in the left, select **Device Configuration**.

Step 4 Click **New**.

Step 5 On the Device Configuration fields for the Subscriber, enter a name, the hostname or IP address or FQDN, and a description for the device.

Note All CUIC Subscribers must be entered here before you can install the software.

Step 6 After you complete the cluster configuration, restart the publisher.

Note For 2000 Agents deployment, the system updates the Live Data failover settings.

Unified Communications Manager License

Note From Release 12.0 onwards, Cisco Smart Licensing replaces Cisco Prime License Manager. To use Cisco Smart Licensing, create and configure a Smart Account before you upgrade or migrate the Unified Communications Manager server. For more information, see **Licensing** section in *Installation Guide for Cisco Unified Communications Manager and IM and Presence Service*, at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Generate and Register License

Procedure

Step 1 Launch Unified Communications Manager in a browser (`https://<IP Address of Unified CM Publisher>`).

Step 2 Click **Cisco Prime License Manager** and navigate to **Licenses** > **Fulfillment**.

Step 3 Under **Other Fulfillment** options, click **Generate License Request**.

Step 4 When the **License Request and Next Steps** window opens, copy the text (PAK ID).

Step 5 Click the **Cisco License Registration** link.

Step 6 Sign in and click **Continue to Product License Registration**.

Step 7 In the **Enter a Single PAK or Token to fulfill** field, paste your PAK ID and click **Fulfill Single PAK/Token**.

You receive the license file in an email message.

Install License

Procedure

Step 1 Unzip the license file from the email message.

Step 2 Under Other Fulfillment Options, select **Fulfill Licenses from File**.

Step 3 Click **Browse** and locate your license file.

Step 4 Click **Install** and close the popup window.

Step 5 Navigate to **Product Instances**. Then click **Add**.

Step 6 Fill in the name, hostname/IP address, username, and password for your Cisco Unified Communications Manager Publisher.

Step 7 Select Product type of Unified CM.

Step 8 Click **OK**.

Step 9 Click **Synchronize Now**.

Configure the Cluster for Cisco Unified Communications Manager

Procedure

Step 1 Launch Unified Communications Manager Publisher in a browser (https://<IP Addr of CUCM Publisher>/ccmadmin).

Step 2 Select **System** > **Server** > **Add New**.

Step 3 On the Server Configuration page, select **CUCM Voice/Video** for the **Server Type**. Click **Next**.

Step 4 On the Server Configuration page, enter the IP Address of the subscriber.

Step 5 Click **Save.**

Create a Unified Communications Manager AXL User Account

Create a Unified Communications Manager AXL user in Unified Communications Manager Administration. First create an Access Control Group with Standard AXL API Access, and then create an Application User with permission for that Access Control Group.

Procedure

Step 1 Launch Unified Communications Manager Administration in a browser (`https://<IP Address of Unified Communications Manager Publisher>/ccmadmin`).

Step 2 Create an Access Control Group, as follows:

a) Navigate to **User Management** > **User Settings** > **Access Control Group**.
b) Click **Add New**.
c) Enter a name for the Access Control Group.
d) Click **Save**.

The **Access Control Group Configuration** page opens.

e) From the **Related Links** drop-down menu, select **Assign Role to Access Control Group** and click **Go**.
f) Click **Assign Role to Group**.

The **Find and List Roles** popup window opens.

g) Click **Find**.
h) Check the **Standard AXL API Access** check box.
i) Click **Add Selected**.
j) Click **Save**.

Step 3 Create an Application User, as follows:

a) Navigate to **User Management** > **Application User**.
b) Click **Add New**.
c) Enter a name and password for the Application User.
d) In the **Permissions Information** section, click **Add to Access Control Group**.

The **Find and List Access Control Group** popup window opens.

e) Click **Find**.
f) Check the check box for the Access Control Group you created.
g) Click **Add Selected.**
h) Click **Save**.

Configure the Cluster for Cisco Finesse

Procedure

Step 1 Launch the Cisco Finesse primary node in a browser (`https://<FQDN of Finesse Primary node>/cfadmin`).

If you are using an IPv6 client, you must include the port number in the URL (https://<*FQDN of Finesse Primary node*>:8445/cfadmin).

Step 2 Go to **Home > Cluster Settings**. (This path is based on the default configuration and assumes that you have not changed the page for the Cluster Settings gadget.)

Step 3 Add the hostname for the Cisco Finesse secondary node.

Step 4 Click **Save**.

Step 5 Restart Cisco Finesse Tomcat as follows:

a) To stop the Cisco Finesse Tomcat service, enter this CLI command: **utils service stop Cisco Finesse Tomcat** .

b) To start the Cisco Finesse Tomcat service, enter this CLI command: **utils service start Cisco Finesse Tomcat** .

Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications

Note This task is required for installation of the subscriber/secondary nodes of the three VOS-based contact center applications: Cisco Cloud Connect, Cisco Finesse, Cisco Unified Communications Manager, and Cisco Unified Intelligence Center.

Before you begin

DNS Configuration is mandatory for installation of Cisco Cloud Connect, Cisco Unified Communications Manager, Cisco Unified Intelligence Center, and Cisco Finesse. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Before you install the subscriber/secondary nodes, you must install the publisher/primary nodes and configure the clusters which include the subscriber's hostnames.

Procedure

Step 1 Create a virtual machine for your VOS-based contact center application using the OVA.

Step 2 Mount the ISO image for the software to the virtual machine.

Step 3 Select the virtual machine and power it on, and open the console.

Step 4 Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.

b) In the **Success** screen, select **OK**.

c) In the **Product Deployment Selection** screen:

- If you are installing Finesse or Unified Communications Manager, select **OK**.
- If you are installing Unified Intelligence Center, select **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center, Live Data, and Cisco Identity Service (IdS) on the same server.
- If you are installing Cloud Connect, select **Cisco Contact Center Cloud Connect**, and then select **OK**.

Step 5 Follow the Install wizard, making selections as follows:

a) In the **Proceed with Install** screen, select **Yes**.
b) In the **Platform Installation Wizard** screen, select **Proceed**.
c) In the **Apply Patch** screen, select **No**.

Finesse does not have this step.

d) In the **Basic Install** screen, select **Continue**.
e) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

Note For Live Data servers, use the same timezone for all the nodes.

f) In the **Auto Negotiation Configuration** screen, select **Continue**.
g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.

Finesse does not have this step.

i) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
j) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.

Important DNS client configuration is mandatory for Finesse. If you do not perform this step, agents cannot sign in to the desktop and you must reinstall Finesse.

k) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
l) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
m) In the **First Node Configuration** screen, select **No**.
n) In the warning screen, select **OK**.
o) In the **Network Connectivity Test Configuration** screen, select **No**.
p) In the **First Node Access Configuration** screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select **OK**.
q) In the **SMTP Host Configuration** screen, select **No**.

Finesse does not have this step.

r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

Step 6 Unmount the ISO image.

Activate Services

Complete the following procedure to activate services.

Procedure

Step 1 Open Cisco Unified CM Administration at `https://<IP Address of the CUCM Publisher>/ccmadmin`.

Step 2 Select Cisco Unified Serviceability from the **Navigation** menu and click **Go**.

Step 3 Select **Tools** > **Service Activation**.

Step 4 From the Server drop-down list, choose the server on which you want to activate the service, and then click **Go**.

Step 5 For the Publisher, check the following services to activate and click **Save**:

- Cisco CallManager
- Cisco IP Voice Media Streaming App
- Cisco CTIManager
- Cisco Tftp
- Cisco Bulk Provisioning Service
- Cisco AXL Web Service
- Cisco Serviceability Reporter
- Cisco CTL Provider
- Cisco Certificate Authority Proxy Function
- Cisco Dialed Number Analyzer Server

Step 6 For the Subscribers, check the follow services to activate and click **Save**:

- Cisco CallManager
- Cisco IP Voice Media Streaming App
- Cisco CTIManager
- Cisco AXL Web Service
- Cisco CTL Provider
- Cisco Dialed Number Analyzer Server

Install the External HDS

Install and Configure the External HDS

Note You must not exceed the maximum number of AW-HDS-DDS that the design permits for the corresponding deployment type.

The default deployment pulls data from the on-box AW-HDS-DDS database on the Unified CCE AW-HDS-DDS, where Real-time, Historical and Call Detail Data are stored.

If you need a longer retention period, you can optionally install the Administration Server, Real Time and Historical Data Server, Detail Data Server (AW-HDS-DDS) on a maximum of two separate, external servers. Each external server is configured as **Central Controller Side A Preferred** or **Central Controller Side B Preferred**.

For more information about retention, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html.

Important The External HDS (AW-HDS-DDS) must be able to connect to the Packaged CCE Side A and Side B ESXi hosts.

Refer to the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html for external HDS server requirements.

Follow this sequence of tasks to install an external HDS.

Sequence	Task
1	Install Microsoft Windows Server, on page 172
2	Install Antivirus Software, on page 171
3	Install Microsoft SQL Server, on page 174
4	Install Cisco Unified Contact Center Enterprise, on page 183
5	Configure SQL Server for CCE Components. Refer the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.
6	Configure the database drive for the amount of data you want to keep. See Configure Database Drive, on page 169
7	Create an HDS Database for the External HDS, on page 201
8	Configure the External HDS , on page 201
9	Configure Unified Intelligence Center SQL User Account on the External HDS, on page 202

Sequence	Task
10	Configure Unified Intelligence Center Data Sources for External HDS. Refer the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.
11	If you have an IPv6 enabled deployment, configure a Forward lookup AAAA record for the External HDS in DNS. Refer to the Configure DNS for IPv6 section in the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Create an HDS Database for the External HDS

Create the HDS database using ICMDBA.

Procedure

Step 1 Open **Unified CCE Tools** > **ICMdba**.

Note You must add instances to display in the ICMDBA. For more information, see Add a UCCE Instance, on page 203.

Step 2 Expand the instance tree view on the newly added external HDS until you can see your instance.

Step 3 Right click on the instance and select **Create**.

Step 4 In the **Select component** drop-down list, select **Administration & Data Server** and click **OK**.

Step 5 In the **Select AW type** drop-down list, select **Enterprise** and click **OK**.

Step 6 From the menu, select **Database > Create**. Click **Add**.

Step 7 Click the **Data** radio button, select the second disk drive, and enter the desired HDS size. Click **OK**.

Note Ensure that there is enough free space in the hard disk (at least 20% of database size) to accommodate the log growth.

Step 8 Click the **Log** radio button, select the second disk drive, and enter the desired log size. Click **OK**.

Note Ensure that there is enough free space in the hard disk (at least 20% of database size) to accommodate the log growth.

Step 9 Click **Create**.

Configure the External HDS

Procedure

Step 1 Open **Unified CCE Web Setup**.

Step 2 Choose **Component Management** > **Administration & Data Servers**. Click **Add.**

Step 3 On the **Deployment** page, configure as follows:

Step 4 On the Add Administration & Data Servers page, configure as follows:

a) Choose the current instance.
b) Choose the deployment type as **Enterprise**.
c) Choose the deployment size as **Small to Medium**.
d) Click **Next.**

Step 5 On the **Role** page, in the Server Role in a Small to Medium Deployment section, select the **Administration Server, Real-time and Historical Data Server and Detail Data Server (AW-HDS-DDS)** option.

Step 6 On the **Administration & Data Servers Connectivity** page:

a) Click the radio button for **Primary Administration & Data Server**.
b) In the **Secondary Administration & Data Server* field, enter the hostname for the server.
c) In the **Primary Administration & Data Server* field, enter the hostname for the server.
d) In the **Primary/Secondary Pair (Site) Name* field, enter **`CCE-AW-1`** for the first External HDS or **`CCE-AW-2`** for the second External HDS.
e) Click **Next.**

Step 7 On the **Database and Options** page, configure as follows:

a) In the **Create Database(s) on Drive** field, choose **C**.
b) DO NOT click the **Agent Re-skilling** web tool. Packaged CCE does not support this tool. Supervisors reskill agents using the Agent tool in Unified CCE Administration.
c) Click **Internet script editor**.
d) Click **Next.**

Step 8 On the **Central Controller Connectivity** page, configure as follows:

a) For Router Side A, enter the IP Address of the Unified CCE Rogger A.
b) For Router Side B, enter the IP Address of the Unified CCE Rogger B.
c) For Logger Side A, enter the IP Address of the Unified CCE Rogger A.
d) For Logger Side B, enter the IP Address of the Unified CCE Rogger B.
e) Enter the Central Controller Domain Name.
f) Click **Central Controller Side A Preferred** or **Central Controller Side B Preferred** .
g) Click **Next.**

Note The Administration & Data Server can connect to the central controller with a hostname of maximum 24 characters.

Step 9 Review the **Summary** page, and then click **Finish.**

Configure Unified Intelligence Center SQL User Account on the External HDS

Procedure

Step 1 Launch Microsoft SQL Server Management Studio using the System Administrator login credentials.

Step 2 Navigate to **Security** >**Logins**, right-click **Logins** and select **New Login**.

This login is used when you configure the data sources for Cisco Unified Intelligence Center reporting.

Step 3 On the General Screen:

a) Enter the Login Name.
b) Select **SQL Server authentication**.
c) Enter and confirm the Password.
d) Uncheck **Enforce password policy**.

Step 4 Click **User Mapping**.

a) Check the databases associated with the AWdb.
b) Choose each database and associate it with the **db_datareader** and **public** role, and click **OK**.

Step 5 Click **OK**.

Add a UCCE Instance

Procedure

Step 1 Launch **Web Setup** in the VM you want installed or upgraded.
Step 2 Sign in as a domain user with local administrator permission.
Step 3 Click **Instance Management** and then click **Add**.
Step 4 In the **Add Instance** dialog box, choose the customer facility and instance.
Step 5 In the **Instance Number** field, enter 0.
Step 6 Click **Save**.

Set Live Data Secondary Node

Use the **set live-data secondary** command to provide the primary node the address of the secondary node.

Procedure

Step 1 Log in to your primary Live Data node.
Step 2 Run the following command to set the secondary node:

set live-data secondary *name*
name
Specifies the hostname or IP address of the Live Data secondary node.

Set IdS Subscriber Node

You must provide the publisher node the address of the subscriber node. You do this with the **set ids subscriber** command.

Procedure

Step 1 Log in to your publisher IdS node.

Step 2 Run the following command to set the subscriber node:

set ids subscriber *name*
name
Specifies the hostname or ip address of the IdS subscriber node address.

What to do next

You can use these Cisco IdS CLI commands only in an IdS standalone deployment. You run these commands on the IdS publisher node.

Required Minimum Privilege Level: Ordinary

Use this command to show IdS subscriber node information.

show ids subscriber

There are no required parameters.

Required Minimum Privilege Level: Advanced

Use this command to unset IdS subscriber node configuration.

unset ids subscriber

There are no required parameters.

Install Enterprise Chat and Email

Enterprise Chat and Email (ECE) is an optional feature that provides chat and email functionality to the contact center. In Packaged CCE 2000 Agents deployment, you can deploy ECE Data Servers on-box for up to 400 agents. Deploy ECE off-box for up to 1500 agents. You can also deploy the ECE Data Servers on a separate server.

Note Packaged CCE requires that the **Context Root Name** is set to **system** while installing ECE. Setting **Context Root Name** to any name other than **system** will result in integration failure between Packaged CCE and ECE. **Context Root Name** can only be set while installing ECE, reinstalling ECE is required to change it.

Note Core servers and external servers support ECE high availability.

- ECE Data Server can be deployed on both Side A and Side B.
- ECE Data Servers can be deployed as external machines.

Deploy the ECE Web Server on an external server. You can place that server either in the same data center as the ECE Data Server or in a DMZ if customer chat interactions require that.

Use OVA file to create a virtual machine for an on-box ECE. For information about creating a virtual machine, see Create a Virtual Machine from the OVA, on page 166.

ECE 12.0 doesn't support the archive database. While upgrading from ECE 11.6 to 12.0 in a PCCE 2000 agent deployment, if you choose to refer to the old archive database, keep a copy of the archive database off the PCCE box. For more information, see the *Planning Database Upgrade from SQL 2014 to SQL 2016* section in the *Enterprise Chat and Email Installation Guide (for Packaged Contact Center Enterprise)* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html.

For capacity information, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise*, available at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html.

Install Cisco Virtualized Voice Browser

Cisco Virtualized Voice Browser (Cisco VVB) provides a platform for interpreting VXML documents. Cisco VVB serves as an alternative to the use of IOS Voice Browsers (VXML gateways). When an incoming call arrives at the contact center, Cisco VVB allocates a VXML port that represents the VoIP endpoint. Cisco VVB sends HTTP requests to the Unified CVP VXML server. The Unified CVP VXML server runs the request and sends back a dynamically generated VXML document.

Cisco VVB is installed on box. Installation and configuration procedures are documented in the *Installation and Upgrade Guide for Cisco Virtualized Voice Browser* at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-installation-guides-list.html.

Install the Language Pack

If a customer requires a language other than the default (English), download the Packaged CCE Language Pack executable from the Unified Contact Center Download Software page.

Install Language Pack

Install the Language Pack on the AW machine and on any External HDS servers after upgrading them.

After you install the Language Pack, the Unified CCE Administration Sign In page has a language drop-down menu that lists all available languages. Select a language to display the user interface and the online help in that language.

Uninstall Language Pack

You can uninstall the Language Pack from Windows **Control Panel > Programs and Features > Uninstall or change a program**.

Set Subscriber or Secondary Node of Cloud Connect

Use the **set cloudconnect subscriber** command to provide the address of the secondary node in the primary node.

Procedure

Step 1 Sign in to your primary Cloud Connect node.

Step 2 Run the following command to set the secondary node:

set cloudconnect subscriber [name]

name – Specifies the FQDN or IP address of the Cloud Connect subscriber node (maximum 255 characters).

Common Software Upgrade Procedures

Run EDMT

Before you begin

- If you are configuring SQL services to run as Virtual account (NT SERVICE) or Network Service account (NT AUTHORITY\NETWORK SERVICE), you must run EDMT as an administrator.
- The installer, not the EDMT, upgrades the AW database for the Administration & Data Server.

Procedure

Step 1 Launch EDMT.exe.

Step 2 In the **Cisco Unified ICM/Contact Center Enterprise Enhanced Database Migration Tool** that appears, click **Next**.

Step 3 Under **Migration Type**, click the **Common Ground** radio button and then click **Next**.

Step 4 In the **Warning** dialog box that appears, click **Yes**.

Step 5 From the **Authentication** drop down list, choose either **Windows Authentication** or **SQL server Authentication**.

Step 6 Click **Refresh Database List**, and select the database you want to migrate from that list.

Step 7 Click **Next**.

Step 8 Click **Start Migration**.

Note The EDMT displays status messages during the migration process, including warnings and errors. Warnings are displayed for informational purposes only and do not stop the migration. Errors stop the migration process and leave the database in a corrupt state. If an error occurs, restore the database from your backup, fix the error, and run the tool again.

Step 9 Click **Exit** after the data migration is complete.

Upgrade VMware vSphere ESXi

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 CVP Reporting Server

You cannot upgrade CVP Reporting Server from 12.0 to 12.6 because the version of IBM Informix database server has changed. You need to uninstall CVP Reporting Server 12.0 and install CVP Reporting Server 12.6 . For more details, see the **Upgrade Unified CVP Reporting Server** section in the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

Upgrade Cisco Voice Gateway IOS Version

Perform this procedure for each gateway on the side you are upgrading.

Upgrade the Cisco Voice Gateway IOS version to the minimum version required by this release. See the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for IOS support information.

For more information, see https://www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/upgrade.pdf.

Procedure

Step 1 Copy the new image from the remote TFTP server into flash memory, making sure that you specify your own TFTP server's IP address and Cisco IOS filename.

Step 2 Verify that the new image was downloaded.

Step 3 Boot using the new image. Update the gateway config to boot using the new version.

Step 4 Reload the gateway to use the new image.

Install Cisco JTAPI Client on PG

After setting up the Cisco Unified Communications Manager (CUCM) PG, you must install the Cisco JTAPI client. PG uses Cisco JTAPI to communicate with CUCM. Install the Cisco JTAPI client from CUCM Administration.

Note Continue with the steps provided in this section if you are installing the JTAPI client for CUCM version earlier than Release 12.5.

To install the JTAPI client for CUCM, Release 12.5 and above, see Install Cisco JTAPI Client on PG, on page 208.

Before you begin

Before you install the JTAPI client, ensure that the previous version is uninstalled.

Procedure

Step 1 Open a browser window on the PG machine.

Step 2 Enter the URL for the Unified Communications Manager Administration utility: http://<*Unified Communications Manager machine name*>/ccmadmin.

Step 3 Enter the username and password that you created while installing and configuring the Unified Communications Manager.

Step 4 Choose **Application** > **Plugins**. Click **Find**.

Step 5 Click the link next to **Download Cisco JTAPI for Windows**.We recommend you to download the 64 bit version. However, if you have already downloaded the 32 bit version, you can proceed to step 7.

Download the JTAPI plugin file.

Step 6 Choose **Save** and save the plugin file to a location of your choice.

Step 7 Open the installer.

Step 8 In the Security Warning box, click **Yes** to install.

Step 9 Choose **Next** or **Continue** through the remaining Setup screens. Accept the default installation path.

Step 10 When prompted for the TFTP Server IP address, enter the CUCM IP address.

Step 11 Click **Finish**.

Step 12 Reboot the machine.

Install Cisco JTAPI Client on PG

Complete the following procedure only if you are installing JTAPI client to connect to Cisco Unified Communications Manager, Release 12.5 and above.

Before you begin

Before you install the JTAPI client, ensure that the previous version is uninstalled.

Procedure

Step 1 Open a browser window on the PG machine.

Step 2 Enter the URL for the Unified Communications Manager Administration utility: http://<*Unified Communications Manager machine name*>/ccmadmin.

Step 3 Enter the username and password that you created while installing and configuring the Unified Communications Manager.

Step 4 Choose **Application** > **Plugins**. Click **Find**.

Step 5 Click the link next to **Download Cisco JTAPI Client for Windows** 64 bit or **Download Cisco JTAPI Client for Windows** 32 bit.

Download the JTAPI plugin file.

Step 6 Choose **Save** and save the plugin file to a location of your choice.

Step 7 Unzip the JTAPI plugin zip file to the default location or a location of your choice.

There are two folders in the unzipped folder `CiscoJTAPIx64` and `CiscoJTAPIx32`.

Step 8 Run the `install64.bat` file in the `CiscoJTAPIx64` folder or run the `install32.bat` file in the `CiscoJTAPIx32` folder.

The default install path for JTAPI client is `C:\Program Files\JTAPITools`.

Step 9 To accept the default installation path, click Enter and proceed.

Follow the instructions. Click Enter whenever necessary as per the instructions.

Note Starting from Cisco Unified Communications Manager (CUCM) 12.5 SU4 and 14.0 (or any other service updates thereafter) on these release trains, only 64-bit version of the JTAPI client is supported on the Agent PG.

The JTAPI client installation completes at the default location. The following message is displayed:

```
Installation Complete.
```

Step 10 Reboot the machine.

What to do next

Note The default location, where the JTAPI client is installed, also contains the `uninstall64.bat` and `uninstall32.bat` file. Use this file to uninstall this version of the client, if necessary.

Upgrade Cisco JTAPI Client on PG

If you upgrade Unified Communications Manager (Unified CM) in the contact center, also upgrade the JTAPI client that resides on the PG. To upgrade the JTAPI client, uninstall the old version of the client, restart the

server, and reinstall a new version. You install the JTAPI client using the Unified Communications Manager Administration application.

To install the JTAPI client for the Unified CM release that you have upgraded to, see the Install Cisco JTAPI Client on PG, on page 208 topic.

Before you begin

Before you perform this procedure, you must:

- Uninstall the old JTAPI client from the Unified Communications Manager PG
- Restart the PG server.

Disable Outbound Options High Availability (If Applicable)

Perform the following steps on Side A:

Procedure

Step 1 Launch **Websetup**. Navigate to **Component Management** > **Loggers**.

Step 2 Edit the **Logger** and navigate to **Additional Options**. Uncheck **Enable High Availability** under **Outbound Option** and click **Next**.

Step 3 Enable **Stop and then start(cycle) the Logger Service for this instance (if it is running)** checkbox . Click **Next** to complete the setup.

Step 4 Repeat similar steps (steps 1, 2, and 3) for side B.

Database Performance Enhancement

After you perform a Common Ground or a Technology Refresh upgrade, complete the procedures described in this section to enhance the performance of the database. This is a one-time process and must be run only on the Logger and AW-HDS databases during a maintenance window.

- Performance Enhancement of TempDB, on page 210 (You can skip this when performing a Technology Refresh upgrade)
- Performance Enhancement of Logger Database, on page 211
- Performance Enhancement of AW-HDS Database, on page 212

Performance Enhancement of TempDB

Perform this procedure on Logger, Rogger, AW-HDS-DDS, AW-HDS and HDS-DDS machines to get the benefits of TempDB features for SQL Server. For more information about the SQL Server TempDB Database and its use, see the Microsoft SQL Server documentation for TempDB Database.

Note This procedure applies to the Common Ground upgrade process only.

Note If the Performance Enhancement of TempDB procedure is already completed on Unified CCE 12.5(1) or 12.6(1), then do not repeat the same procedure upon upgrading to Unified CCE 12.6(2).

Procedure

Step 1 Use **Unified CCE Service Control** to stop the Logger and Distributor services.

Step 2 Login to **SQL Server Management Studio** and run the following queries on the primary database.

- To modify the existing TempDB Initial size to the recommended value:

```
ALTER DATABASE tempdb MODIFY FILE
   (NAME = 'tempdev', SIZE = 800, FILEGROWTH = 100)
ALTER DATABASE tempdb MODIFY FILE
   (NAME = 'templog', SIZE = 600, FILEGROWTH = 10%)
```

- To add multiple TempDB files:

```
USE [master];
GO
ALTER DATABASE [tempdb] ADD FILE (NAME = N'tempdev2', FILENAME = N'<SQL Server TempDB
path>' , SIZE = 800 , FILEGROWTH = 100);
ALTER DATABASE [tempdb] ADD FILE (NAME = N'tempdev3', FILENAME = N'<SQL Server TempDB
path>' , SIZE = 800 , FILEGROWTH = 100);
ALTER DATABASE [tempdb] ADD FILE (NAME = N'tempdev4', FILENAME = N'<SQL Server TempDB
path>' , SIZE = 800 , FILEGROWTH = 100);
GO
```

Note

- For example,

```
<SQL Server TempDB path> = C:\Program Files\Microsoft SQL
Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\tempdev2.ndf
```

- Make sure that you modify the values in the query based on the machines. For more information, see Increase Database and Log File Size for TempDB, on page 178.

Step 3 Restart the SQL Services.

Step 4 Start the Logger and Distributor services.

Performance Enhancement of Logger Database

Perform this procedure on Side A and Side B of the Logger database.

Procedure

Step 1 Use the Unified CCE Service Control to stop the Logger service.

Step 2 From the command prompt, run the **RunFF.bat** file which is located in the `<ICM install directory>:\icm\bin` directory.

Step 3 Proceed with the application of fill factor to Unified ICM databases.

Note: Based on the size of the database, it takes several minutes to several hours to apply fill factor to the database. For example, it takes anywhere between 2 to 3 hours for a 300-GB HDS. After the process is completed, the log file is stored in `<SystemDrive>:\temp\<DatabaseName>_Result.txt`.

Step 4 Use the Unified CCE Service Control to start the Logger service.

Troubleshooting Tips

See the `RunFF.bat/help` file for more information.

Performance Enhancement of AW-HDS Database

Procedure

Step 1 Use the Unified CCE Service Control to stop the Distributor service.

Step 2 From the command prompt, run the **RunFF.bat** file which is located in the `<ICM install directory>:\icm\bin` directory.

Step 3 Proceed with the application of fill factor to Unified ICM databases.

Note: Based on the size of the database, it takes several minutes to several hours to apply fill factor to the database. For example, it takes between 2 to 3 hours for a 300-GB HDS. After the process is completed, the log file is stored in `<SystemDrive>:\temp\<DatabaseName>_Result.txt`.

Step 4 Use the Unified CCE Service Control to start the Distributor service.

Troubleshooting Tips

See the `RunFF.bat/help` file for more information.

Improve Reporting Performance

To improve the performance of the reporting application, modify the following Windows settings on the database servers (AW-HDS, AW-HDS-DDS, HDS-DDS).

- Increase the Paging File Size to 1.5 times the server's memory.

  To change the Paging File Size, from the Control Panel search for Virtual Memory. In the Virtual Memory dialog box, select **Custom size**. Set both **Initial size** and **Maximum size** to 1.5 times the server memory.

- Set the server's **Power Options** to **High Performance**.

  From the Control Panel, select **Power Options**. By default, the **Balanced** plan is selected. Select **Show additional plans** and select **High performance**.

In SQL Server, disable **Auto Update Statistics** for AW and HDS databases.

In the SQL Server Management Studio, right-click the database name in the Object Explorer and select **Properties**. Select the **Options** page. In the **Automatic** section of the page, set **Auto Create Statistics** and **Auto Update Statistics** to **False**.

Reduce Reserved Unused Space for HDS and Logger

Enable trace flag 692 on HDS database server to reduce the growth of reserved unused space on the AW-HDS, AW-HDS-DDS, HDS-DDS database servers and Logger database, after you upgrade or migrate to Microsoft SQL 2017 or 2019. For more information about the trace flag 692, see the Microsoft Documentation.

Procedure

Run the following command to enable trace flag 692 on HDS database server and Logger database:

```
DBCC TRACEON (692, -1);
GO
```

Note An increase in the unused space may lead to unexpected purge trigger in HDS and Logger, trace flag 692 helps in mitigating this unexpected purge issue. After you enable the trace flag, there will be an increase of 10% to 15% CPU for a short duration. If the trace flag needs to be retained, the server startup options has to be updated using the -T(upper case) option. For more information, see https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/database-engine-service-startup-options?view=sql-server-ver15.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) facilitates the exchange of management information among network devices so that administrators can manage network performance and solve network problems. SNMP community strings, users, and network destinations are configured in Cisco Unified Serviceability.

Unified Serviceability is one of the tools that open from the Navigation drop-down in Cisco Unified Communications Solutions tools. You can also access Unified Serviceability by entering http://x.x.x.x/ccmservice/, where x.x.x.x is the IP address of the publisher.

See the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html for information about configuring SNMP for Unified CCE.

Community Strings

The SNMP agent uses community strings to provide security. You must configure community strings to access any management information base (MIB). Add new community strings in the Cisco Serviceability Administration interface.

A community string is configured with:

- a server
- a name of up to 32 characters

- a setting to accept SNMP packets from any host or from specified hosts
- access privileges (readonly, readwrite, readwritenotify, notifyonly, readnotifyonly, and none)
- a setting to apply the community string to all nodes in the cluster

Notification Destinations

Add notification destinations for delivery of SNMP notification events when events occur. Add and maintain notification destinations in the Cisco Serviceability Administration interface.

A notification destination is configured with:

- a server
- the host IP addresses of the trap destination
- a port number
- the SNMP version (V1 or V2c)
- the community string name to be used in the notification messages that the host generates
- the notification type
- a setting to apply to the notification destination configuration to all nodes in the cluster