Installing and Upgrading Guide for Cisco Hosted Collaboration Solution for Contact Center, Release 12.5(1) and 12.5(2)

First Published: 2020-02-05

Last Modified: 2022-07-26

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

Preface xi

Change History xi

About this Guide xii

Audience xii

Related Docs xii

Communications, Services, and Additional Information xii

Field Notice xiii

Documentation Feedback xiii

Conventions xiii

CHAPTER 1

Preparation 1

Important Consideration 1

Installation Approach 1

System Installation Dependencies 2

Automation Software 2

Hardware Requirements 3

HyperFlex M5 Support 3

Specification Based Hardware Support 4

Java Requirements 4

Certificate Management Requirements 4

Network Infrastructure 5

CHAPTER 2

Shared Component Installation 7

Configure an Identity Provider (IdP) 7

Install and Configure Active Directory Federation Services 7

Authentication Types 8

Install and Configure Unified CCDM 8
Common Procedures for Deploying Unified CCDM Servers 9
Configure Windows 9
Associate Unified CCDM Component Servers with Service Provider AD Domain 11
Configure Secondary Drive 11
Install the Diagnostic Framework for System CLI 12
Configure SNMP Traps 12
Deploy Unified CCDM Database Server 14
Procedures for Deploying Unified CCDM Data Server 16
Deploy Unified CCDM Web Server 20
Install Unified CCDM Web Server 21
Install CCDM Identity Server on Web Server 22
Configure Unified CCDM 22
Procedures for Configuring Unified CCDM 22
Install and Configure Unified Communication Domain Manager 28
Multinode Cluster Hardware Specifications 29
Multinode Installation 29
Create Virtual Machines from OVA Files 33
Create the HCM-F Device 35
Create a Provider 36
Add Reseller 37
Install and Configure Session Border Controller 38
Installing and Configuring Prime Collaboration Assurance and Analytics 38
Log in to Prime Collaboration 39
Enabling HCM-F and Prime Collaboration Assurance to Communicate 39
Install and Configure ASA Firewall and NAT 40
Setup ASA 40
Configure Multiple Context Modes 41
Enable Multiple Context Modes 41
Enable Interfaces 41
Configure Security Contexts 42
Configure Interfaces in the Context 42

CHAPTER 3 Core Component Installation 45

Core Components Installation Approach 45
Core Component Voice Gateway Installation 45
Configure Service Interface for Carrier Network 46
Configure Codec List 46
Golden Template Requirements 47
Create Golden Template for Unified CCE Rogger 48
Create Golden Template for Unified CCE Router 49
Create Golden Template for Unified CCE Logger 49
Create Golden Template for Unified CCE AW-HDS-DDS 50
Create Golden Template for Unified CCE AW-HDS 50
Create Golden template for Unified CCE HDS-DDS 51
Create Golden Template for Unified CCE PG 52
Create Golden Template for Unified CVP Server 52
Create Golden Template for Unified CVP OAMP Server 53
Create Golden Template for Unified CVP Reporting Server 53
Create Golden Template for Cisco Finesse 54
Create Golden Template for Cisco Unified Intelligence Center Coresident Deployment 54
Create Golden Template for Cisco Unified Intelligence Center 55
Create Golden Template for Live Data Reporting System 55
Create Golden Template for Cisco Identity Service 56
Create Golden Template for Cisco Unified Communications Manager 56
Common Procedures for Golden Templates 57
Download OVA Files 57
Create Virtual Machines 58
Mount ISO Files 59
Unmount ISO File 59
Install Microsoft Windows Server 59
Install VMware Tools for Windows 61
Install Antivirus Software 61
Disable Port Blocking 62
Install Microsoft SQL Server 63
Increase Database and Log File Size for TempDB 67
Convert the Virtual Machine to a Golden Template 67
Verification of the Downloaded ISO 67

CHAPTER 4 **Post-Installation** 69

Post-Installation Tasks 69

CHAPTER 5 **Upgrade** 71

Overview of the Upgrade Workflow 71

Upgrading Management Components 72

Upgrade HCM-F 72

Validate the HCM-F Upgrade 73

Upgrade UCDM 73

Validate the Unified CDM Upgrade 74

Upgrade Prime Collaboration Assurance 74

Validate the Upgrade of Prime Collaboration Assurance 74

Upgrade Unified CCDM 76

Validate the Unified CCDM Upgrade 76

Standard CC Upgrade 77

Upgrading Unified Customer Voice Portal Components 77

Upgrade the Unified Customer Voice Portal 77

Validate the Customer Voice Portal Upgrade 77

Upgrading Gateway Components 78

Upgrade Gateway Components 78

Upgrading the Cisco ASR 1000 Series Router for Cisco Unified Border Element (SP Edition) 78

Upgrade the IOS on the Cisco ASR 1006 for Cisco Unified Border Element (SP Edition) 78

Validate the Upgrade of Gateway Components 79

Upgrading the Unified Component 80

Upgrading the Unified Component 80

Upgrading Reporting Components 81

Upgrade Cisco Unified Intelligence Center 81

Validate the Upgrade of Unified Intelligence Center 81

Upgrading Desktop Components 81

Upgrade Finesse 81

Validate the Finesse Upgrade 82

Upgrade Desktop Clients 82

Validate the Upgrade of Desktop Clients 82

Upgrading Call-Processing Components 82
Upgrading Cisco Virtualized Voice Browser Components 82
Upgrade Cisco Unified Communications Manager 83
Validate the Upgrade of Cisco Unified Communications Manager 83

CHAPTER 6 **Uninstallation** 85
Uninstallation of Unified ICM/CCE base version 12.5(1) 85
Uninstall Unified CCE Maintenance Release 12.5(2) 85

CHAPTER 7 **CCE Orchestration** 87
Overview 87
Email Notification 87
Orchestration in CCE Deployment 88
System Requirements 88
Orchestration Support using Cloud Connect Server 89
Parallel Running of CLI 89
Orchestration Deployment Task Flow 90
Administration Task Flow 90
Maintenance Task Flow 91
Deployment Tasks 91
Generate the Artifactory API Key 91
CLI to configure proxy for orchestration 92
CLI to configure artifactory URL and API key 93
Onboard VOS Nodes to Orchestration Control Node 98
Onboard Windows nodes to orchestration control node 99
Add Deployment Type and Deployment Name 100
Validate Onboarded Nodes for Orchestration 101
Configure Email Notification 101
Configure Windows Server for Updates (Optional) 103
Administration Tasks 103
Check Installed Software Version and Patches 104
Install or Rollback Patch for Cloud Connect Server 104
List Available Patches for Specific Node or Group of Nodes 105
Install Patch to Specific Node or Group of Nodes 105

Roll Back Patch from Specific Node or Group of Nodes 106
Install Windows Updates to Specific Node or Group of Nodes 107
Roll Back Windows Update from Specific Node or Group of Nodes 108
Enable or Disable Compatibility Enforcement 108
List Available Upgrade Options 109
Upgrade a Specific Node or Group of Nodes or All Nodes 109
Perform Switch Forward on Specific VOS Node or Group of Nodes 111
Roll Back Upgrade from Specific Node or Group of Nodes 112
Check Status 113
Check Last Known Orchestration Operation Status on Remote Node 113
Start Unified ICM Services 114
Maintenance Tasks 114
Update VOS Nodes Onboarded to Orchestration Control Node 114
Remove VOS Nodes from Orchestration Control Node 115
Update Windows Nodes Onboarded to Orchestration Control Node 115
Validate Updated Nodes Onboarded for Orchestration 115
Configure Email Configuration 115
Delete Configuration for Email Notification 116
Unsubscribe Email Notification 117
Export and Import of Nodes Managed by Orchestration Control Node 117
Export Current Patch Level Details 118
Serviceability 119
Enable and View Windows Open SSH Logs 120
Configure SSH public key on Windows nodes 120
Self-Signed Certificate 121
Get Tomcat Certificate from Cloud Connect Server 121
Import Cloud Connect Server Tomcat Certificate to VOS Nodes 122
Things to Know 122

CHAPTER 8 **Appendix** 125
Core Components Server 125
Install Unified Contact Center Enterprise 125
Install Unified CVP Server 126
Install Unified CVP OAMP Server 126

Install Unified CVP Reporting Server 127
Install Voice OS-Based Applications 128
Install Publishers/Primary Nodes of VOS-Based Contact Center Applications 128
Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications 130

Preface

- Change History, on page xi
- About this Guide, on page xii
- Audience, on page xii
- Related Docs, on page xii
- Communications, Services, and Additional Information, on page xii
- Field Notice, on page xiii
- Documentation Feedback, on page xiii
- Conventions, on page xiii

Change History

Change	See	Date
12.5(2) MR changes	MR related changes in applicable sections	July 2022
12.5.2	Added the release number- 12.5(2) to title	July 2022
Dual Platform	Dual Platform support updates in applicable sections	July 2022
CCE Orchestration	CCE Orchestration, on page 87	August 2020
Initial Release of the Document for Release 12.5(1)		
Added a new section	Java Requirements, on page 4	March 2021

Change	See	Date
Removed prerequisite and modified note in the Section, Before you begin Modified features list	Install Microsoft SQL Server	February 2020
Added new procedure	Verification of the Downloaded ISO	
Updated the procedure	Disable Port Blocking	
Added certificate details	Upgrading the Unified Component	

About this Guide

This document describes how to install the core and shared components, and software for a new Cisco HCS for Contact Center solution, or to upgrade an existing Cisco HCS for Contact Center solution.

Audience

This guide is intended for users who install and upgrade Cisco HCS for Contact Center solution.

This guide assumes that you are already familiar with Cisco Contact Center products. You must acquire the necessary knowledge and experience regarding deployment and management of virtual machines before you deploy components on VMware virtual machines. Therefore, you must have a sound knowledge of the VMware infrastructure.

Cisco HCS for Contact Center is a subset of Core HCS, this document assumes that the HCS infrastructure is ready to set up the contact center. Therefore, components such as UCDM, CUBE Enterprise, and PCA must be installed as part of HCS setup.

Related Docs

Design Considerations and guidelines for deploying a Cisco HCS for Contact Center solution including various components and subsystems. See, https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-implementation-design-guides-list.html

Post-installation procedure for Cisco HCS for Contact Center, See https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.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 Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices
- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at https://cway.cisco.com/mynotifications.

Documentation Feedback

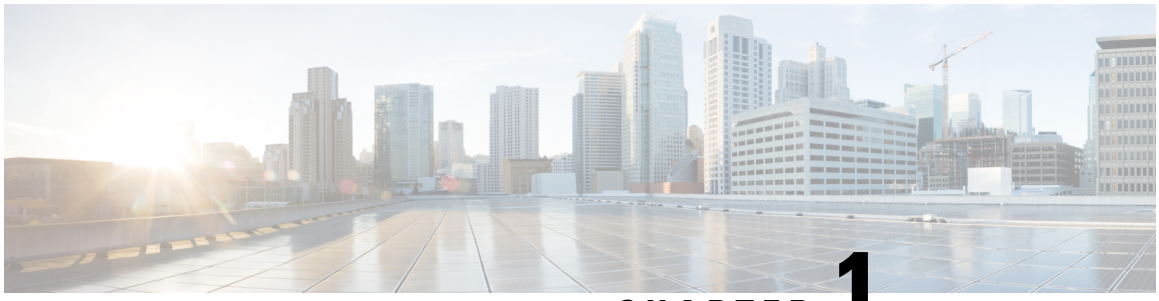
To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

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*.
`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.



CHAPTER 1

Preparation

Note This Cisco Unified Contact Center Enterprise Installation and Upgrade Guide provides the Install and Upgrade details and procedures for both 12.5(1) release and 12.5(2) maintenance release.

- Important Consideration, on page 1
- Installation Approach, on page 1
- System Installation Dependencies, on page 2
- Network Infrastructure, on page 5

Important Consideration

Note Before proceeding with ICM application installation, ensure that you follow the antivirus guidelines specified in the Section, Antivirus Guidelines of the Security 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.

Installation Approach

Cisco HCS for Contact Center service, delivers Cisco Unified Contact Center Enterprise (Unified CCE) in a virtualized environment on Cisco Unified Computing System (UCS).

Cisco HCS for Contact Center offers the same shared management (service fulfillment and assurance) and aggregation (carrier trunks) that is common for all customer instances and used for other Cisco HCS services.

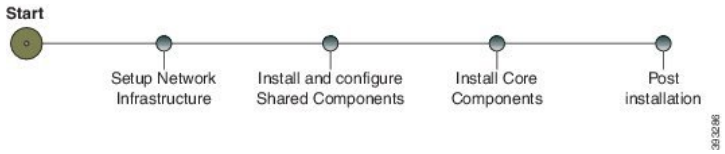
Cisco Core components include, Unified CVP, Unified CCE, Unified Communication Manager, Cisco Finesse, Unified Intelligence Center, CUBE-E. Install the core components using the golden template process as the standard approach.

Install the shared management and aggregation layer that consists of Unified Communication Domain Manager (UCDM), Cisco Unified Contact Center Domain Manager (Unified CCDM), Cisco Prime Collaboration - Assurance (PCA), and Cisco Adaptive Security Appliance (ASA). This combines the Cisco HCS components with multiple network connections and routes requests to a dedicated customer instance.

Install the network infrastructure layer that includes the implementation of UCS platform.

After you install the above, as part of post installation you can configure the customer instances for the supported deployment models. Depending upon your HCS for Contact Center deployment model, you can configure dedicated customer instances of 500, 2000, 4000, or 12000 agents and shared customer instances of 100 or 500 agents.

The following workflow describes the high-level installation sequence for Cisco HCS for Contact Center.



Related Topics

Shared Component Installation, on page 7
Core Components Installation Approach, on page 45

System Installation Dependencies

The components within each release set are compatible with each other and will interoperate correctly. The overall system may not be operational until you install all components or until you complete the initial configuration or setup.

For Nexus, ASA, and CUBE Enterprise supported release version, see https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html.

For information on all other component hardware and software versions and compatibility, see *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html.

Automation Software

Note Automation software is required for golden templates only.

Software	Version	Download	Notes
GoldenTemplateTool zip file	12.6(1)	HCS-CC-12.6.1-GoldenTemplate.zip	Download and extract the `GoldenTemplateTool.zip` file to run the automation tool. For more information, see *Automated Cloning and OS Customization* section in *Configuring Guide for Cisco HCS for Contact Center* https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

Software	Version	Download	Notes
PowerCLI	6.0, 32-bit	Download and then install this VMWare tool on the client computer to run the automation scripts. http://downloads.vmware.com/d/details/pcli50/dHRAYnQlKmpiZHAlJQ==	Use PowerCLI to run the automation script.
WinImage	8.5	Download and then install WinImage 8.5 on the client computer to run the automation scripts. See http://winimage.com/download.htm.	To configure: • Cisco Unified Communications Manager publisher and subscribers • Cisco Unified Intelligence Center publisher and subscriber • Cisco Finesse primary and secondary nodes WinImage creates a floppy image (.flp file) from the platformConfig.xml file. This file contains parameters for customizing publishers/primary and subscribers/ secondary nodes.

Hardware Requirements

HCS for Contact Center supports the following configurations:

For information on the TRC server support for this release, see the *Virtualization for Cisco HCS for Contact Center* guide at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/hcs_cc_virt.html

HyperFlex M5 Support

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.

Specification Based Hardware Support

Cisco HCS for Contact Center supports specification based hardware, but limits this support only to the UCS B-Series blade hardware. This section provides supported server hardware, component version, and storage configurations.

For more information on specification based hardware such as CPU types, see the*Collaboration Virtualization Hardware* guide at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-hardware.html

Java Requirements

A new 12.5(1a) base installer is available for customers, which has OpenJDK JRE as the supporting Java run time for all the CCE applications. Its predecessor the 12.5(1) installer employs Oracle JRE. Any installation done using the 12.5(1) installer can continue to use Oracle JRE, and can receive Java security updates and fixes from the Oracle website.

However, if there is a need to apply an ES on 12.5(1) that mandates the installation of ES55 (mandatory OpenJDK ES), then the Java updates would have to be downloaded and installed from the OpenLogic website.

CCE VMs installed using the 12.5(1a) installer would need the OpenJDK patches applied. You can verify the base installer version to be 12.5(1a) from **Control Panel** > **Programs** > **Programs and Features** > **Cisco Unified ICM/CCE 12.5.1a**.

Certificate Management Requirements

During installation of 12.5(2), Unified CCE installs the Java version 8 update 332. If your system has a Java version that is lower than version 8 update 332, perform the following steps:

Procedure

Step 1 Before you install 12.5(2):

a) Run the command at the command prompt: `cd %CCE_JAVA_HOME%\bin`.

Important Use %JAVA_HOME% if you are employing Oracle JRE.

b) Export the certificates of all the components imported into the truststore.

c) The command to export the certificates is *keytool -export -keystore <JRE path>\lib\security\cacerts -alias <alias of the component> -file <filepath>.cer*

d) Enter the truststore password when prompted.

Step 2 After 12.5(2) installation is complete, perform the following steps:

a) Run the command at the command prompt: `cd %CCE_JAVA_HOME%\bin`.

b) Import the certificates for all the components that you previously exported from the truststore before you installed 12.5(2). The command to import certificates is *keytool -import -keystore <JRE path>\lib\security\cacerts -file <filepath>.cer -alias <alias>*.

c) Enter the truststore password when prompted.

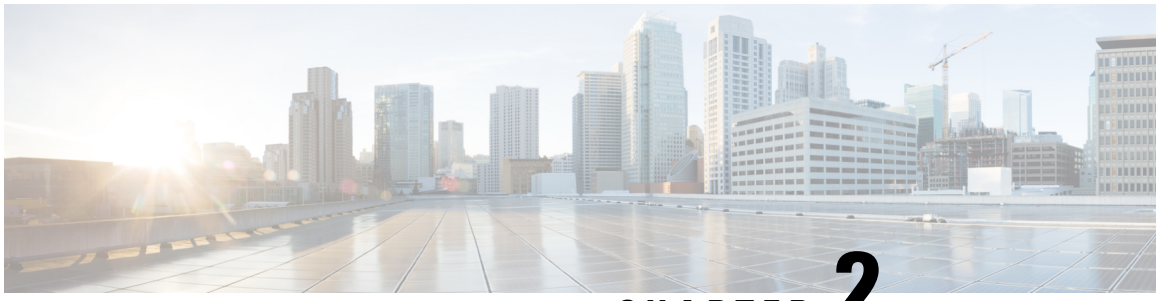
d) Enter 'yes' when prompted to trust the certificate.

Network Infrastructure

This section provides information on how to setup the network infrastructure for Cisco HCS for Contact Center. This section does not provide detailed installation instructions for individual components installation. For details information on installation, see Cisco Hosted Collaboration Solution, Installation Guide.

- Install and configure the Cisco UCS Server and Cisco UCS Manager.
- Install and configure the SAN Storage.
- Install and configure the MDS Series Switch.

  You can install the MDS Series Switch any time after the Nexus 7000 and 5500 switch.
- Install and configure the vCenter.
- Install and configure the Cisco Nexus 1000V Series Switch.



CHAPTER 2

Shared Component Installation

- Configure an Identity Provider (IdP), on page 7
- Install and Configure Unified CCDM, on page 8
- Install and Configure Unified Communication Domain Manager, on page 28
- Install and Configure Session Border Controller, on page 38
- Installing and Configuring Prime Collaboration Assurance and Analytics, on page 38
- Install and Configure ASA Firewall and NAT, on page 40

Configure an Identity Provider (IdP)

To support SSO for the contact center solution, configure an Identity Provider (IdP) that is compliant with the Security Assertion Markup Language 2.0 (SAML v2) Oasis standard. The IdP stores user profiles and provides authentication services to the contact center solution.

Note For a current list of supported Identity Provider products and versions, see the *Contact Center Enterprise Compatibility Matrix*.

This section provides sample configuration information for Microsoft AD FS.

Follow this sequence of tasks to configure the Identity Provider.

Sequence	Task
1	Install and Configure Active Directory Federation Services, on page 7
2	Set Authentication Type. See Authentication Types, on page 8.

Install and Configure Active Directory Federation Services

Follow Microsoft instructions and guidelines to install Microsoft Active Directory Federation Services (AD FS).

For example, see *Active Directory Federation Services Overview* at https://technet.microsoft.com/en-us/library/hh831502(v=ws.11).aspx

- For AD FS in Windows Server (AD FS 3.0), see the *AD FS Content Map* at http://aka.ms/adfscontentmap and *AD FS Technical Reference* at https://technet.microsoft.com/en-us/library/dn303410(v=ws.11).aspx.

Note Cisco IdS does not support AD FS Automatic Certificate Rollover. If the AD FS certificate gets rolled over, then re-establish the trust relationship between the IdS and AD FS.

Authentication Types

Cisco Identity Service supports form-based authentication of the Identity Provider.

For information on enabling form-based authentication in ADFS, see Microsoft documentation:

- For ADFS 3.0 see https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/

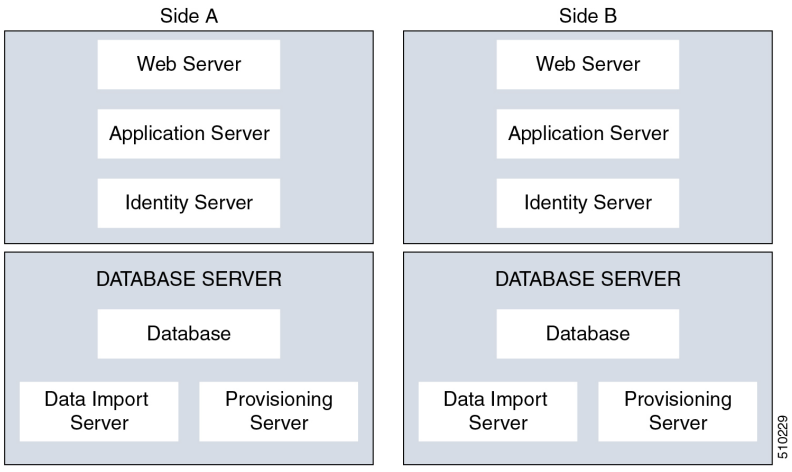
For Kerberos authentication to work, ensure to disable the form-based authentication.

- In AD FS on Windows Server , set the Authentication Type to Forms-based authentication (FBA). Refer to the following Microsoft TechNet article, http://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspx
- In AD FS on Windows Server, set the Authentication Policy to Forms Authentication. Refer to the following Microsoft TechNet article, https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/

Install and Configure Unified CCDM

For Cisco HCS for Contact Center, implement a dual-tier (distributed) system, as shown in the following figure. This system keeps the Web/Application and Identity Components of the Unified CCDM separated from the database server components.

Figure 1: Unified CCDM Dual-Tier Deployment



For dual-sided systems, complete the installation of the Unified CCDM servers on side A, before you begin the installation on side B.

Related Topics

Deploy Unified CCDM Database Server, on page 14
Deploy Unified CCDM Web Server, on page 20
Configure Unified CCDM, on page 22

Common Procedures for Deploying Unified CCDM Servers

Configure Windows

Complete the following procedure to configure Windows on all the Unified CCDM servers.

Related Topics

Configure Windows Feature Requirements, on page 9
Turn off FIPS Compliance, on page 10
Disable UAC, on page 10

Configure Windows Feature Requirements

Procedure

Step 1 Select **Server Manager** > **Manage** > **Add Roles and Features**.

Step 2 On the **Before you begin** page, click **Next**.

Step 3 On the **Select Installation Type** page, select the **Role-based or feature-based installation** option, then click **Next**.

Step 4 On the **Select destination server** page, select the **Select a server from the server pool** option, then click **Next**.

Step 5 On the **Select server roles** page, check the following check boxes:

- Application Server
- Select **File and Storage Services** > **File and iSCSI Services** and check the **File Server** check-box
- Web Server (IIS)

Step 6 Click **Next**.

Step 7 On the **Select features** page, check the **.Net Framework 4.5 Features** check box, then click **Next**.

Step 8 On the **Application server** page, click **Next**.

Step 9 On the **Select role services** page, check the following check boxes:

- .NET Framework 4.5
- COM+ Network Access
- Incoming Network Transactions
- Outgoing Networking Transactions

- TCP Port Sharing
- Web Server (IIS) Support
- Message Queuing Activation
- Named Pipes Activation
- TCP Activation

Step 10 Click **Next**.

Step 11 On the **Web server roles (IIS)** page, click **Next**.

Step 12 On the **Select role services** page, select the required role services, then click **Next**.

Step 13 Click **Specify an alternate source path**, then enter `\sources\sxs` this is available at Microsoft Windows Installer DVD or ISO. Click **OK**.

Step 14 Click **Install**.

Step 15 After installation, restart the server.

Turn off FIPS Compliance

Procedure

Step 1 Open the **Local Security Policy** application.

Step 2 Open the **Local Policies** folder, and then double-click **Security Options** to view the list of policies.

Step 3 Ensure that you disable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** policy.

Disable UAC

User Account Control (UAC) protects the operating system from malicious programs. When enabled, UAC may cause issues with the software used to install Unified CCDM. Disable UAC on all servers before you install the Unified CCDM. Complete the following procedure to disable UAC.

Procedure

Step 1 Select **Start** > **Control Panel** > **System and Security** > **Action Center** > **Change User Account Control settings**.

Step 2 Set **UAC** to **Never Notify**.

Step 3 Click **OK**.

Step 4 Restart your machine to commit to the new UAC settings.

You have now disabled UAC and are ready to install the Unified CCDM.

Note Re-enable UAC after you complete the Unified CCDM installation.

Associate Unified CCDM Component Servers with Service Provider AD Domain

Complete the following procedure to associate the Unified CCDM Component servers with Service Provider AD Domain.

Procedure

Step 1 Sign in to the machine using a local administrator account.
Step 2 Select **Start** > **Administrative Tools** > **Server Manager**.
Step 3 Select **Local Server** in the left panel and click **WORKGROUP** to change system properties.
Step 4 In the **Computer Name** tab, click **Change**.
Step 5 Select the **Domain** option to change the member from **Workgroup** to **Domain**.
Step 6 Enter the fully qualified Service Provider domain name and click **OK**.
Step 7 In the **Windows Security** pop-up window, validate the domain credentials and click **OK**.
Step 8 After successful authentication, click **OK**.
Step 9 Reboot the server and sign in with domain credentials.

Configure Secondary Drive

DO THIS FOR Virtual Machines that require an additional hard drive to archive data.

Procedure

Step 1 Open **Computer Management**.
Step 2 Expand **Storage** in the left pane, click **Disk Management**.
Step 3 Right-click **Disk 1** and choose **Online**.
Step 4 Right-click **Disk 1** and choose **Initialize Disk**.
Step 5 In Initialize Disk pop up window, under Select disks. Check **Disk 1** and choose **MBR (Master Boot Record)** under **Use the following partition style for the selected disks** pane. Click **OK**.
Step 6 Create a new disk partition as follows: right-click the disk you just initialized, choose **New Simple Volume**, and run the wizard.

Install the Diagnostic Framework for System CLI

Procedure

Step 1 To install the Diagnostic Framework component, start the Unified CCDM Installer, click **Support Tools** and select **Diagnostic Framework**.

The **Domain Manager: Diagnostic Framework Install Shield Wizard** window displays.

Step 2 Click **Next** to go through each window in turn.

Step 3 Accept the license agreement, then click **Next**.

Step 4 In the **Certificate** window, select the type of certificate installed with the Diagnostic Framework.

- **Self Signed:** A new certificate will be generated by the installer. This type of certificate should be used only for lab or test deployments.
- **Trusted Certificate:** An existing certificate, issued by a valid certificate server, will be associated at a later date. This option should be used for production deployments.

Step 5 Click **Next**.

Step 6 In the **wsmadmin Password Information** window, enter and confirm the password for the **wsmadmin** user, which is created to access the Unified System CLI tool. Click **Next**.

Step 7 In the **Ready to Install the Program** window, click **Install**.

Step 8 After installation, click **Finish**.

Step 9 Unmount the ISO image.

Configure SNMP Traps

Simple Network Management Protocol (SNMP) traps may be raised from Unified CCDM by configuring Windows to send selected events to an SNMP monitor. Configure Windows using a Windows utility called evntwin.exe. This utility converts events written to the Windows Event log into SNMP traps that are raised and forwarded by the Windows SNMP service to an SNMP management tool.

To configure SNMP traps for use with Unified CCDM, follow these steps:

- Enable Windows SNMP Feature, on page 12
- Configure SNMP Service for Trap Forwarding, on page 13
- Configure Windows Events to Forward to SNMP, on page 13

Enable Windows SNMP Feature

Enabling the SNMP feature in Windows is required to configure the Windows event forwarding to SNMP. In the Unified CCDM servers, enable the SNMP feature as follows:

Procedure

Step 1 Select **Server Manager** > **Manage** > **Add Roles and Features**.

Step 2 On the **Before you begin** page, click **Next**.

Step 3 On the **Select Installation Type** page, select the **Role-based or feature-based installation** option, then click **Next**.

Step 4 On the **Select destination server** page, select the **Select a server from the server pool** option, then click **Next**.

Step 5 On the **Select server roles** page, click **Next** .

Step 6 On the **Select features** page, check the **SNMP Service** . Check the **SNMP WMI Provider** check box, then click **Next**.

Step 7 Click **Install** to complete the SNMP deployment.

Step 8 Close the **Server Manager** application.

Configure SNMP Service for Trap Forwarding

Configure the SNMP service to forward traps to the management tool, which is used to report and alert.

Procedure

Step 1 In the MMC console, select **Files > Add/Remove Snap-in...**

Step 2 From the **Available Snap-ins** list, select **Services** and click **Add**.

Step 3 In the **Services** dialog box, select **Local computer** and click **Finish**.

Step 4 Click **OK**.
The **Services(Local)** node will be added to the **Console Root** node.

Step 5 Select **Services(Local)** and in the **Services(Local)** tab that is displayed, right-click **SNMP Services** and then select **Properties**.
The **SNMP Service Properties** dialog box is displayed.

Step 6 In the **Traps** tab, in the **Community Name** field, enter **`public`**, then click **Add to list**.

Step 7 Click **Add**.

Step 8 In the **SNMP Service Configuration** dialog box, enter the hostname or IP address of the system, which receives the trap information—The server hosting the management agents or reporting and alerting tools. Click **Add** to add the trap destination.

Step 9 If there is more than one system, it is required to receive the trap information, configure SNMP services for the trap forwarding on all systems.

Step 10 Click **OK**.

Configure Windows Events to Forward to SNMP

Finally, use the `evntwin.exe` tool to configure the Windows events to be forwarded as SNMP traps. Any event that is raised in the Windows Event Log may be configured to generate an SNMP trap.

Procedure

Step 1 In the **Run** command, enter **`evntwin.exe`**.

Step 2 Select **Custom**, then click **Edit**.

Step 3 In the **Event Sources** list, expand the **Application** source to see the available Unified CCDM events. The Unified CCDM events and their uses are listed in the following table.

Event Source	Description
Unified CCDM Application Server Monitoring	The core monitoring service for the application server—This posts connection change events to the event log.
Unified CCDM Data Import Server Monitoring	The data import service used for importing data from CCE etc.
Unified CCDM Partition Table Manager Monitoring	Connection monitoring for the partition manager service, which creates partitioning tables in the database.
Unified CCDM Provisioning Server Monitoring	Service used for provisioning changes on remote equipment, for example, CCE etc.
Unified CCDM Partition Table Manager	Core application service to create partitioning tables in the database.
X_ANALYTICALDATA, X_HIERARCHY, X_IMPORTER etc.	Individual services configured in Windows for Unified CCDM—These can be used for subscribing to standard service events. For example, start/stop events etc.

Step 4 Configure an event source for generating SNMP traps, select the event source, wait a few moments, then click **Add** once it is enabled. In the **Properties** window, specify the required trap properties, then click **OK**.

Step 5 After setting the required SNMP traps, click **Apply**.

Deploy Unified CCDM Database Server

Follow the procedure to install the Unified CCDM database server on side A and side B.

Before you begin

Download the OVA files. Use `UCCE_12.5_Win2016_vmv13_v1.0` to deploy the Unified CCDM Database server.

Create a naming convention for the Unified CCDM Web server, as the hostname of the Unified CCDM Web server is required to install and configure the Unified CCDM Database server.

Note Do not use hyphens in the server name.

Procedure

Step 1 Create Virtual Machine for the Unified CCDM Database server.

Step 2 Install Microsoft Windows server.

Step 3 Configure Windows.

Step 4 Associate Unified CCDM component servers with the service provider AD domain.

Step 5 Configure secondary drive.

Step 6 Install Microsoft SQL server.

Step 7 Configure Distributed Transaction Coordinator (DTC).

Step 8 Configure Windows Server Firewall for SQL Server.

Step 9 Install SQL Server Management Studio.

Step 10 Install the Unified CCDM Database server.

Note Before installing the Unified CCDM Database server on side B, install the Unified CCDM Web server on side A.

Step 11 Add SQL sign-in for the Unified CCDM Web server.

Step 12 Install the Unified CCDM Portal Database.

Step 13 Install the diagnostic framework for the system CLI.

Step 14 Configure SNMP traps.

Note
- Back up the SQL Server databases regularly and truncate the transaction logs to prevent them from becoming excessively large.
- Schedule backups when there is no user activity.

Related Topics

Create Virtual Machines, on page 58
Configure Windows , on page 9
Associate Unified CCDM Component Servers with Service Provider AD Domain, on page 11
Configure Secondary Drive, on page 11
Install Microsoft SQL Server, on page 63
Configure DTC, on page 16
Install Microsoft Windows Server, on page 59
Install Unified CCDM Database Server, on page 16
Add SQL Login for Unified CCDM Web Server, on page 19
Install Unified CCDM Portal Database, on page 17
Install the Diagnostic Framework for System CLI , on page 12
Configure SNMP Traps, on page 12

Procedures for Deploying Unified CCDM Data Server

Configure DTC

Procedure

Step 1 Open the **Component Services** application.

Step 2 Expand **Component Services** > **Computers** > **My Computer** > **Distributed Transaction Coordinator**.

Step 3 Right click **Local DTC** and select **Properties**.

Step 4 Select the **Security** tab.

Step 5 In the **Security** tab, configure:

a) Ensure that **Security Settings** has **Network DTC Access** checked, and **Transaction Manager Communication** has **Allow Inbound** and **Allow Outbound** checked.

b) Set the **Transaction Manager Communication** to **No Authentication Required**.

c) Click **OK**.

Configure Windows Server Firewall for SQL Server

Procedure

Step 1 Open the **Server Manager** application.

Step 2 Select **Tools** > **Windows Firewall with Advanced Security** and click **Inbound Rules**.

Step 3 In the **Actions** pane, click **New Rule**.

Step 4 Select **Port** as the rule type and click **Next**.

Step 5 Select **TCP** as the protocol and enter `1433` as the specific local ports, then **Next**.

Step 6 Select `Allow the connection`. Click **Next**.

Step 7 Select the profile options that are appropriate to your deployment and click **Next**.

Step 8 Enter a name for the rule and click **Finish** to create the rule.

Install Unified CCDM Database Server

Procedure

Step 1 Mount the Unified CCDM ISO image to the virtual machine.

Step 2 Double-click the ISO image.

Step 3 In the **Cisco Unified CCDM Installation** window, from the **Server Installation** list, select the **Database server** component.
System runs the prerequisite check.

Step 4 Ensure all the prerequisites are checked. After the prerequisite check, click **Install**.

Step 5 In the **Domain Manager: Database Components - InstallShield wizard** window, click **Next**.

Step 6 Accept the license agreement, then click **Next**.

Step 7 In the **Cryptography Configuration** window, enter and confirm the passphrase using 6 to 35 characters, then click **Next**.

This passphrase encrypts system passwords and must be identical across all servers within a cluster. Enter the same password in the **Confirm Passphrase** field.

Step 8 In the **Configure Database** window, configure:

a) In the **Catalog** field, enter the name of the Unified CCDM database catalog. The default catalog name is Portal.

b) In the **Authentication** field, select the authentication mode to connect to the Unified CCDM database.

- **Windows Authentication** - This is the default authentication mode.
- **SQL Authentication** - Select this option only if you are using a database server on a different domain. For this option, enter the SQL Server Username and Password.

c) Click **Next**.

Step 9 In the **Destination Folder** window, accept the default location to install the database server, then click **Next**.

Step 10 In the **Ready to Install Program** window, click **Install**.

Step 11 After the installation, uncheck the **Launch Database Management Utility** check box. You can manually set up the database, later.

Step 12 Click **Finish**.

Note Repeat the steps to set up the Unified CCDM Database server on Side B.

Install Unified CCDM Portal Database

Complete the following procedure to set up the database server:

Procedure

Step 1 Open **Database Installer**.

Step 2 On the **Database Setup** page, click **Next**.

Step 3 From the **Database setup** page, select **Install a new database**.

Step 4 Click **Next**.

Step 5 On the **SQL Server Connection Details** page, enter:

a) In the **Server Name** field, enter the name of the Unified CCDM database server. The default server name is Local.

b) From the **Database Name** drop-down list, enter the name of the Unified CCDM database catalog. The default database name is Portal.

c) In the **Authentication** field, select the authentication mode to connect to the Unified CCDM database.

- **Windows Authentication** - This is the default authentication mode.

- **SQL Authentication** - Select this option only if you are using a database server on a different domain. For this option, enter the SQL Server Username and Password.

d) Click **Next**.

Step 6 Click **Test Connection** to ensure the connection is established to the SQL Server, then click **OK**.

Step 7 Click **Next**.

Step 8 In the **Optimize System Databases** window, then click **Next**.

Step 9 For installation of the portal database server on Side B, check the **Replicated Configuration** check box.

a) In the **Setup Replication** window, select **Replicated Configuration** and enter:

- In the **Share Name** field, enter the name. The default share name is **ReplData Folder**.
- In the **Folder Path** field, enter the path. The default path is `C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\repldata`.

b) Click **Next**.

Step 10 In the **Configure the Location of Data Files** window, for non-customized installation of SQL Server, accept the defaults and click **Next**. For the custom installation of SQL Server, configure the data files:

a) Check the file group or file groups check box which you want to change.
b) Browse the file group or file groups location.
c) Enter the size for the selected file group or file groups.

Note Uncheck the **Set Initial Size to Max Size** check box to specify the initial size.

d) Click **Update**.
e) Click **Default** to restore all file groups to default settings.
f) Click **Next**.

Step 11 In the **Configure Local Administrator Details** window. Enter the password and confirm, then click **Next**.

Note You cannot retrieve or reset the password.

Step 12 In the **Configure SQL Server Agent Service Identity** window, configure:

a) In the **Account Type** field, enter the user account type. For a distributed installation, this must be a domain user account.
b) In the **User Name** field, enter the user name. The default username is **sql_agent_user**.
c) Optional, for a single sided single server system, check the **Automatically create the user account if missing** check box to automatically create a local user.
d) Enter and confirm the password.

Ensure that the password meets the system's complexity requirements.

e) Click **Next**.

- **User Name** - Enter the name of the user account. Default value is sql_agent_user. If you selected the Account Type as Domain, enter the domain user account name instead. If you have specified a domain user, you will need to prefix the user name with the domain name, followed by a backslash.
-

Step 13 In the **Configure the Location of the Identity Database Data Files** window, check all the file group check boxes to set the location, then click **Next**.

Step 14 In Ready to Install the database page, Click **Next**.

Step 15 In the Web Application Servers Network Service Configuration window, configure the following:

- **Domain** - The network domain in which the web server is on, for example ACMEDOM.
- **Machine Name** - The name of the machine, for example WEBSERVERA.
- Click **Add** to add each Web Server to the list.
- When all Web Servers have been added, click **Next**.

Step 16 In the **Ready to install the Database** window, click **Next**.

Step 17 Click **Close**.

Step 18 Start the following Unified CCDM services under the Windows services:

- CCDM: Data Import Server
- CCDM: Partition Table Manager
- CCDM: Provisioning Server

Step 19 Repeat the steps to set up database for Unified CCDM Data Server on Side B.

Add SQL Login for Unified CCDM Web Server

In distributed deployment, create SQL logins to establish connection between the Unified CCDM web server and data server.

Procedure

Step 1 Log in to the Cisco Unified CCDM database server using domain administrator credentials.

Step 2 Open the **SQL Server Management Studio** window.

Step 3 Select **Security** > **Logins**.

Step 4 Right-click the **Logins** option and click **New Logins**.

Step 5 To add SQL logins for Side A and Side B Unified CCDM web servers, configure the following settings on the **General** page:

a) In the **Login Name** field, enter the machine name. The default name is **<DOMAIN>\<Unified CCDM-WEB SERVER HOSTNAME>$**.
b) Select the **Windows Authentication** unless you are connecting to a server on another domain.
c) Set the **Default language** to **English**.

Step 6 On the **Server Roles** page, check the **public** and **sysadmin** check boxes.

Step 7 On the **User Mapping** page, configure the settings:

a) From the **Users Mapped to this Login** options, check the **Portal** and **IdSvr3Config** check boxes.
b) From the **Database role membership for Portal** options, check the **portalapp_role**, **portalreporting_role**, **portalrs_role**, and **public** check boxes to grant the portal login credentials.
c) From the **Database role membership for IdSvr3Config** options, check the **db_owner** and **public** check boxes.

Step 8 Click **OK**.

Step 9 Repeat the steps to add SQL login for the Unified CCDM Web Servers for Side B.

Deploy Unified CCDM Web Server

Follow the procedure to install the Unified CCDM Web server on side A and side B.

Before you begin

Download the OVA files. Use `UCCE_12.5_Win2016_vmv13_v1.0` to deploy the Unified CCDM Web server.

Note Do not use hyphens in the server name.

Procedure

Step 1 Create Virtual Machine for the Unified CCDM Web server.

Step 2 Install Microsoft Windows Server.

Step 3 Configure Windows.

Step 4 Associate Unified CCDM component servers to respective service provider AD domain.

Step 5 Configure the secondary drive.

Step 6 Install the Unified CCDM Web server.

Note Before installing Unified CCDM Web server on Side B, install the Unified CCDM Data server on Side B.

Step 7 Install the Unified CCDM Identity server on the Web server.

Note Before installing Unified CCDM Identity Server, install the Unified CCDM Web Server and Data server.

Step 8 Install the diagnostic framework for the system CLI.

Step 9 Configure SNMP traps.

Related Topics

Create Virtual Machines, on page 58
Install Microsoft Windows Server, on page 59
Configure Windows , on page 9
Associate Unified CCDM Component Servers with Service Provider AD Domain, on page 11
Configure Secondary Drive, on page 11
Install Unified CCDM Web Server, on page 21
Install CCDM Identity Server on Web Server, on page 22
Install the Diagnostic Framework for System CLI , on page 12
Configure SNMP Traps, on page 12

Install Unified CCDM Web Server

Complete the following procedure to install the App or Web server component:

Before you begin

Complete the Unified CCDM Data server installation.

Procedure

Step 1 Mount the Unified CCDM ISO image to the virtual machine.

Step 2 Double-click the ISO image.

Step 3 In the **Cisco Unified CCDM Installation** window, select **App/Web Server** and wait until it completes all prerequisite checks, then click **Install**.

Step 4 In the **Domain Manager: Application Server Components - IntsallShield Wizard** window, click **Next**.

Step 5 Accept the license agreement, then click **Next**.

Step 6 In the **Cryptography Configuration** window, enter and confirm the passphrase using 6 to 35 characters, then click **Next**.

This passphrase encrypts system passwords and must be identical across all servers within a cluster. Enter the same password in the **Confirm Passphrase** field.

Step 7 In the **Destination Folder** field, retain the default location, then click **Next**.

Step 8 In the **Configure Database** window:

a) In the **SQLServer Name** field, enter the Side A database server hostname. The default option is valid only for the All-in-One deployment type.

Note When you install the app or web server on Side B, enter the Side B database server hostname.

b) From the **Catalog Name** list, select the name that is used while installing the Database Server component. The default value is Portal.

c) In the **Connect Using** pane, select the appropriate sign-in option:

- **Windows authentication** - This is a default option.
- **SQL Server authentication** - Select this option only if you are using a database catalog on a different domain.

Note For this option, enter the SQL Server Username and Password.

Step 9 In the **Ready to Install the Program** window, click **Install**. When the installation completes, click **Finish**.

Step 10 Click **Yes** to restart your system for the changes to take effect.

Note In a dual-sided Unified CCDM deployment, repeat this installation for side B replication. Before installing side B, complete the side A installation for all the components.

Install CCDM Identity Server on Web Server

Complete the following procedure to install the Identity server on CCDM App or Web Server.

Procedure

Step 1 In the **Cisco Unified CCDM Installation** window, select **Identity Server** and wait for the prerequisite checks, click **Install**.

Step 2 In the **Identity Server setup Wizard** window, click **Next**.

Step 3 Accept the license agreement, then click **Next**.

Step 4 In the **Destination Folder** field, retain the default location for the Identity Server Installation, then click **Next**.

Step 5 Click **Finish**.

Configure Unified CCDM

Unified CCDM cluster configuration is to establish the communications channel between different Unified CCDM components. This configuration helps each Unified CCDM component to connect to the appropriate channels during failure.

Procedure

Step 1 Launch the Integrated Configuration Environment.

Step 2 Set up Unified CCDM Servers.

Step 3 Configure Replication.

Step 4 Obtain Digital Certificates.

Step 5 Log into Unified CCDM.

Related Topics

Obtain Digital Certificate , on page 25
Login to Unified CCDM, on page 28

Procedures for Configuring Unified CCDM

Launch the Integrated Configuration Environment

Complete the following procedure to launch the Integrated Configuration Environment (ICE) in the Unified CCDM data server.

Procedure

Step 1 Open the **Integrated Configuration Environment** application.

Step 2 On the **Database Connection** page, enter:

a) The **Server Name** field default value is **current machine**.
b) In the **Database Name** field, accept the default value (Portal).
c) In the **Authentication** field, accept the default value.

Step 3 Click **Test** to test the connection to the database server for the first time. If the test fails, check the **Database Connection** settings.

Step 4 Click **OK** to open the ICE.

When ICE starts, the Cluster Configuration tool is the default tool. You can use the **Tool** drop-down list in the toolbar to switch to other ICE tools.

Set up Unified CCDM Servers

Complete the following procedure to set up Unified CCDM servers.

Procedure

Step 1 Open the **Integrated Configuration Environment** application.

Step 2 In the **Select Deployment Type** window, select the **Two Tier** option, then click **Next**.

Step 3 In the **Configure Redundancy** window, select **Dual-Sided system**, then click **Next**.

Step 4 For the two-tier deployment, enter the number of web servers for each side. For dual-sided configurations, configure the equal number of app or web servers for each side of the system, then click **Next**.

Step 5 In the **Configure Servers** window, enter:

a) In the **Primary Server** pane, enter the name and IP address of the primary database server.
b) In the **Secondary Server** pane, enter the name and IP address of the secondary database server, then click **Next**.

Step 6 In the **Configure Application Servers (1)** window, enter:

a) In the **Primary Server** pane, enter the name, IP address, and FQDN of the primary web server.
b) In the **Secondary Server** pane, enter the name, IP address, and FQDN of the secondary web server, then click **Next**.

Note Enter the FQDN in lowercase.

Step 7 In the **Configure Database Connection** window, enter:

a) In the **Catalog** field, enter the name of the Unified CCDM Relational database. The default catalog name is Portal.
b) In the **Authentication** field, select the authentication mode to connect to the Unified CCDM relational database.

- **Windows Authentication** - This is the default authentication mode.
- **SQL Authentication** - Select this option only if you are using a database server on a different domain. Enter the SQL Server username and password.

Step 8 Click **Next**.

Step 9 Optional, click **Print** to print the deployment summary.

Step 10 Verify deployment details, then click **Next**.

Displays a confirmation message.

Step 11 Click **Exit**.

Step 12 Click **Save**.

Configure Replication

Procedure

Step 1 Launch the Integrated Configuration Environment for Unified CCDM Database Server.

Step 2 From the **Tool** drop-down list, select **Replication Manager**.

The dual-sided Unified CCDM deployment, Replication Manager helps to replicate SQL Servers between Unified CCDM databases.

Step 3 Set up SQL Server replication for the Unified CCDM databases.

Step 4 Monitor the general health of SQL Server replication between Unified CCDM databases.

Setup

Procedure

Step 1 Click the **Setup** tab to see the replication setup details and configure or disable replication.

Step 2 In the **CCDM Database Server Properties** pane, check the **Identity Database Replication Enabled** check-box.

Step 3 In the **Distributor Properties** pane, retain the default values.

Note The distributor is created on the Unified CCDM Database Subscriber Server.

Step 4 Click **Configure** to start the replication process.

Note After replication, all the options are dimmed except **Disable**.

Monitor

The Monitor option monitors the general health of SQL Server Replication between Unified CCDM databases. The monitor can also start or stop various replication agents. This option shows the agent details only if SQL Server Replication is currently configured.

Procedure

Step 1 Click the **Monitor** tab.

Step 2 After Unified CCDM replication, top-left pane shows a list of **Publishers** and their publications.

Step 3 Select the **Publication** to see **Subscriptions** or **Agents** details.
The **Agents** tab lists **Snapshot Agent**, **Log Reader Agent**, and **Queue Reader Agent** that are available for the selected publication.

Step 4 In the **Sessions in the 24 Hours** pane, you can see the session details of the subscriptions or agents.

Step 5 In the **Actions in selected session** pane, shows the actions during the selected session and also provides the information about the agent's failure.

Note You can start or stop the replication agents, select the **Agents** tab, right-click on the status of the agent and select **Start** or **Stop**.

Configuring SSL for Unified CCDM

Follow these steps, to configure SSL for the Unified CCDM web application:

Sequence	Task
1	Obtain Digital Certificate , on page 25
2	Export the Certificate in PFX Format , on page 27
3	Configure SSL for the Web Application, on page 27

Obtain Digital Certificate

You can obtain a digital certificate in one of the following ways:

- purchase from an external certificate authority, for public use
- generate internally, for secure use within the issuing organization

Note Use a digital certificate with a key length of at least 2048 bits. Some recent browsers may reject certificates with shorted key lengths.

If you do not already have a suitable certificate, you can request or generate one as follows:

1. Open **Internet Information Services (IIS) Manager** and select the web server in the folder hierarchy.
2. Select the **Features View** tab, and in the IIS group, click **Server Certificates**.
3. Create a internal or external digital certificate.

Note The Common Name is the application domain name. Ensure that you enter the Common Name exactly as it is specified. The Common Name is derived as follows:

- For deployments with a registered address (including load-balanced deployments): enter the registered address, starting from www. For example, if your registered address is `https://www.Unified CCDM.com`, enter `www.Unified CCDM.com`.
- For deployments with a single internal address (including load-balanced deployments): enter the part of the address after https://. For example, if your internal address is `https://UnifiedCCDM.intranet.local`, enter `Unified CCDM.intranet.local`
- For deployments where the web servers will be accessed directly with no load-balancing: enter the fully qualified domain name of the server being configured. For example, `webserver1.mydomain.com`.

Related Topics

Request an External Certificate , on page 26
Generate an Internal Certificate, on page 26

Request an External Certificate

Procedure

Step 1 In the **Actions** pane, select **Create Certificate Request** to display the **Request Certificate** dialog box.

Step 2 In the **Common Name** field, enter the application domain name as defined above.

Step 3 Complete the other fields as appropriate, and click **Next**.

Step 4 In the **Cryptographic Service Provider Properties** dialog box leave the default **Cryptographic Service Provider**.

Step 5 Select a bit length of at least 2048. Click **Next**.

Step 6 Specify a file name for the certificate, and then click **Finish**.

Step 7 When you receive the certificate from the certificate authority, repeat step 1 and step 2 above to show the Server Certificates and Action panes, and in the **Action** pane, select **Complete Certificate Request**.

Step 8 Enter the file name of the certificate, and a friendly name of your choice and click **OK**.

Generate an Internal Certificate

Procedure

Step 1 Select **Create Domain Certificate** in the **Actions** pane to display the **Distinguished Name Properties** dialog box.

Step 2 In the **Common Name** field, enter the application domain name as defined above.

Step 3 Complete the other fields as appropriate, and click **Next**.

Step 4 In the **Online Certification Authority** dialog box specify the **Online Authority** and a friendly name.

Step 5 Click **Finish**.

Export the Certificate in PFX Format

Procedure

Step 1 In IIS Manager, select the **Features View** tab, and in the IIS group, click on **Server Certificates**.

Step 2 Select the certificate in the **Actions** pane and click **Export**.

Step 3 In the **Export Certificate** dialog box, do the following:

a) Enter a file name in the **Export to** field or click **Browse** to select the folder in which you want the exported certificate stored.

b) If you want to protect the exported certificate with a password, enter a password in the **Password** field.

c) Click **OK**.

The certificate is exported as a PFX file.

Configure SSL for the Web Application

Procedure

Step 1 In a web browser, navigate to `https://<web-address>/SSLConfig`, where `<web-address>` is the web address of your Unified CCDM deployment.

Example:

For example, if your web address is `https://Unified CCDM.intranet.local`, enter `https://UnifiedCCDM.intranet.local/SSLConfig`.

Step 2 In the **Authentication** dialog box, enter the user name and password of a Windows domain user with administrator rights on the domain.

Step 3 On the **SSL Certificate Configuration** page, click **Choose File** and browse to the PFX file you created in the previous section. Click **Open** to select the file.

Step 4 If the PFX file is password-protected, enter the password in **Password** field. If not, leave **Password** field empty.

Step 5 Click **Upload** to start the SSL configuration.

When the SSL configuration is complete, the following message is shown:

```
SSL Configuration Complete.
```

Login to Unified CCDM

Procedure

Step 1 To access the Unified CCDM portal, enter *https://<webserver FQDN>/Portal* in browser.
This displays the **Unified CCDM** web page.

Step 2 To sign in to a new system, use **`Administrator`**' as the username and enter the password you entered when you installed Unified CCDM.

Related Topics

Procedures for Configuring Unified CCDM, on page 22

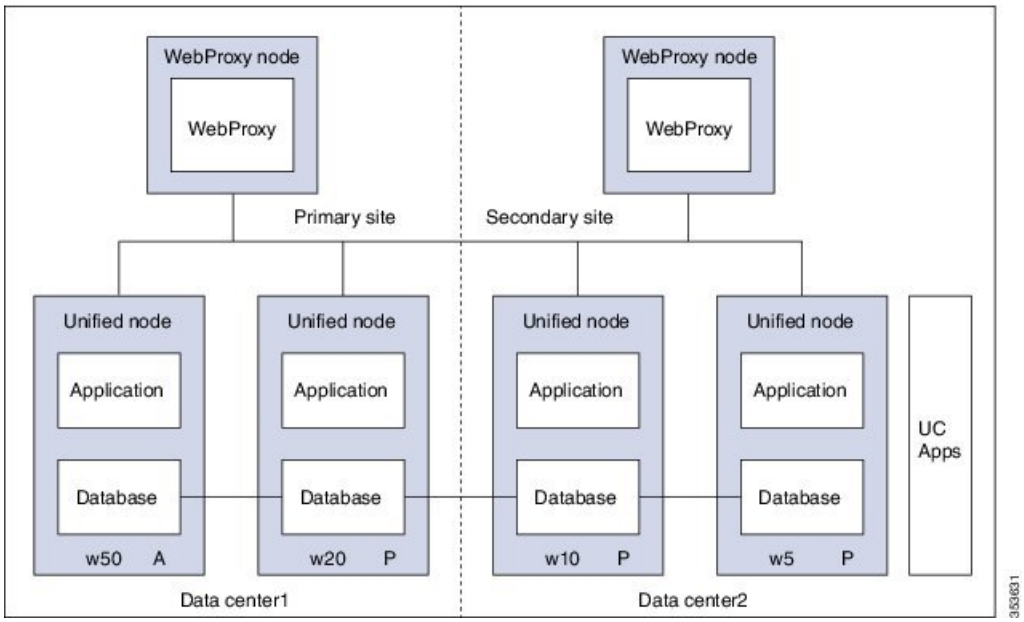
Install and Configure Unified Communication Domain Manager

Cisco HCS for Contact Center, implements the VOS-based—Unified Communication Domain Manager multinode deployment. In this deployment, install four (or more) Unified instances and two (or more) WebProxy instances. These instances are clustered and split over two different geographical locations to provide high availability and disaster recovery.

- A WebProxy role installs only the front-end web server together with an ability to distribute load among multiple middleware nodes.
- A Unified node comprises of application and database roles on a single node.
- WebProxy and Unified nodes can be contained in separate firewalled networks.
- Database synchronization takes places between all database roles, therefore it provides disaster recovery and high availability.
- All nodes in the cluster are active.

Following figure shows the multinode implementation of the Unified Communication Domain Manager:

Figure 2: Graphical Representation of Geo-Redundant Cluster



The functional roles of each node are:

- **WebProxy:** It does load balancing across multiple application roles.
- **Application:** It is a transactional business logic.
- **Database:** It is a persistent data store.

Related Topics

Multinode Installation, on page 29

Multinode Cluster Hardware Specifications

For information about implementing virtual machines within the HCS solution, see Cisco HCS Virtual Machine Requirements.

Multinode Installation

Install a multinode consisting of either four or six Unified instances of and two WebProxy instances.

- A WebProxy node installs only the front-end web server, with the ability to distribute load among multiple middleware nodes.
- A Unified node consists of the Application and Database roles on one node. For geo-redundancy, there are two or four Unified nodes in the Primary Site and two Unified nodes in the Disaster Recovery (DR) Site in active-active setup.

  Cisco Hosted Collaboration Solution supports three configurations of Cisco Unified Communications Domain Manager 10.x+. These configurations provide the service provider with options for scale and Geo-Redundancy support.

Configuration	Number of Unified Nodes	Number of Proxy Nodes	Supported Scale (# Subscribers)	Geo-Redundancy (Y/N)
Standalone CUCDM	1	0	20,000	NA
Multi-Node CUCDM (across Data Centers)	4	2	200,000	Yes (Active-Active)
	6	2	200,000	Yes (Active-Passive)
Multi-Node CUCDM (One Data Center)	4	2	200,000	No

Note

- For geo-redundant Multinode Cluster deployment with six Unified Nodes, there are four Unified nodes in the Primary Site and two Unified nodes in the Disaster Recovery (DR) Site in active-standby setup.
- Installation of the template and upgrade takes approximately two hours. You can follow the progress on the GUI transaction list.

Before you begin

If you received the product on DVD, extract the Unified CDM ISO to get the platform-install ISO and the Unified CDM template file.

If you selected electronic software delivery, use the link that you received to download the product ISO file. Mount the Unified CDM ISO to get the platform-install ISO and the Unified CDM template file.

Optionally, download or extract language pack template files to support languages other than English.

Procedure

Step 1 Install the WebProxy instances.

For each WebProxy instance, create a new VM using the platform-install OVA. Use the instructions shown in Create Virtual Machines from OVA Files, on page 33. For role, select **(3) WebProxy**. Specify the appropriate data center (Primary/DR site) for each WebProxy instance.

Step 2 Install the Unified instances.

For each Unified instance, create a new VM using the platform-install OVA. Use the instructions shown in Create Virtual Machines from OVA Files, on page 33. For role, select **(2) Unified**. Specify the appropriate data center (Primary/DR Site) for each Unified instance.

The following Unified nodes are required in the cluster:

- One Unified node as the Primary node at the Primary site
- One Unified node as the Secondary node at the Primary site

Note For six Unified Node Multi Cluster deployment there are three Unified node as the Secondary node at the Primary site

- Two Unified nodes as the Secondary nodes at the DR site

Step 3 Prepare each node to be added to the cluster. On each WebProxy and Unified node, except for the primary Unified node, run the **cluster prepnode** command.

Step 4 Add nodes to the cluster.

a) Log in to the primary Unified node.
b) Add the Unified and WebProxy nodes to the cluster with the **cluster add <ip_addr>** command.
c) Verify the list of nodes in the cluster with the **cluster list** command.

Step 5 Add the network domain.

a) Configure the domain with the **cluster run all network domain <domain_name>** command.
b) Verify the configured network domain with the **cluster run all network domain** command.
Each node shows the domain that you configured.
c) Verify the DNS configuration with the **cluster run all network dns** command.
Each node responds with the DNS server address.
d) Attempt to contact each node in the cluster with the **cluster run all diag ping <hostname>** command.
e) (Optional) Shut down all the nodes with the **cluster run all system shutdown** command. Take a snapshot of each node. Restart each node.

Step 6 Determine whether security updates are required by running the **cluster run all security check** command on each cluster.

Step 7 If at least one update is required for any cluster, run the **cluster run all security update** command on every cluster.

Step 8 Install VMware tools on each node.

a) In vSphere, right-click the name of the appropriate VM.
b) Select **Guest** > **Install/Upgrade VMware Tools**.

If you are prompted to disconnect the mounted CD-ROM, click **Yes**.

c) Log in to each node and run the **app install vmware** command.

Step 9 Configure the cluster.

a) Provide a weight for each database server with the **database weight add <database_ip> <priority>** command.

Use weights of 40, 30, 20, and 10 for the four Unified nodes and weights of 60, 50, 40, 30, 20, and 10 for the six Unified nodes. The higher the value, the more priority.

For Multinode Cluster deployment with four Unified Nodes in a geo-redundant system containing two data center infrastructures in two physical locations the following weights are used:

- Specify a weight of 40 for the Primary node at the Primary site
- Specify a weight of 30 for the Secondary node at the Primary site
- Specify weights of 20 and 10 for the Secondary nodes at the DR site

For Multinode Cluster deployment with six Unified Nodes in a geo-redundant system containing two data center infrastructures in two physical locations the following weights are used:

- Specify a weight of 60 for the Primary node at the Primary site
- Specify a weight of 50 for the Secondary node at the Primary site
- Specify a weight of 40 for the Secondary node at the Primary site
- Specify a weight of 30 for the Secondary node at the Primary site
- Specify weights of 20 and 10 for the Secondary nodes at the DR site

Note For information on web weight used for Web Proxy node, refer *Cisco Unified Communications Domain Manager Best Practices Guide*.

b) Select a Primary Unified node and set it up as the Primary Unified node with the following command: **cluster provision primary <IP address of primary database node>**.

Allow approximately 2 hours for the operation to complete for two WebProxy and four Unified nodes.

If no primary node exists, you are prompted to select a node to be the primary node.

c) When provisioning is complete, verify the status of the cluster with the **cluster status** command.

If a service is down, run the **cluster run <node_ip> app start** command to restart the service.

d) (Optional) If required, set the web weights configurations (Active-Active, Active-Standby, Standalone). From the primary Unified node, run the required web weight commands for the Web Proxy nodes. See Multi Data Center Deployments in the *Cisco Unified Communications Domain Manager Best Practices Guide* for detailed information.

e) (Optional) If required, enable or disable Self-service or admin web services on the web proxy nodes. This may be required for security purposes.The commands must be run on the relevant web proxy node. It is not advisable to run the commands on a standalone system, but only on a cluster. The commands will automatically reconfigure and restart the nginx process, which results in some downtime. Request URLs to a disabled service will redirect the user to the active service.

- To disable or enable admin or Self-service web services on the web proxy node: use **web service disable <selfservice|admin>** or **web service enable <selfservice|admin>** command.
- To list web services on the web proxy node: use the **web service list** command.

f) (Optional) Shut down all the nodes gracefully, snapshot and restart:

1. From the selected primary Unified node, run **cluster run notme system shutdown**.
2. From the selected primary Unified node, run **system shutdown**.
3. Take a VMWare snapshot of each node and then remove any previous snapshot.
4. Restart each node.

Step 10 Initialize the database and clear all data with the **voss cleardown** command on the primary database node.

Step 11 Import the template.

a) Copy the template file to the primary Unified node with the **scp <template_file> platform@<unified_node_ip_address>:media** command.

b) Log in to the primary Unified node and import the template with the **app template media/<template_file>** command.

The following message appears: `Services have been restarted. Please ignore any other messages to restart services.` The template upgrade automatically restarts necessary applications.

c) When prompted to set the sysadmin password, provide and confirm a password.
d) When prompted to set the hcsadmin password, provide and confirm a password.

Step 12 (For Cisco Unified CDM 10.6(1) only) Install the Macro_Update.template file on secondary Unified nodes.

a) Upload the new Macro_Update.template file to the `media` directory on the Unified CDM server via SFTP.

1. From the VM console, enter **sftp platform@<cucdm10 hostname>**.
2. Enter **cd media**.
3. Enter **put Macro_Update_xx.template**.

b) Enter the following command: **app template media/Macro_Update_xx.template**.
The template installs on each secondary node in less than a minute.

Step 13 (Optional) Install language templates for languages other than English.

a) Copy the language template file to any Unified node with the **scp <language_template_file> platform@<unified_node_ip_address>:./media** command.
b) Log in to the Unified node and install the template with the **app template media/<language_template_file>** command.

Example:

For example, to install French, `app template media/CUCDMLanguagePack_fr-fr.template`.

Create Virtual Machines from OVA Files

You can import the OVA file into VMware vCenter Server. One OVA file is used to deploy all the functional roles. You choose the specific role when the installation wizard is run.

Procedure

Step 1 Sign in to vSphere to access the ESXi Host.
Step 2 Choose **File > Deploy OVF Template**.
Step 3 Choose **Source**, browse to the location of the .ova file, and click **Next**.
Step 4 On the Name and Location page, enter a Name for this server.
Step 5 Choose the resource pool in which to locate the VM.
Step 6 Choose the data store you want to use to deploy the new VM.
Step 7 On the **Disk Format** page, choose **Thick provisioned Eager Zeroed format** for the virtual disk format.

Note In production environments, "thick provisioning" is mandatory. Thick provisioned Lazy Zero is also supported, but Thin provisioned is not supported.

Step 8 On the Network Mapping, choose your network on which this VM will reside.

Step 9 Do not select **Power on after deployment**.

Step 10 On the **Ready to Complete** page, click **Finish** to start the deployment.

Step 11 After the VM is created, verify the memory, CPU, and disk settings against the requirements shown in Multinode Cluster Hardware Specifications, on page 29.

Step 12 Power on the VM.

Step 13 Select the following options in the installation wizard:

Option	Option name	Description
1	IP	The IP address of the server.
2	netmask	The network mask for the server.
3	gateway	The IP address of the network gateway.
4	DNS	The DNS server is optional. Ensure that the DNS server is capable of looking up all hostnames referred to, including NTP server and remote backup locations.
5	NTP	The NTP server is mandatory to ensure that time keeping is accurate and synchronized among nodes in the same cluster.
6	hostname	The hostname, not the fully qualified domain name (FQDN).
7	role	• A WebProxy role installs only the front-end web server together with ability to distribute load among multiple middleware nodes. • An Application node is the main transaction processing engine and includes a web server which can operate by itself, or route transactions from a web node. • A Database node provides persistent storage of data. • A Standalone node consists of the Web, Application, and Database roles on one node. • A Unified node consists of the Web, Application, and Database roles on one node. On installation, the system needs to be clustered with other nodes and the cluster provisioned.
8	data center	The system's geographic location (data center name, city, country that a customer can use to identify the system location). You cannot change this setting once set.
9	platform password	Platform password must be at least eight characters long and must contain both uppercase and lowercase letters and at least one numeric or special character.
13	install	Completes the installation configuration and installs .

When the installation of the OVA is complete, a sign-in prompt for the platform user is displayed.

What to do next

Return to Multinode Installation, on page 29 to complete the overall installation procedure.

Create the HCM-F Device

After you create the HCM-F device, data synchronization begins if there is a network connection and the NBI REST service is running on the HCM-F server.

Before you begin

- Install and configure HCM-F. For more information, see the **Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide**

  .
- Verify that the NBI REST SDR Web Service is running
  1. Sign in to the HCM-F CLI as the user administrator.
  2. Run the **utils service list** command. Verify that the Cisco HCS NBI REST SDR Web Service is running.
  3. If not running, start it with the **utils service start Cisco HCS NBI REST SDR Web Service** command.

Procedure

Step 1 Sign in to as hcsadmin@sys.hcs.

Step 2 Create a new HCM-F instance:

a) Select **Device Management** > **HCM-F** and click **Add**.
b) Enter the HCM-F hostname.
c) Enter the HCM-F administrator Username.
d) Enter the HCM-F administrator Password.
e) Select the HCM-F Version v10_0 from the drop-down list.
f) Click **Save**.

Step 3 If the previous step fails:

- Verify that HCM-F Hostname is correct
- Verify that HCM-F administrator Username and administrator Password are correct
- Verify that HCM-F Version is correct
- Verify that the domain is set correctly using the CLI:
  a. `ssh platform@<cucdm hostname>`
  b. **network domain**

Step 4 After a couple of minutes, verify that the initial synchronization between and HCM-F is successful:

a) Select **Provider Management** > **Advanced** > **SDR Service Provider**.
b) The sync is successful if the default entry, "Service Provider Name", appears.

What to do next

If the initial sync is not working after following the previous steps, verify that the HCM-F REST API is working by browsing to the following: `http://<hcmf_app_node_host>/sdr/rest/<hcmf_version>/entity/ServiceProvider`. This command returns the JSON representation of the predefined service provider instance in the HCM-F Shared Data Repository (SDR). If you get an error, log in as the administrator on the HCM-F app node CLI and verify that the REST service is running:

To display the services, run the command: **utils service list**.

In the output, you see `Cisco HCS NBI REST SDR Web Service[STARTED].`

If this service is not started, start it with the command: **utils service start Cisco HCS NBI REST SDR Web Service**

For data sync failures, try importing the new HCM-F:

1. Select **Device Management** > **HCM-F** and click the HCM-F device.
2. Update the Hostname and click **Save**.
3. Import the new HCM-F:
   a. Select **Device Management** > **Advanced** > **Perform Actions**.
   b. In the Action field, select Import.
   c. In the Device field, select the HCM-F server.
   d. Click **Save** and wait a few minutes.
4. Check the provider under **Provider Management** > **Advanced** > **SDR Service Provider**.

Create a Provider

Note In Cisco Unified CDM 10.6(2) or later, the provider name is set to the current service provider name in HCM-F. You can decouple the provider name in Cisco Unified CDM from the service provider name in HCM-F.

Procedure

Step 1 Log in to as hcsadmin@sys.hcs.

Step 2 Select **Provider Management** > **Providers**.

Step 3 Click **Add**.

Step 4 On the **Service Provider Details** tab, complete the following fields:

Field	Description
Name	The name of the provider. This field is mandatory. **Note** Once you have saved the provider, you cannot change the provider name.

Field	Description
	Note Any spaces in the provider name are converted to underscores in the provider local administrator name and email, if **Create Local Admin** is checked.
Description	A description of the provider.
Domain Name	The domain of the provider. For example, provider.com. Used when creating the default local administrator so the administrator can sign in with an email ID such as ProviderAdmin@provider.com. This field is mandatory.
Create Local Admin	Controls whether a default local administrator is created.
Cloned Admin Role	The HCS default provider role used to create a new role prefixed with the provider name. The created provider role, shown in **Default Admin Role** field, is assigned to the default local administrator. This field appears only if **Create Local Admin** is checked.
Default Admin Role	The created provider role that is assigned to the default local administrator. This field is read only and appears only if **Create Local Admin** is checked.
Default Admin Password	The password to assign to the default local administrator. This mandatory field appears only if **Create Local Admin** is checked.
Repeat Default Admin Password	Confirm the default local administrator password. This mandatory field appears only if **Create Local Admin** is checked.

Step 5 On the **Contact Information** tab, enter address, email, and phone information as appropriate.

Step 6 Click **Save**.

The provider hierarchy node in , the Service Provider name in SDR, and optionally a default provider administrator are created.

Add Reseller

Procedure

Step 1 Login to the Cisco Unified Communications Domain Manager as the Provider admin. Enter provider admin's email address as username, it is case sensitive.

Example:

<provider_name>Admin@<domain_name>.

Step 2 Navigate to **Reseller Management** > **Resellers** from the menu.

Step 3 Click **Add**.

Step 4 Provide necessary details in the following:

a) Enter **Name**.

b) Enter **Description**.
c) Enter **Domain Name**.
d) Check **Create Local Admin** check box.
e) Keep the default values for **Clone Admin role** and **Default Admin Role**.
f) Enter **Default Admin** password and confirm in **Confirm** password text box.

Step 5 Click **Save**.

What to do next

Integrate Unified Communication Domain Manager with the customer instance. For more information, see the *Configuration Guide for Cisco Hosted Collaboration Solution for Contact Center* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/tsd-products-support-series-home.html

Install and Configure Session Border Controller

For complete installation and configuration instructions, see https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

Installing and Configuring Prime Collaboration Assurance and Analytics

To verify the supported version of Prime Collaboration Assurance and Analytics for this release of Cisco HCS, 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.

For complete installation and configuration instructions, see the *Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide* at https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.html.

The *Cisco Prime Collaboration Quick Start Guide* explains all aspects of installing and configuring Prime Collaboration Assurance in Advanced mode (so that you can select the Managed Service Provider deployment):

- Licensing
- Deployment models
- Deploying OVAs
- Configuring OVAs
- Required post installation tasks

Important

- The Prime Collaboration Assurance 12.1 and above MSP mode supports large and very large OVA. See the *Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide* for detailed information.

Log in to Prime Collaboration

Invoke Prime Collaboration Assurance using the client browser.

To log in to the Prime Collaboration application:

Procedure

Step 1 Open a browser session from your machine. Specify the IP address of either Prime Collaboration Assurance application.

Step 2 Enter any one of the following: `http://IP Address` or `https://IP Address`.

Note HTTPS is enabled by default for Prime Collaboration Assurance. Based on the browser you are using, one of the following appears:

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

These windows appear because Prime Collaboration uses a self-signed certificate.

Step 3 Remove the SSL certificate warning. See Removing SSL Certificate Warning at http://docwiki.cisco.com/wiki/troubleshooting_cisco_prime_collaboration

The Prime Collaboration login page appears.

Step 4 In the Prime Collaboration login page, you must log in as a globaladmin, using the same the credentials that you specified during the configuration.

Enabling HCM-F and Prime Collaboration Assurance to Communicate

The HCM-F versions compatible with Prime Collaboration Assurance is specified in the table. Prime Collaboration Assurance 11.6 and above version supports enhanced security.

To install the patch file for Prime Collaboration Assurance and Analytics use the link Download Software.

To install the .cop file on HCM-F use the link https://upload.cisco.com/cgi-bin/swc/fileexg/main.cgi.

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 for details on the supported HCMF .cop file and PCA patch file.

Note

- Different versions of Prime Collaboration Assurance running in the same environment are not supported.
- HCM-F does not support uninstalling of ES files.
- Cisco Hosted Collaboration Solution supports a single HCM-F with one or more PCA for monitoring customer and devices.

Install and Configure ASA Firewall and NAT

Cisco Adaptive Security Appliance (ASA) Firewall partitions a single ASA into multiple virtual devices that keeps customer traffic separate and secure, and also makes configuration easier. All customer traffic is first sent to the firewall before forwarding to the computer resources.

Related Topics

Setup ASA, on page 40
Configure Multiple Context Modes, on page 41

Setup ASA

To initiate the basic setup in Cisco ASA, access the command-line interface and configure the credentials.

Procedure

Step 1 Connect a PC to the console port using console cable. Connect to console using a terminal emulator and set 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control.

Step 2 Press **Enter**.

Displays the following prompt:

```
hostname>
```

This indicates you are in user EXEC mode.

Step 3 Enter the following commands to access privileged EXEC mode:

```
hostname>enable
Password:
hostname#
```

Note Default, password is blank. Press **Enter** key to continue.

Step 4 Enter the following commands to access the global configuration mode:

```
hostname#configure terminal
hostname(config)#
```

Step 5 Enter `hostname` command to configure the hostname:

Example:

```
hostname(config)#hostname CISCOASA
CISCOASA(config)#
```

Step 6 Enter `enable passsword` command to configure the password:

```
CISCOASA(config)#enable password <enter the password>
```

Example:

```
CISCOASA(config)#enable password Password1234
CISCOASA(config)#exit
```

Step 7 Enter the following commands to save configuration:

```
hostname# copy running-config startup-config
```

Configure Multiple Context Modes

Procedure

Step 1 Enable the multiple context modes.

Step 2 Enable the interfaces.

Step 3 Configure the security contexts.

Step 4 Optional, in configure mode, enter `hostname(config)#mac-address auto` command to assign the MAC addresses to the context interfaces automatically.

Step 5 Configure interfaces in the context.

Related Topics

Enable Multiple Context Modes, on page 41
Enable Interfaces, on page 41
Configure Security Contexts, on page 42
Configure Interfaces in the Context, on page 42

Enable Multiple Context Modes

Procedure

Enter the following commands:

```
hostname#changeto system
hostname#configure terminal
hostname(config)#mode multiple
```

Note After you enable the multiple context mode, optionally you can configure the classes for resource management. You need not to create classes for HCS as you can use the default class.

Enable Interfaces

Complete the following procedure to configure interfaces:

Procedure

Step 1 Navigate to interface management 0/0 and enter the following commands:

```
hostname(config)#interface management 0/0
hostname(config-if)#no shut
```

Step 2 Navigate to interface gigabitethernet 0/0 and enter the following commands:

```
hostname(config)#interface gigabitethernet 0/0
hostname(config-if)#no shut
```

Configure Security Contexts

Complete the following procedure to configure security contexts:

Procedure

Step 1 Configure the admin context name in the global configuration mode:

```
hostname(config)#admin-context admin
```

Step 2 Navigate to the context admin:

```
hostname(config)#context admin
```

Step 3 Configure the admin context definitions:

```
hostname(config-ctx)#description admin Context for admin purposes
```

a) Allocate interface management 0/0 for admin context.

```
hostname(config-ctx)#allocate-interface management0/0 invisible
```

b) Create `admin.cfg` in disk 0.

```
hostname(config-ctx)#config-url disk0:/admin.cfg
```

Configure Interfaces in the Context

Complete the following procedure to configure interfaces in the admin context:

Procedure

Step 1 Navigate to admin context in configure mode:

```
hostname#changeto context admin
```

Step 2 Navigate to the interface management:

```
hostname/admin#configure terminal
hostname/admin(config)#interface management 0/0
```

Step 3 Enter a name for management interface of the admin context:

```
hostname/admin(config-if)#nameif management
```

Enter the IP address of the management interface:

```
hostname/admin(config-if)#ip address ip_address subnet_mask
hostname/admin(config-if)#exit
```

Example:

```
hostname/admin(config-if)#ip address 209.165.200.225 255.255.255.224
```

Step 4 Configure the following in global configuration mode to allow SSH to the admin context:

a) Generate an RSA key pair that is required for SSH. The modulus size value is 1024.

```
hostname/admin(config)#crypto key generate rsa modulus modulus_size
```

b) Save the RSA keys to persistent flash memory.

```
hostname/admin(config)#write memory
```

c) Enables local authentication for SSH access.

```
hostname/admin(config)#aaa authentication ssh console LOCAL
```

d) Create a user in the local database for SSH access.

```
hostname/admin(config)#username abcd password xxxx
```

e) Enter the IP address of the management interface from which the ASA accepts SSH connections.

```
hostname/admin(config)# ssh ip_address subnet_mask management
```

Example:

```
hostname/admin(config)# ssh 209.165.200.225 255.255.255.224 management
```

f) Set the duration to idle SSH session before the ASA disconnects the session.

```
hostname/admin(config)#ssh timeout 5
```

g) Enable HTTPS server and default port is 443.

```
hostname/admin(config)#http server enable
```

h) Enter the same IP address of management interface to access through HTTPS.

```
hostname/admin(config)# http server ip_address subnet_mask
```

i) Enter Default Static Route.

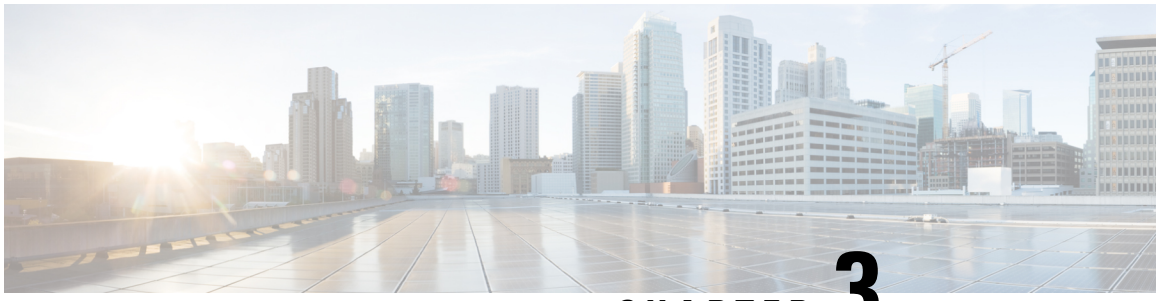
```
hostname/admin(config)# route management 0.0.0.0 0.0.0.0 ip_address
```

Example:

```
hostname/admin(config)#http server 209.165.200.225 255.255.255.224
hostname/admin(config)#route management 0.0.0.0 0.0.0.0 209.165.200.226
```

What to do next

Integrate Cisco ASA with the customer instance. For more information, see the *Configuration Guide for Cisco Hosted Collaboration Solution for Contact Center* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/tsd-products-support-series-home.html



CHAPTER 3

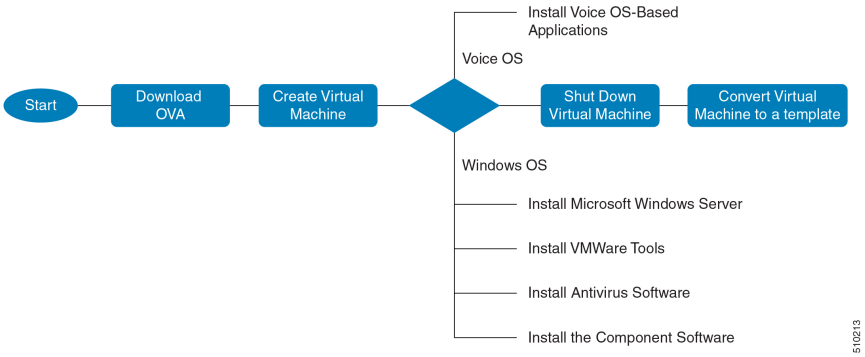
Core Component Installation

- Core Components Installation Approach, on page 45
- Golden Template Requirements, on page 47
- Common Procedures for Golden Templates, on page 57

Core Components Installation Approach

You can use golden templates to clone and deploy contact center core components as virtual machines (VM) on servers.

Figure 3: High-Level Golden Template Workflow



Note If you chose to create virtual machines directly on destination servers, do not convert the virtual machine to a template. For VOS based machines, see *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Core Component Voice Gateway Installation

For instructions on deploying the Cisco CSR 1000v OVA using vSphere, see the Cisco CSR 1000v Series Cloud Services Router Software Configuration Guide at: https://www.cisco.com/c/en/us/td/docs/routers/

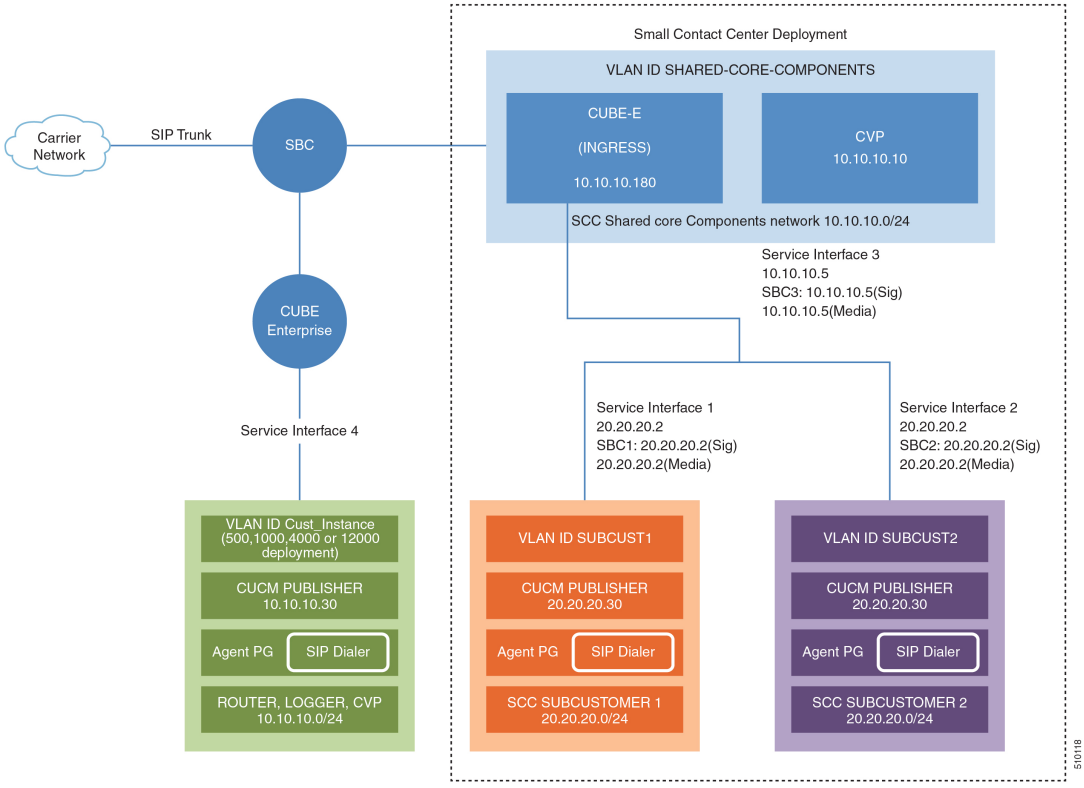
csr1000/software/configuration/b_CSR1000v_Configuration_Guide/b_CSR1000v_Configuration_Guide_chapter_011.html#d41950e959a1635

For information on Integrated Services Routers, see https://www.cisco.com/c/en/us/td/docs/routers/access/4400/release/xe-16-rn/isr4k-rel-notes-xe-16_3.html

Note If the SBC supports CUBE Enterprise with Multi-VRF, you can send calls directly from the SBC to the CVP without a dedicated CUBE Enterprise for the HCS for Contact Center instances. However, using the aggregation SBC without a dedicated CUBE Enterprise affects performance and scalability.

The following figure shows the CUBE Enterprise topology for HCS deployment.

Figure 4: CUBE Enterprise Topology for HCS Deployment Models



Configure Service Interface for Carrier Network

To create the service interface for carrier network, perform the following instructions.

```
interface GigabitEthernet1
ip address 192.168.10.2 255.255.255.0
negotiation auto
```

Configure Codec List

To configure codec list, perform the following instructions.

```
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8
codec preference 3 g729br8
codec preference 5 g711alaw
```

Note For Small Contact Center deployments, you may configure the carrier interface as a VRF.

Golden Template Requirements

Contact center core components vary for each deployment model. The following table provides information about the golden templates for required core components.

Table 1: Golden Templates for HCS for Contact Center Core Components

Golden Templates	2000 Agents	4000 Agents	12000 Agents	24000 Agents	Small Contact Center
Unified CCE Rogger	Yes	Yes	—	—	Yes
Unified CCE Router	—	—	Yes	Yes	—
Unified CCE Logger	—	—	Yes	Yes	—
Unified CCE AW-HDS-DDS	Yes	Yes	—	—	Yes
Unified CCE AW-HDS	—	—	Yes	Yes	—
Unified CCE HDS-DDS	—	—	Yes	Yes	—
Unified CCE Agent PG	—	—	—	—	Yes
Unified CCE VRU PG	—	—	—	—	Yes
Unified CCE PG	Yes	Yes	Yes	Yes	—
Unified CVP Server	Yes	Yes	Yes	Yes	Yes
Unified CVP OAMP Server	Yes	Yes	Yes	Yes	Yes

Golden Templates	2000 Agents	4000 Agents	12000 Agents	24000 Agents	Small Contact Center
Unified CVP Reporting Server	Yes	Yes	Yes	Yes	Yes
Cisco Finesse	Yes	Yes	Yes	Yes	Yes
Cisco Unified Intelligence Center Coresident Deployment	Yes	—	—	—	—
Cisco Unified Intelligence Center	—	Yes	Yes	Yes	Yes
Live Data Reporting System	—	Yes	Yes	Yes	Yes
Cisco Identity Service	—	Yes	Yes	Yes	Yes
Cisco Unified Communications Manager	Yes	Yes	Yes	Yes	Yes

Create Golden Template for Unified CCE Rogger

Before you begin

Download the OVA files. Use `UCCE_12.5_Windows_vmv13_v1.0` to create the golden template.

Note After you deploy OVA for 500 agents deployment (HCS for CC 2000 reference only), edit the settings and change the MHz reservation to 2500.

Procedure

Step 1 Create a virtual machine for Unified CCE Rogger using the OVA.

Step 2 Install Microsoft Windows server.

Step 3 Install an anti-virus software.

Step 4 Install Microsoft SQL server.

Step 5 Install Unified Contact Center Enterprise.

Step 6 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Microsoft Windows Server, on page 59
Install Antivirus Software, on page 61
Install Microsoft SQL Server, on page 63
Install Unified Contact Center Enterprise, on page 125
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Unified CCE Router

Before you begin

Download the OVA files. Use `UCCE_12.5_Windows_vmv13_v1.0` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CCE Router using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install Unified Contact Center Enterprise.
Step 5 Convert the virtual machine to a template.

Related Topics

Create Virtual Machines, on page 58
Install Microsoft Windows Server, on page 59
Install Antivirus Software, on page 61
Install Unified Contact Center Enterprise, on page 125
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Unified CCE Logger

Before you begin

Download the OVA files. Use `UCCE_12.5_Windows_vmv13_v1.0` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CCE Logger using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install Microsoft SQL server.
Step 5 Install Unified Contact Center Enterprise.

Step 6 Convert the virtual machine to a template.

Related Topics

Create Virtual Machines, on page 58
Install Microsoft Windows Server, on page 59
Install Antivirus Software, on page 61
Install Microsoft SQL Server, on page 63
Install Unified Contact Center Enterprise, on page 125
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Unified CCE AW-HDS-DDS

Before you begin

Download the OVA files. Use `UCCE_12.5_Windows_vmv13_v1.0` to create the golden template.

Note After you deploy OVA for 500 agents deployment (HCS for Contact Center 2000 reference only), edit the settings and change the Memory to 8GB and MHz Reservation to 3200.

Procedure

Step 1 Create a virtual machine for Unified CCE AW-HDS-DDS using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install Microsoft SQL server.
Step 5 Install Unified Contact Center Enterprise.
Step 6 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Microsoft Windows Server, on page 59
Install Antivirus Software, on page 61
Install Microsoft SQL Server, on page 63
Install Unified Contact Center Enterprise, on page 125
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Unified CCE AW-HDS

Before you begin

Download the OVA files. Use `UCCE_12.5_Windows_vmv13_v1.0` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CCE AW-HDS using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install Microsoft SQL server.
Step 5 Install Unified Contact Center Enterprise.
Step 6 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Microsoft Windows Server, on page 59
Install Antivirus Software, on page 61
Install Microsoft SQL Server, on page 63
Install Unified Contact Center Enterprise, on page 125
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden template for Unified CCE HDS-DDS

Before you begin

Download the OVA files. Use `UCCE_12.5_Windows_vmv13_v1.0` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CCE HDS-DDS using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install Microsoft SQL server.
Step 5 Install Unified Contact Center Enterprise.
Step 6 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Microsoft Windows Server, on page 59
Install Antivirus Software, on page 61
Install Microsoft SQL Server, on page 63
Install Unified Contact Center Enterprise, on page 125
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Unified CCE PG

Before you begin

Download the OVA files. Use `UCCE_12.5_Windows_vmv13_v1.0` to create the golden template.

Note For 500 agents deployment of the HCS for Contact Center 2000 agent reference, select the **Small PG** OVA.

Procedure

Step 1 Create a virtual machine for Unified CCE PG using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install Unified Contact Center Enterprise.
Step 5 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Microsoft Windows Server, on page 59
Install Antivirus Software, on page 61
Install Unified Contact Center Enterprise, on page 125
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Unified CVP Server

Before you begin

Download the OVA files. Use `UCCE_12.5_Windows_vmv13_v1.0` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CVP Server using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install the Unified CVP Server.
Step 5 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Microsoft Windows Server, on page 59
Install Antivirus Software, on page 61

Install Unified CVP Server, on page 126
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Unified CVP OAMP Server

Before you begin

Download the OVA files. Use `UCCE_12.5_Windows_vmv13_v1.0` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CVP OAMP Server using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install the Unified CVP OAMP server.
Step 5 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Microsoft Windows Server, on page 59
Install Antivirus Software, on page 61
Install Unified CVP OAMP Server, on page 126
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Unified CVP Reporting Server

Before you begin

Download the OVA files. Use `UCCE_12.5_Windows_vmv13_v1.0` to create the golden template.

Procedure

Step 1 Create a virtual machine for Unified CVP Reporting server using the OVA.
Step 2 Install Microsoft Windows server.
Step 3 Install an anti-virus software.
Step 4 Install the Unified CVP Reporting server.
Step 5 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Microsoft Windows Server, on page 59
Install Antivirus Software, on page 61

Install Unified CVP Reporting Server, on page 127
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Cisco Finesse

Before you begin

Download the OVA files. Use `Finesse_12.5.1_VOS12.5.1_vmv13_v1.3` to create the golden template.

Note For Small Contact Center 100 agents dedicated sub-customer deployment and 500 agents deployment (HCS for Contact Center 2000 reference and Small Contact Center 500 agent deployment), select the Finesse **500 agents** OVA.

After you deploy OVA for 500 agents deployment (HCS for Contact Center 2000 reference and Small Contact Center 500 agent deployment) change the vCPU value to 4.

Procedure

Step 1 Create a virtual machine for Cisco Finesse.

Step 2 Install **Cisco Finesse**.

Step 3 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Voice OS-Based Applications, on page 128
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Cisco Unified Intelligence Center Coresident Deployment

Before you begin

Cisco Unified Intelligence Center coresident deployment includes Cisco Unified Intelligence Center, Live Data, and Identity Service components.

Download the OVA files. Use `CUIC_12.5.1_vmv13_v2.15` to create the golden template.

Note After you deploy OVA for 500 agents deployment (HCS for Contact Center 2000 reference only), edit the settings and change the memory to 12 GB.

Procedure

Step 1 Create a virtual machine for Cisco Unified Intelligence Center coresident deployment using the OVA.

Step 2 To install **Cisco Unified Intelligence Center with Live Data and Ids**, follow the installation procedure in the **Install Voice OS based Application** and select **Cisco Unified Intelligence Center with Live Data and Ids** in the **Product Deployment Selection** page .

Step 3 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Voice OS-Based Applications, on page 128
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Cisco Unified Intelligence Center

Before you begin

Download the OVA files. Use `CUIC_12.5.1_vmv13_v2.15` to create the golden template.

Procedure

Step 1 Create a virtual machine for Cisco Unified Intelligence Center using the OVA.

Step 2 To install **Cisco Unified Intelligence Center**, follow the installation procedure in the **Install Voice OS based Application** and select **Cisco Unified Intelligence Center** in the **Product Deployment Selection** page.

Step 3 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Voice OS-Based Applications, on page 128
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Live Data Reporting System

Before you begin

Download the OVA files. Use `UCCELD_12.5_VOS_vmv13_v1.0` to create the golden template.

Note See related links to run the steps.

Procedure

Step 1 Create a virtual machine for Live Data Reporting System using the OVA.

Step 2 Select **Live Data** in the **Product Deployment Selection** page .

Step 3 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Voice OS-Based Applications, on page 128
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Cisco Identity Service

Before you begin

Download the OVA files. Use `IDS_12.5.1_VOS_vmv13_v1.0` to create the golden template.

Procedure

Step 1 Create a virtual machine for Cisco Identity Service using the OVA.

Step 2 To install **Cisco Identity Service (Ids)**, follow the installation procedure in the **Install Voice OS based Application** and select **Cisco Identity Service (Ids)** in the **Product Deployment Selection** page.

Step 3 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Voice OS-Based Applications, on page 128
Convert the Virtual Machine to a Golden Template, on page 67

Create Golden Template for Cisco Unified Communications Manager

Before you begin

Download the OVA files. Use `cucm_11.5_vmv8_v1.1` or `cucm_12.5_vmv13_v1.0` to create the golden template.

Note Select the **2500 agents** OVA for SCC 100 agents dedicated sub-customer deployment and 500 agents deployment (HCS for Contact Center 2000 reference and Small Contact Center 500 agent deployment). After you deploy the OVA edit the settings and change the vCPU value to 2.

Procedure

Step 1 Create a virtual machine for Cisco Unified Communications Manager using the OVA.

Step 2 To install **Cisco Unified Communications Manager**, follow the installation procedure in the **Install Voice OS based Application** and select **Cisco Unified Communications Manager** in the **Product Deployment Selection** page.

Step 3 Convert the virtual machine to a golden template.

Related Topics

Create Virtual Machines, on page 58
Install Voice OS-Based Applications, on page 128
Convert the Virtual Machine to a Golden Template, on page 67

Common Procedures for Golden Templates

Related Topics

Create Golden Template for Unified CCE Rogger, on page 48
Create Golden Template for Unified CCE Router, on page 49
Create Golden Template for Unified CCE Logger, on page 49
Create Golden Template for Unified CCE AW-HDS-DDS, on page 50
Create Golden Template for Unified CCE AW-HDS, on page 50
Create Golden template for Unified CCE HDS-DDS, on page 51
Create Golden Template for Unified CCE PG, on page 52
Create Golden Template for Unified CVP Server, on page 52
Create Golden Template for Unified CVP OAMP Server, on page 53
Create Golden Template for Unified CVP Reporting Server, on page 53
Create Golden Template for Cisco Finesse, on page 54
Create Golden Template for Cisco Unified Intelligence Center Coresident Deployment, on page 54
Create Golden Template for Cisco Unified Intelligence Center, on page 55
Create Golden Template for Cisco Identity Service, on page 56
Create Golden Template for Cisco Unified Communications Manager, on page 56

Download OVA Files

Open Virtualization Format files (OVAs) are required for golden templates. Cisco HCS for Contact Center uses the OVAs that define the basic structure of the corresponding VMs that are created. The structure definition Includes the CPU, RAM, disk space, reservation for CPU, and reservation for memory.

Note The VMs and software components are optimized for Cisco HCS for Contact Center. You must use the OVAs for Cisco HCS for Contact Center.

Before you begin

You must have a valid service contract associated with your Cisco.com profile

Procedure

Step 1 Go to the *Hosted Collaboration Solution for Contact Center* Download Software page on Cisco.com.

Step 2 Select the required software type.

Step 3 Click **Download** and save the OVA file to your local drive. When you create VMs, select the OVA required for the application.

Create Virtual Machines

Procedure

Step 1 Launch the VMware vSphere client and select **File** > **Deploy OVF Template**.

Step 2 Browse to the location on your local drive, where you have stored the OVA. Click **Open** to select the OVA file, click **Next**.

Step 3 On the **OVF Template Details** page, click **Next**.

Step 4 On the **Name and Location** page, in the **Name** field, enter the name of virtual machine, then click **Next**.

Note Enter a maximum of 32 characters; spaces and special characters are not allowed.

Step 5 On the **Deployment Configuration** page, select the appropriate configuration from the drop-down list, click **Next**.

Step 6 On the **Resource Pool** page, select the required resource pool, then click **Next**.

Note Skip this step if you do not have a resource pool allocated in the host server.

Step 7 On the **Storage** page, select a data store you want to deploy in the new virtual machine, then click **Next**.

Step 8 On the **Disk Format** page, select **Thick provisioned Lazy Zeroed**, then click **Next**.

Note Thin provision format is used for the template creation process, it is not supported for production use.

Step 9 On the **Network Mapping** page, select the appropriate network from the **Destination Network** drop-down list, then click **Next**.

Note For Unified Contact Center Enterprise machines, confirm that **Network Mapping** page is correct:

- Public to Visible Network
- Private to Private Network

Step 10 Click **Finish**.

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**.

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 Open the **Network and Sharing Center**, and in the View your basic network info and set up connections section, click **Ethernet**.

Step 12 In the Ethernet Status window, click **Properties**.

Step 13 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**.

Step 14 Navigate to **Control Panel** > **System and Security** > **System**. Follow the instructions:

a) Click**Change Settings**.
b) In Computer name tab, click **Change**.
c) Change the name of the computer from the name randomly generated during Microsoft Windows Server installation. The name does not contain underscores or spaces.

d) Select **Domain** radio button to change the member from Workgroup to Domain.
e) Enter qualified domain name and click **OK**.
f) In the Windows security dialog, validate the domain credentials and click **OK**.
g) On successful authentication, click **OK**.
h) Reboot the server and sign in with domain credentials.

Restart your system for the change to take effect.

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.

Install VMware Tools for Windows

Procedure

Step 1 From the vSphere Client, right-click the virtual machine, select **Power**, and click **Power On**.

Step 2 Click the **Summary** tab.

In the General section, the VMware Tools field indicates whether VMware Tools are:

- installed and current
- installed and not current
- not installed

Step 3 Click the **Console** tab to make sure that the guest operating system starts successfully. Log in if prompted.

Step 4 Right-click the virtual machine, select **Guest OS**, and then click **Install/Upgrade VMware Tools**. The **Install/Upgrade VMware Tools** window appears with the option - Interactive Tools Upgrade and Automatic Tools Upgrade.

a) To install/upgrade the VMware tools manually, select the **Interactive Tools Upgrade** option, and click **OK**. Follow the on-screen instructions to install/upgrade the VMware tools, and restart the virtual machine when prompted.
b) To install/upgrade the VMware tools automatically, select the **Automatic Tools Upgrade** option, and click **OK**. This process takes a few minutes to complete, and restart the virtual machine when prompted.

Install Antivirus Software

Perform this procedure for both golden-template and for direct-install options.

Install any of the antivirus software products supported by HCS for CC for Contact Center.

For more information on the anitvirus software and versions supported by HCS for CC for Contact Center, see *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html.

Install any of the antivirus software products supported by Enterprise Chat and Email. For more information on the anitvirus software and versions supported by Enterprise Chat and Email, see the *System Requirements for Enterprise Chat and Email* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-implementation-design-guides-list.htm.

Important Update antivirus software, manually - do not enable automatic updates.

Tip 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:

- Launch the VirusScan console.
- Right-click **Access Protection**, then select **Properties**.
- In the **Anti-virus Standard Protection** category, make sure that the Prevent IRC communication check box is unchecked in the **Block** column.

Important HCS for CC for Contact Center supports Symantec Endpoint Protection.

Be aware that in the firewall component of Symantec Endpoint Protection 12.1, the Network Threat Protection feature, must be disabled. If it remains enabled, which is the default, both sides of the duplexed router shows up in simplex mode, thus blocking communications between each side of the router. This blocking impacts all deployment types.

If you retain the default (enabled) start services on side A and B of the router, a Symantec message pops up in the system tray indicating: The client will block traffic from IP address [side A router address] for the next 600 seconds(s). This message also appears in the client management security log. The Symantec Network Threat Protection traffic log indicates that a default firewall rule called “Block_all” was dynamically enabled. The result in both sides of the router come up in simplex mode.

To avoid the issue, you must disable the **Symantec** firewall and restart both sides of the router. To do this, double click the Symantec icon in the system tray and select **Change Settings**. Then configure settings for Network Threat Protection and uncheck the **Enable Firewall** check box at the top of the Firewall tab.

Disable Port Blocking

If you have installed Unified CVP Server components on a computer that has antivirus software configured to block ports, exclude Unified CVP processes and Tomcat executable files.

Note Exclude the following folders from on-access scanning configuration of the AV program for all Antivirus scans:

`c:\Cisco`, `c:\Temp`, `c:\tmp`, `c:\db`, `c:\IFMXDATA`

It is the customer's responsibility to deploy the VXML applications after the Antivirus scans. This also applies to the custom `java/jar/class` files deployed in the shared path.

For more information on the Virus Scan guidelines, refer to the following sections of the UCCE documentation:

The Virus Protection section of UCCE Design Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

The General Antivirus Guidelines section of the Security 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

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.

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.

Procedure

Step 1 Mount the Microsoft SQL Server ISO image to the virtual machine. For more information, see Mount ISO Files, on page 59.

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 Backwards Compatibility**
- **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 67.

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.

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**.

What to do next

Note Before installing 12.5(1) ICM on SQL Server 2019, make sure to install ODBC Driver 13 for SQL Server® manually.

Caution Do not change the SQL port number. Retain the default port numbers as 1433 for TCP and 1434 for UDP connections. In case you change the port numbers, the applications like CCEAdmin will not work.

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

Convert the Virtual Machine to a Golden Template

Perform this procedure for the golden-template install option.

Note VMware uses the term *Template*. HCS for Contact Center uses the term *Golden Template* for templates consisting of application and operating systems that are used for HCS for Contact Center.

Before you begin

Ensure that the Windows-based template virtual machine is in the WORKGROUP.

Procedure

Step 1 If the VM is not already powered off, from the **VM** menu, select **Power** > **Shut down the guest**.

Step 2 From the VMware vCenter **Inventory** menu, right-click the virtual machine and choose **Template** > **Convert to Template**.

Verification of the Downloaded ISO

Perform the following procedure to validate the downloaded ISO 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 , ISO Image signature file and the Public key.der file in the same folder for the specific product component.

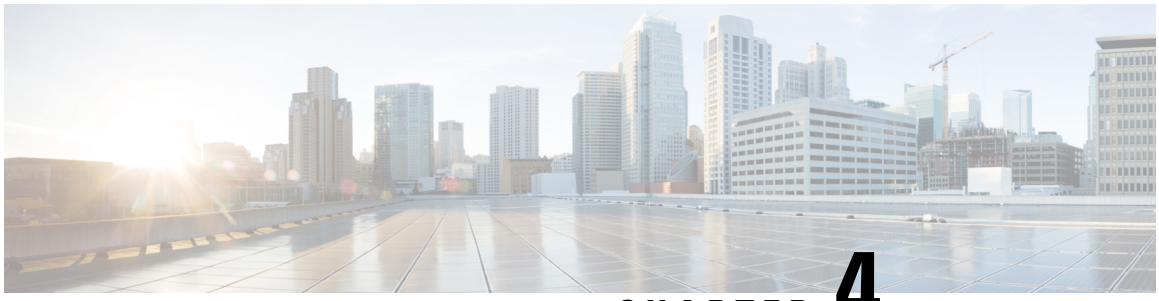
Step 4 Launch **Command Prompt** on the system.

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  <ISO Image
```

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 .



CHAPTER 4

Post-Installation

- Post-Installation Tasks, on page 69

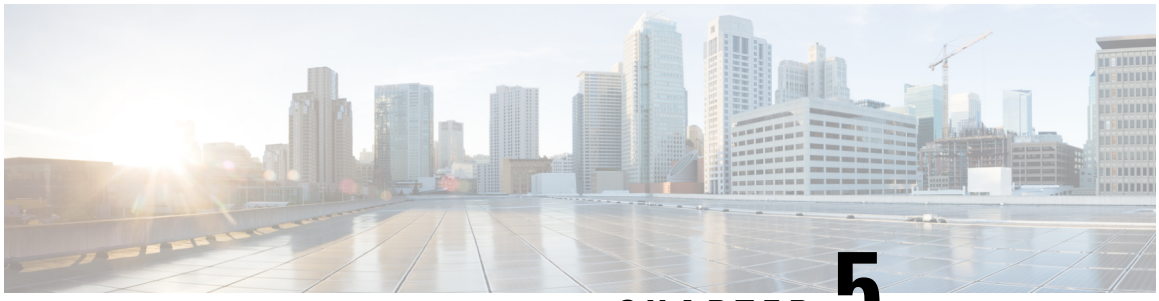
Post-Installation Tasks

After you install the Cisco HCS for Contact Center components, configure the customer instance for each deployment model that you choose. For more details on the customer instance configurations, see *Configure Customer Instance* chapter in *Configuring Guide for Cisco HCS for Contact Center* https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

Before you configure the customer instance, do:

- Clone and OS customization
- Automated cloning and OS customization
- Manual cloning and OS customization

For more information on these steps, see *Configuring Guide for Cisco HCS for Contact Center* https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.



CHAPTER 5

Upgrade

- Overview of the Upgrade Workflow, on page 71
- Upgrading Management Components , on page 72
- Standard CC Upgrade, on page 77

Overview of the Upgrade Workflow

The upgrade process is evaluated by the HCS for CC deployment type you plan to upgrade. Follow the section in the table to plan for your upgrade from 12.0 to 12.5 (x).

Current Deployment Type	Target Deployment Type	Upgrade Process
HCS for CC 500	HCS for CC 2000	Migration CC Upgrade
HCS for CC 1000	HCS for CC 2000	Migration CC Upgrade
HCS for CC 4000	HCS for CC 4000	Standard CC Upgrade
HCS for CC 12000	HCS for CC 12000	Standard CC Upgrade

Note

- All upgrades from 12.0 to 12.5(x) are Standard CC upgrades.
- The Small Contact Center (SCC) deployment uses the HCS for CC 4000 deployment type and follows same upgrade process.

Perform the Cisco HCS for Contact Center upgrade in the same sequence as the upgrade and validation steps are described in this document.

For more information, see *Cisco Hosted Collaboration Solution Documentation*, https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

The following upgrade paths are supported:

Upgrade from 12.0(x) to 12.5(1) is supported in this release. Use EDMT during this upgrade process.

Upgrade from 12.5(1) to 12.5(x) is supported in this release.

Upgrading Management Components

Upgrade HCM-F

Before you begin

Before upgrading a Cisco HCM-F application node, perform the following tasks.

- Create a valid DRF backup of your HCM-F.
- From the command-line interface on the application node, run **show hcs cluster nodes** to verify that the node is at the pre-upgrade version.
- Obtain the upgrade media for upgrading the HCM-F platform: upgrade disk or a downloaded executable file.

Procedure

Step 1 If you downloaded the executable file from Cisco.com, perform one of the following steps.

- Prepare to upgrade from a local folder.
  a. Copy the upgrade file to a temporary folder on a local hard drive.
  b. Open an SFTP client and connect to the HCM-F server using your adminsftp user ID and password.
  c. Run the **cd upgrade** command to navigate to the upgrade folder.
  d. Run the **put [upgrade file name]** command to transfer the file.
- Prepare to load an ISO file.
  a. Copy the upgrade ISO to a data store that is accessible by your virtual machine.
  b. Attach the ISO image to the CD/DVD drive of the virtual machine.
- Put the upgrade file on an FTP or SFTP server that is accessible by the virtual machine that you are upgrading.

Step 2 Copy the contents of the upgrade disk or downloaded files to the virtual machine that you are upgrading. Ensure that the upgrade filename begins with 'HCS.'

Step 3 On the virtual machine that you are upgrading, log in to the HCM-F command-line interface and run the **utils system upgrade initiate** command.

Step 4 Choose the source from which you want to upgrade.

- Remote file system via SFTP
- Remote file system via FTP
- Local DVD/CD

- Local Upload Directory

Step 5 Follow system prompts for the upgrade option you chose.
The system prompts you when the upgrade is complete.

Step 6 If you did not choose to automatically switch versions, run the **utils system switch-version** command. Enter **yes** to reboot the server and switch to the new software version.

Step 7 From the HCM-F command-line interface, run the **show version active** command to verify that the software version is the upgraded version.

Step 8 If you performed step 6, run the **utils service list** command to view services. Then run **utils service start [service name]** to restart any services that were stopped before the upgrade.

Validate the HCM-F Upgrade

Perform the following steps to validate the upgrade of Cisco HCM-F.

Procedure

Step 1 Verify that no error logs were created during or after the upgrade.

Step 2 Run the **show version active** command to verify that the active version is the upgraded version.

Step 3 Run the **utils service list** command to verify that all services are running as they were before the upgrade.

Step 4 Sign in to the administration interface and click the **About** link to verify that the interface displays the upgraded version.

Step 5 Verify that all synchronization is successful for Service Provider, Data Center, vCenter, Customer, and UCS Manager.

Step 6 Verify that Hosted License Manager does not contain post-upgrade errors. Also verify that licenses are assigned to the proper customers.

Step 7 Depending on which you used for the upgrade, ensure that Platform Manager or Prime Collaboration Deployment is running.

Step 8 Verify that Service Inventory is running.

Upgrade UCDM

Procedure

Step 1 Create a backup using the platform command-line interface. You can back up the cluster or back up each node individually.

Step 2 Turn off any scheduled imports.

Step 3 Check for running imports. Either wait for them to complete or cancel them.

Step 4 Upgrade multinode environment. See, *Upgrade a Multinode Environment* section in *Cisco Hosted Collaboration Solution Upgrade and Migration Guide* https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

The *Cisco Unified Communications Domain Manager Planning and Install Guide* also contains installation instructions for multinode environments. You can find the guide on the **Component Documentation** tab here: https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-version-10-6-1/model.html.

Validate the Unified CDM Upgrade

Take the following steps to validate the upgrade of Unified CDM in a multinode or standalone environment.

Procedure

Step 1 Sign in to the user interface as hcsadmin, and click **About** > **Extended Version** to verify the upgrade.

Step 2 Reactivate the scheduled imports that you turned off before upgrading.

Step 3 Use the command-line interface on the primary node to run the **cluster status** command.
The command returns a list of clusters and their status.

Step 4 Attempt to associate a phone with a user:

a) In Unified CDM, navigate to **Subscriber Management** > **Phone** and add a phone.
b) Add a line to the phone.
c) Navigate to **Subscriber Management** > **Agent Line** and identify the new phone as an agent line.
d) In Unified CM, navigate to **User Management** > **Application User** and verify that the new phone is associated with pguser.

Upgrade Prime Collaboration Assurance

Cisco supports the upgrade to Cisco Prime Collaboration Assurance 11.6 or later version.

To upgrade Prime Collaboration Assurance, follow the steps in the "Overview of Data Migration Assistant" topic in the *Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide* : https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.html.

Note For downloading the Prime Collaboration patch, refer to the Dowload Software page. Navigate to **Products > Cloud and System Management > Collaboration and Unified Communications Management > Prime Collaboration**.

Validate the Upgrade of Prime Collaboration Assurance

Take the following steps to validate the upgrade of Prime Collaboration Assurance.

Validation consists of adding a Contact Center customer component and verifying that the component is in Managed state. In this example, we add the Customer Voice Portal component.

Procedure

Step 1 Sign in to HCM-F as an administrator.

Step 2 Add a cluster.

a) Navigate to **Cluster Management** > **Cluster** and click **Add New**.
b) Enter the cluster name.
c) Select the customer associated with the cluster.
d) Select **CC** as the cluster type.
e) Select the cluster application version.
f) In the **Application Monitoring the Cluster** field, select the hostname of the Prime Collaboration Assurance instance.
g) Click **Save**.

Step 3 Add the Customer Voice Portal component.

a) Navigate to **Application Management** > **Cluster Application**.
b) In the General Information section, complete the following steps:
   - Click **Add New**.
   - In the **Application Type** field, select **CVP**.
   - Provide the hostname for the Customer Voice Portal component.
   - Select the appropriate cluster.
   - Click **Save**.
c) In the Credentials section, complete the following steps:
   - Click **Add New**.
   - In the **Credential Type** field, select **SNMP_V2**.
   - Provide the community string for the Customer Voice Portal component.
   - Select the **Read Only** access type.
   - Click **Save**.
   - Click **Add New**.
   - In the **Credential Type** field, select **ADMIN**.
   - Provide the administrator credentials. For Customer Voice Portal, the User ID is wsmadmin. Use the password that is configured for the OAMP web interface.
   - Select the **Read Only** access type.
   - Click **Save**.
d) In the Network Addresses section, complete the following steps:

- Click **Add New**.
- In the **Network Space** field, select **Application Space**.
- Provide the IPv4 address and the hostname.
- Click **Save**.
- Click **Add New**.
- In the **Network Space** field, select **Service Provider Space**.
- Provide the NAT IPv4 address and the hostname.
- Click **Save**.

Step 4 Navigate to the **Current Inventory** (Inventory > Inventory Management) page.
The **State** column shows the Customer Voice Portal as **Managed**.

Upgrade Unified CCDM

To upgrade Cisco Unified Contact Center Domain Manager, follow the installation steps in the *Installation and Configuration Guide for Cisco Unified Contact Center Domain Manager*: https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

Validate the Unified CCDM Upgrade

Take the following steps to verify the upgrade of Unified CCDM.

Verification Task	Success Criteria
Provisioning Tests for Unified CCE	
Log in to the side A web server (portal). Create a Skill Group to test the provisioning from the side A web server. Run this test for each configured Unified CCE instance.	You can successfully create the Skill Group, and it is visible on side A, and on side B if applicable.
Log in to the side A web server (Portal). Create an Agent to test the provisioning from the side A web server. Run this test for each configured Unified CCE instance.	You can successfully create an Agent, and it is visible on side A, and on side B if applicable.
Create a Skill Group on the Administrative Workstation using the Cisco Skill Group Explorer tool. After a few minutes, verify that the Skill Group was imported into Unified CCDM.	The Skill Group is visible on side A, and on side B if applicable.
Replication Tests for Dual-Sided Deployments	
Log in to the side B web server (Portal). Create a Skill Group to test Unified CCE provisioning from the side B web server. Run this test for each configured Unified CCE instance.	You can successfully create the Skill Group, and it is visible on side A.

Verification Task	Success Criteria
Create a Skill Group on the Administrative Workstation using the Cisco Skill Group Explorer tool. After a few minutes, verify that the Skill Group was imported into Unified CCDM.	The Skill Group is visible on side A and on side B.
Log in to the side B web server (Portal). Create an IP phone to test Unified CM provisioning from the side B web server.	The IP phone is visible on side A and on side B.

Standard CC Upgrade

Upgrading Unified Customer Voice Portal Components

Upgrade the Unified Customer Voice Portal

Follow these steps to upgrade Cisco Unified Customer Voice Portal.

Procedure

Step 1 Back up the Unified CVP Operations Console configuration.

Step 2 Install the upgrade software.
For more information, see the "Unified CVP Upgrade" chapter in the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

Validate the Customer Voice Portal Upgrade

Follow these steps to validate the upgrade of Cisco Unified Customer Voice Portal.

Procedure

Step 1 Log in to the Operations Console.

Step 2 Validate the version of each component.

Step 3 Verify that all services are running.

Step 4 Make a test inbound PSTN call to an agent.

Upgrading Gateway Components

Upgrade Gateway Components

Follow the steps to upgrade Cisco Unified Border Element (SP Edition), Cisco Unified Border Element (Enterprise Edition), or a virtual peripheral gateway (vPGW). For more information, see the following topics and guides:

- For upgrading Cisco Unified Border Element Enterprise see *Common Upgrade Tasks* section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
- Upgrade the IOS on the Cisco ASR 1006 for Cisco Unified Border Element (SP Edition), on page 78
- Upgrading the Cisco ASR 1000 Series Router for Cisco Unified Border Element (SP Edition), on page 78
- The *vPGW Documentation* guides on the **Component Documentation** tab: https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-version-10-6-1/model.html

Procedure

Step 1 Back up all the gateways.

Step 2 Use the gateway consoles to back up component configurations.

Step 3 Upgrade the gateways.

Upgrading the Cisco ASR 1000 Series Router for Cisco Unified Border Element (SP Edition)

Cisco Unified Border Element (SP Edition) is used as a demarcation between the Cisco HCS network and an outside network, such as IMS, PSTN, or other SIP network. The ASR 1000 Series router is connected to the aggregation switches at the aggregation layer.

To upgrade this component, follow the procedures in the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*: https://www.cisco.com/c/en/us/support/routers/asr-1000-series-aggregation-services-routers/products-installation-and-configuration-guides-list.html.

When you have a redundant Cisco Unified Border Element (SP Edition) deployed, upgrade the component using the procedures in *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model* : https://www.cisco.com/c/en/us/support/routers/asr-1000-series-aggregation-services-routers/products-installation-and-configuration-guides-list.html.

To upgrade the ROMmon image on a Cisco ASR 1000 Series router, see the *Cisco ASR 1000 Series Routers ROMmon Upgrade Guide*: https://www.cisco.com/c/en/us/support/routers/asr-1000-series-aggregation-services-routers/products-maintenance-guides-list.html.

Upgrade the IOS on the Cisco ASR 1006 for Cisco Unified Border Element (SP Edition)

Use this procedure to upgrade Cisco Unified Border Element (SP Edition) ASR 1006 from version IOS 15.3(3)S to IOS 15.3(3)S4.

Before you begin

1. Ensure Cisco Unified Border Element (SP Edition) is configured for inter-chassis redundancy, with one Cisco ASR 1006 Aggregation Service Router in the Active state and the other in the Standby state.
2. Save the current configuration and download the software image to the boot flash of both of the ASR 1006 devices. It takes about 15 minutes.

Procedure

Step 1 Enter the CLI command **show redundancy application group <RG Group Id>** to determine which Session Border Controller (SBC) is Active. The Primary SBC is the Active chassis and the Secondary SBC is the Standby chassis.

Step 2 Download the new software version to the Primary and Secondary SBCs.

Step 3 On the Secondary SBC, enter the CLI command **boot system bootflash: <new image>** to change the boot variable to point to the new image.

Step 4 On the Primary SBC, perform an SBC sync from configuration mode. Enter the sbc configuration by running the CLI command **sbc <name of SBC>** and then run the CLI command **sync**.

Step 5 On the Secondary SBC, enter the CLI command **write memory** to save the running configuration.

Step 6 On the Primary SBC, enter the CLI command **redundancy > application redundancy > group # > shutdown** to shut down the redundancy group.
The Secondary SBC immediately becomes the Active Cisco Unified Border Element and all active calls are preserved. There is no service outage when the switchover of the Active SBC takes place.

Step 7 On the Primary SBC, change the boot variable to point to new software image and save the running configuration.

Step 8 Reload the Primary chassis for upgrade and wait for this SBC to come up with upgraded version.
It can take 10 to 12 minutes after the box is reloaded before the SBC reinitializes with the upgraded version.

Step 9 On the Secondary SBC, shut down the redundancy and immediately run the CLI command **no shutdown** of the redundancy group on the Primary SBC. Keep the duration between shutting down the redundancy group in the Secondary SBC and the **no shutdown** command in the Primary box as minimal as possible.
This step causes a service outage of approximately 4 minutes. The Primary box becomes the Active Cisco Unified Border Element (SP Edition) with upgraded software and starts servicing the calls.

Step 10 Save the running configuration in the Primary SBC.

Step 11 Reload the Secondary chassis for upgrade. When prompted to save the configuration before proceeding with the reload, enter “No” so that after the upgrade the Secondary SBC comes up in Standby mode.

Validate the Upgrade of Gateway Components

This section describes the steps to verify the upgrade of Cisco Unified Border Element (SP Edition), Metaswitch Perimeta Session Border Controller, Cisco Unified Border Element (Enterprise Edition), or a virtual peripheral gateway (vPGW).

Procedure

Step 1 Use Telnet or SSH to access the gateways and verify the version you upgraded to.

Step 2 Make an inbound call to an agent and verify the prompts. You can run the **debug voip dial peer** command to ensure that the inbound call uses the correct dial peer.

Upgrading the Unified Component

Upgrading the Unified Component

Follow the steps to upgrade the Cisco Unified Contact Center Enterprise Central Controller.

Unless otherwise indicated, the following steps reference topics in 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.

Procedure

Step 1 Upgrade the Administration and Data server that is connected to Side A.
For more information, see the "Migrate HDS Database and Upgrade the Unified CCE Administration & Data Server" topic.

Step 2 Perform the Database Performance Enhancement.

For more information, see the **Database Performance Enhancement** section in 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.

Step 3 Bring the Side A logger and call router into service.
For more information, see the "Bring Upgraded Side A into Service" topic.

Step 4 Upgrade Cisco Unified Intelligence Center reporting templates.
For more information, 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.

Step 5 Upgrade the Unified CCE Administration Client.
For more information, see the "Upgrade Unified CCE Administration Client" topic.

Step 6 Upgrade the gateways.
For more information, see the "Upgrade Peripheral Gateways" section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Step 7 Upgrade the Outbound Option Dialer.
For more information, see the "Upgrade Outbound Option Dialer" section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Step 8 Upgrade the CTI server.
For more information, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html

What to do next

To establish secure connection between a client and a server, use one of the following security certificates:

- CA certificates
- Self-signed certificates

For more information, see *Certificates for CCE Web Administration* section in the *Cisco Hosted Collaboration Solution for Contact Center Configuration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-and-configuration-guides-list.html.

Upgrading Reporting Components

Upgrade Cisco Unified Intelligence Center

To upgrade Cisco Unified Intelligence Center, see the *Installation and Upgrade Guide for Cisco Unified Intelligence Center*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html.

Validate the Upgrade of Unified Intelligence Center

Take the following steps to validate the upgrade of Cisco Unified Intelligence Center.

Procedure

Step 1 Open the Unified OS Administration web page at the following URL, where [server-name] is the hostname or IP address of the node: `https://[server-name]/cmplatform`.

Step 2 Sign in with administrator credentials.

Step 3 Navigate to **Settings** > **Version** and verify the software version on the active and inactive partitions.

Upgrading Desktop Components

Upgrade Finesse

To upgrade Cisco Finesse, see the *Cisco Finesse Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html.

Note ES42 provides the ability to connect a maximum of two versions of Finesse to the same PG during the upgrade or migration process to facilitate the migration of agentsand supervisors to the new Finesse version. However, this mode of operation isnot supported for production use beyond the upgrade or migration phase.

Validate the Finesse Upgrade

Take the following steps to validate the upgrade of Cisco Finesse.

Procedure

Step 1 Ensure that the version of Finesse is the version you upgraded to. From the command line interface, you can run the **show status** command to verify the version.

Step 2 In the Finesse console, verify that all services are up.

Step 3 Log in to an agent and run desktop-initiated tests such as Call Hold, Transfer, and Conference.

Upgrade Desktop Clients

(Optional). To upgrade CTI OS Agent and Supervisor desktops, see the *CTI OS System Manager Guide for Cisco Unified ICM/Contact Center Enterprise*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Validate the Upgrade of Desktop Clients

Take the following steps to validate the upgrade of CTI OS Agent and Supervisor desktops.

Procedure

Step 1 Validate the version of each desktop.

Step 2 Sign in to an agent and run desktop-initiated tests such as Call Hold, Transfer, and Conference.

Upgrading Call-Processing Components

Upgrading Cisco Virtualized Voice Browser Components

Upgrade Cisco Virtualized Voice Browser

To upgrade the Cisco Virtualized Voice Browser, follow the steps in the "Cisco Virtualized Voice Browser Upgrade" chapter in the *Installation and Upgrade Guide for Cisco Virtualized Voice Browser Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-installation-guides-list.html

Validate the Cisco Virtualized Voice Browser Upgrade

Follow these steps to validate the upgrade of Cisco Virtualized Voice Browser portal.

Procedure

Step 1 Log into Cisco Virtualized Voice Browser portal.

Step 2 Check the existing configuration.

Upgrade Cisco Unified Communications Manager

Take the following steps to upgrade Cisco Unified Communications Manager.

Procedure

Step 1 Upgrade Cisco Unified CM.
For more information, see the *Upgrade Guide for Cisco Unified Communications Manager*: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Step 2 Uninstall and then reinstall the JTAPI client on the Cisco Unified CM peripheral gateway.
For more information, see the "Upgrade Cisco JTAPI Client on the Unified Communications Manager PG" topic in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

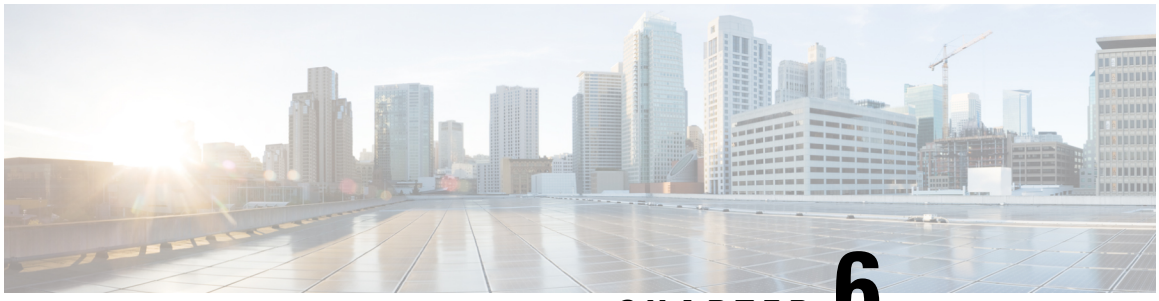
Validate the Upgrade of Cisco Unified Communications Manager

Take the following steps to validate the upgrade of Cisco Unified Communications Manager.

Procedure

Step 1 In Cisco Unified CDM, add an IP phone. For more information, see the *Cisco Hosted Collaboration Solution End-User Provisioning Guide*: https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html.

Step 2 In Cisco Unified CM, verify that the phone was added.



CHAPTER 6

Uninstallation

- Uninstallation of Unified ICM/CCE base version 12.5(1), on page 85
- Uninstall Unified CCE Maintenance Release 12.5(2), on page 85

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.

Uninstall Unified CCE Maintenance Release 12.5(2)

This is a procedure to uninstall Unified CCE Maintenance Release 12.5(2)

Procedure

Step 1 Log in to your system as a user with administrative privileges.

Step 2 Choose **Control Panel** > **Programs and Features** > **Cisco ICM Maintenance Release ICM 12.5(2)** > **Uninstall**.
The InstallShield Wizard launches.

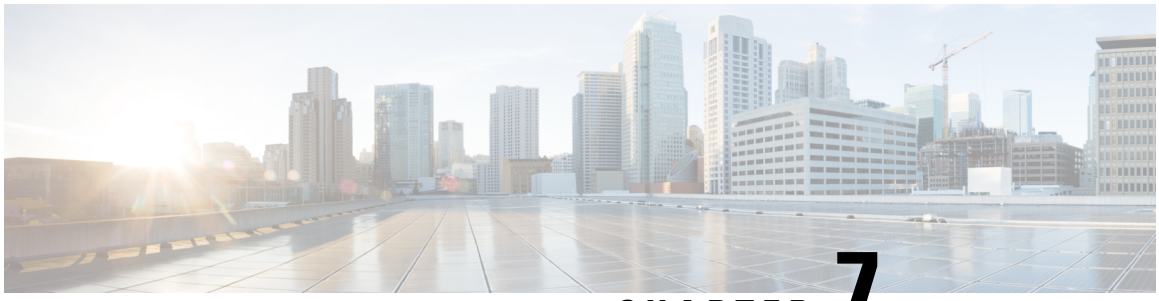
Step 3 On the confirmation window, click **Yes**.

Step 4 (Optional) On the **Installation Messages** window, click **Next**.

Post installation window specifies if any service is set to manual then a pop-up window displays a notification that some services were automatically changed to manual as part of the uninstallation. Make sure that both A and B sides of your system operate properly after uninstalling Unified CCE Release 12.5(2). Then, set the ICM services that were changed during the uninstallation back to their original setting (Automatic).

Step 5 At the prompt, restart the machine.

The Unified CCE Maintenance Release 12.5(2) application is uninstalled from your machine.



CHAPTER 7

CCE Orchestration

Note Orchestration is not supported for 12000, 24000 and 36000 agent deployment models. HCS-SCC (Small Contact Center) deployment model is currently not supported for Orchestration. Each tenant is required to have its own controller node for orchestration.

- Overview, on page 87
- Orchestration in CCE Deployment, on page 88
- Configure SSH public key on Windows nodes, on page 120
- Self-Signed Certificate, on page 121
- Things to Know, on page 122

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.

System Requirements

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

Note Cloud Connect 12.6(1) requires the latest ES i.e., **cloudconnect.1261.ES04.23.cop.sgn** or above on both the publisher and subscriber nodes of Cloud Connect server. You must apply this ES before initiating any orchestration commands.

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 initiating 12.5(2) or 12.6(1) upgrade on VOS nodes from Orchestration, install the Mandatory ES **ucos.keymanagement.v01.cop.sgn** from Orchestration on target 12.5(1) VOS nodes.

Windows Component Upgrade

Unified ICM 12.5(1)	Install mandatory ES66 or Unified ICM 12.5(2) manually	Unified ICM 12.5(1) nodes onboarded with manual install of ES66 will get an option for upgrade to or rollback from Unified CCE 12.5(2) and 12.6(1)
Unified CVP 12.5(1)	Install mandatory ES23 manually	

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)

Note

- Unified CCE 12.5(1) to Unified CCE 12.5(2) software upgrade is supported in orchestration.
- Unified CCE 12.5(2) to Unified CCE 12.6(1) upgrade is not supported either manually or via orchestration.

See System Requirements, on page 88 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.

Orchestration Deployment Task Flow

CLI to configure artifactory URL and API key, on page 93
Generate the Artifactory API Key, on page 91
CLI to configure proxy for orchestration, on page 92
Onboard VOS Nodes to Orchestration Control Node, on page 98
Onboard Windows nodes to orchestration control node, on page 99
Add Deployment Type and Deployment Name, on page 100
Validate Onboarded Nodes for Orchestration, on page 101
Configure Email Notification, on page 101
Configure Windows Server for Updates (Optional), on page 103

Administration Task Flow

Check Installed Software Version and Patches, on page 104
Install or Rollback Patch for Cloud Connect Server, on page 104
List Available Patches for Specific Node or Group of Nodes, on page 105
Install Patch to Specific Node or Group of Nodes, on page 105
Roll Back Patch from Specific Node or Group of Nodes, on page 106
Install Windows Updates to Specific Node or Group of Nodes, on page 107
Roll Back Windows Update from Specific Node or Group of Nodes, on page 108
Enable or Disable Compatibility Enforcement, on page 108
List Available Upgrade Options , on page 109
Upgrade a Specific Node or Group of Nodes or All Nodes , on page 109
Perform Switch Forward on Specific VOS Node or Group of Nodes , on page 111

Roll Back Upgrade from Specific Node or Group of Nodes, on page 112
Check Last Known Orchestration Operation Status on Remote Node, on page 113
Check Status, on page 113
Start Unified ICM Services, on page 114

Maintenance Task Flow

Update VOS Nodes Onboarded to Orchestration Control Node, on page 114
Remove VOS Nodes from Orchestration Control Node, on page 115
Update Windows Nodes Onboarded to Orchestration Control Node, on page 115
Validate Updated Nodes Onboarded for Orchestration, on page 115
Configure Email Configuration, on page 115
Delete Configuration for Email Notification, on page 116
Unsubscribe Email Notification, on page 117
Export and Import of Nodes Managed by Orchestration Control Node, on page 117
Export Current Patch Level Details, on page 118
Serviceability, on page 119
Enable and View Windows Open SSH Logs, on page 120

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 2: 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 3: 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 4: 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. **Note** Cloud Connect 12.6(1) requires the latest ES i.e., **cloudconnect.1261.ES04.23.cop.sgn** or above on both the publisher and subscriber nodes of Cloud Connect server to retrieve the product name and corresponding MDFID of the product in 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 Cisco Technical Assistance Center

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. Restart the Cloud Connect server to enforce the cleanup and download the restricted vs unrestricted software. Download starts 10 minutes after restart.

Note On the successful configuration of artifactory details, artifacts are downloaded locally to the Cloud Connect server at the configured 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, then the Cloud Connect server can be restarted and the download starts 10 minutes after restart. Usage of orchestration-related CLI is blocked during download, and this duration depends on the number of artifacts to be downloaded.

Table 5: 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 121.

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 120.

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 117.

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.

Field	Description
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 117.

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 117.

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
  - HCS-CC-2000-Agents
  - HCS-CC-4000-Agents

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 117.

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 102
2	Validate Email Configuration, on page 103
3	Subscribe to Email Notification, on page 103
4	Configure Email Notification, on page 101

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 for Cloud Connect Server

To install a patch or to roll back a previously installed patch on Cloud Connect server , run the **utils system upgrade initiate** command. The **Local Repository** option in this command lists the patches available from Cisco artifactory for patch install or rollback on Cloud Connect server. This command can be run separately on the Cloud Connect publisher and subscriber nodes.

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 .

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 . The patches available for patch install or rollback are listed from Cisco artifactory.
Expected Inputs	Select the **Local Repository** option to list the patches available for patch install or rollback . Select the patch to install or roll back .
Expected Outcome	The selected patch for install or rollback is installed on 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 93 for configuring Cisco artifactory.

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

Note Patch install or roll back 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.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 113.

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.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 113.

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.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.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.

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) or 12.0(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 111.

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.
- All nodes upgrade to 12.5(2) is not supported.
- All nodes upgrade from 12.5(2) to 12.6(1) is not supported.

Note You can check the status of upgrade which is currently in-progress. For more information, see Check Status, on page 113.

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 113.

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 113.

Check Status

To check the current status of patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forward, , 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 . 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-forward for each node. If there is no patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forward, then you see the status of the previous upgrade, rollback.

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, 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

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 99.

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 101.

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 100.

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):

- Ansible logs by selecting 'Ansible Controller' as the service

- Audit logs by selecting 'Orchestration Audit' as the 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 or MR patch before performing this procedure. See System Requirements, on page 88 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**.

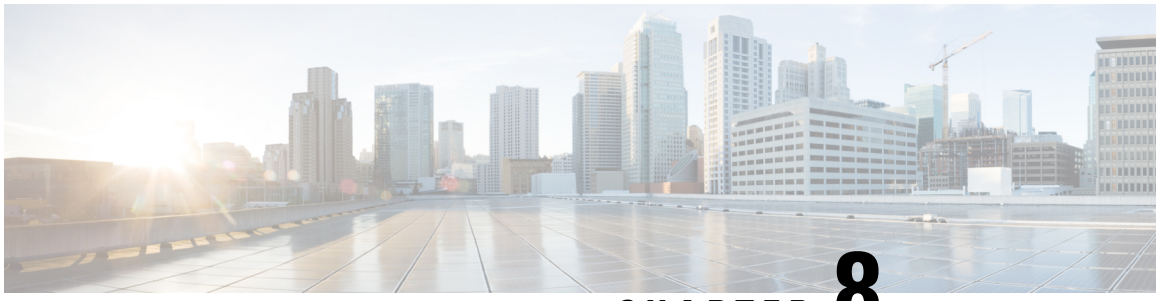
Step 7 Restart the specific VOS node by running the **utils system restart** command.

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.



CHAPTER 8

Appendix

- Core Components Server, on page 125

Core Components Server

Install Unified Contact Center Enterprise

Procedure

Step 1	Add the virtual machine template into the domain.
Step 2	Mount the Unified Contact Center Enterprise ISO image to the virtual machine.
Step 3	From the `ICM-CCE-CCH` Installer directory, run `setup.exe` and follow the InstallShield procedures.
Step 4	In the **Select the installation method** window, select **Fresh Install**, then click **Next**.
Step 5	In the **Maintenance Release (MR)** window, keep the **Maintenance Release Location** field blank, then click **Next**.
Step 6	In the **Installation Location** window, select the drive `C`, then click **Next**.
Step 7	In the **Ready to Copy Files** window, click **Install**.
Step 8	In the **Installation Complete** window, click **Yes, I want to restart my computer now**, then click **Finish**.
Step 9	Apply the Unified Contact Center Enterprise maintenance release, if applicable.
Step 10	Unmount the Unified Contact Center Enterprise ISO image.
Step 11	Move the virtual machine template back to the workgroup.

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.

Related Topics

Create Virtual Machines, on page 58
Mount ISO File
Create Golden Template for Unified CCE Rogger, on page 48
Create Golden Template for Unified CCE Router, on page 49

Create Golden Template for Unified CCE Logger, on page 49
Create Golden Template for Unified CCE AW-HDS-DDS, on page 50
Create Golden Template for Unified CCE AW-HDS, on page 50
Create Golden template for Unified CCE HDS-DDS, on page 51
Create Golden Template for Unified CCE PG, on page 52

Install Unified CVP Server

Procedure

Step 1 Mount the Unified CVP ISO image to the virtual machine.

Step 2 Copy the current Engineering Specials (ES) to the local drive.

Note Ignore this step if there are no Engineering Specials.

Step 3 From the `CVP\Installer_Windows` directory, run `setup.exe`.

Step 4 In the **Install Shield Wizard** window:

a) Accept the license agreement and click **Next**.
b) In the **Select Packages** window, select **CVP Server**, then click **Next**.
c) In the **Choose Destination Location** window, select the folder locations for the CVP Installation Folder and the Media Files Installation Folder, then click **Next**.
d) In the **X.509 Certificate** window, enter the information that you want to include in the certificate.
e) In the **Ready to Install the Program** window, click **Install**.
f) Click **Yes, I want to restart my computer now**, Click **Finish**.

Step 5 Copy the required **Cisco Unified CVP Engineering Special** file to the desktop.

Step 6 If Unified CVP Engineering Specials are available, follow the Install Shield wizard. Ignore this step if there are no Engineering Specials.

Step 7 Add any custom media files to the appropriate location.

Step 8 Unmount the ISO image.

Related Topics

Mount ISO File
Create Golden Template for Unified CVP Server, on page 52

Install Unified CVP OAMP Server

Procedure

Step 1 Mount the Unified CVP ISO image to the virtual machine.

Step 2 From the `CVP\Installer_Windows` directory, run `setup.exe`.

Step 3 Accept the license agreement, click **Next**.

Step 4 In the **Select Packages** window, select the **Operations Console** option, then click **Next**.

Step 5 On the **Choose Destination Location** window, accept the default locations, then click **Next**.

Step 6 In the **X.509 certificate** window, enter the information that you want to include in the certificate, then click **Next**.

Step 7 In the **Ready to Install** window, click **Install**.

Step 8 Enter the operations console password that meets the criteria detailed on the **Operations Console Password** window, then click **Next**.

Step 9 Click **Yes, I want to restart my computer**, then click **Finish**.

Step 10 Unmount the Unified CVP ISO image.

Related Topics

Mount ISO File

Create Golden Template for Unified CVP OAMP Server, on page 53

Install Unified CVP Reporting Server

Procedure

Step 1 Mount the Unified CVP ISO image to the virtual machine.

Step 2 Copy the current Engineering Specials (ES) to the local drive.

Note Ignore this step if there are no Engineering Specials.

Step 3 From the `CVP\Installer_Windows` directory, run `setup.exe`.

Step 4 In the **Install Shield Wizard** window:

a) Accept the license agreement, then click **Next**.

b) In the **Select Packages** window, select **Reporting Server**, then click **Next**.

c) In the **Choose Destination Location** window, select the folder location for the CVP Installation Folder, then click **Next**.

d) In the **X.509 certificate** window, enter the information that you want to include in the certificate, then click **Next**.

e) In the **Choose the Database data and backups drive** window, enter the name of the drive (typically E), and click **Next**.

f) In the **Database size selection** window, select **Standard (250GB)** or **Premium (375GB)**, then click **Next**.

Note Select **Standard** for 500 agent deployment and **Premium** for other HCS agent deployments.

g) In the **Ready to Install** window, click **Install**.

h) Enter the CVP Reporting Server password when prompted.

It can take some time for the database to install.

i) Restart the server after installation.

Step 5 Copy the required CVP Engineering Special file to the desktop.

Step 6 If Unified CVP Engineering Specials are available, follow the Install Shield wizard to install them. Ignore this step if there are no Engineering Specials.

Step 7 Unmount the ISO image.

Related Topics

Mount ISO File
Create Golden Template for Unified CVP Reporting Server, on page 53

Install Voice OS-Based Applications

Use the following procedures to install Voice OS-basedapplications:

- Cisco Virtualized Voice Browser

Procedure

Step 1 Mount the ISO file to the virtual machine and switch on.

Step 2 Follow the Install wizard:

a) On the **Disk found** page, click **OK** to check the media before installation.
b) Click **OK**.
c) On the **Product Deployment Selection** page, select the required product and click **OK**.
d) On the **Proceed with Install** page, click **Yes**.
e) On the **Platform Installation Wizard** page, select the **Skip** option.

After installation, displays the **Pre-existing Configuration Information** page.

f) Press **Ctrl+Alt** to free your cursor.

Step 3 Shut down the virtual machine.

Step 4 Unmount the ISO image.

Related Topics

Mount ISO File
Create Golden Template for Cisco Finesse, on page 54
Create Golden Template for Cisco Unified Intelligence Center, on page 55
Create Golden Template for Cisco Unified Intelligence Center Coresident Deployment, on page 54
Create Golden Template for Live Data Reporting System, on page 55
Create Golden Template for Cisco Identity Service, on page 56
Create Golden Template for Cisco Unified Communications Manager, on page 56

Install Publishers/Primary Nodes of VOS-Based Contact Center Applications

Before you begin

DNS Configuration is mandatory for installation of 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 your product is any one of the following, choose the product and click **OK**.

- Cisco Unified Communications Manager
- Cisco Finesse
- Cisco Virtualized Voice Browser

If your product is Cisco Unified Intelligence Center, you can choose from one of the following options:

- Cisco Unified Intelligence Center
- Live Data
- Cisco Identity Service (IdS)
- Cisco Unified Intelligence Center with Live Data and IdS
- For the 2000 agent reference design, choose the coresident deployment option **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.
- For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center** , **Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

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**.

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**.

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**.

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**.
s) In the **Security Configuration** screen, enter the security password and select **OK**.
t) In the **SMTP Host Configuration** screen, select **No**.
u) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
v) 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.

Related Topics

Create Virtual Machines, on page 58
Mount ISO File

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 Finesse, Cisco Unified Communications Manager, and Cisco Unified Intelligence Center.

Before you begin

DNS Configuration is mandatory for installation of 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.

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 your product is any one of the following, choose the product and click **OK**.

- Cisco Unified Communications Manager
- Cisco Finesse
- Cisco Virtualized Voice Browser

If your product is Cisco Unified Intelligence Center, you can choose from one of the following options:

- Cisco Unified Intelligence Center
- Live Data
- Cisco Identity Service (IdS)
- Cisco Unified Intelligence Center with Live Data and IdS
- For the 2000 agent reference design, choose the coresident deployment option **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.
- For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center** , **Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

Step 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**.
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**.
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.
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**.
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.

Related Topics

Create Virtual Machines, on page 58
Mount ISO File

INDEX

A

antivirus software 61
automation 2
    zip file 2

C

collation 63

G

golden templates 67
    converting from virtual machines 67

I

install 59, 61, 63
    antivirus software 61
    Microsoft SQL Server 63
    Microsoft Windows Server 59
ISO files 59
    mount and unmount 59
ISO files *(continued)*
    mounting 59

M

Microsoft SQL Server 63
    install 63
Microsoft Windows Server 59
    install 59

P

PowerCLI 2

V

virtual machines 67
    convert to golden templates 67

W

WinImage 2