Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide Release 11.6(1)

First Published: 2017-08-24

Last Modified: 2018-05-28

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

CONTENTS

Preface

Change History

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

Change	See	Date
Added RAID configuration for C240 M5SX servers	Configure RAID for C240 M5SX, on page 9	June 2018
Added support for C240 M5SX servers.	Initialize the Packaged CCE 2000 Agents Deployment Type, on page 71	June 2018
Added spec-based hardware support	Initialize the Packaged CCE 2000 Agents Deployment Type, on page 71	November 2017

Change	See	Date
Initial Release of Document for Release 11.6(1)		August 2017
Added new chapter for Packaged CCE 11.5 to 11.6 Upgrade.	Packaged CCE 11.5 to 11.6 Upgrade, on page 209	
Added information for no support of IP address change.	Initialize the Packaged CCE 2000 Agents Deployment Type, on page 71	
Added a new section for VMware settings for Unified Communications Manager.	Update VMware Settings for Cisco Unified Communications Manager, on page 188	
Added a new section for setting users as system administrators under the Install Microsoft SQL Server section.	Set Users as System Administrators, on page 53	
Added information on integration of single Unified CM cluster to a single Packaged CCE deployment.	Initialize the Packaged CCE 2000 Agents Deployment Type, on page 71 Validate Packaged CCE Deployment and Build System Inventory, on page 204	
Added information on B200 M4 and the C240 M4 servers support for on-box installation for ECE.	Solution Components , on page 1 Install and Configure Enterprise Chat and Email, on page 133	
Updated the link for the Enterprise Chat and Email Installation Guide (for Packaged Contact Center Enterprise)	Install and Configure Enterprise Chat and Email, on page 133	

About This Guide

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

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

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

Audience

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

Related Documents

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

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

Field Alerts and Field Notices

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

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

Documentation Feedback

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

contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Conventions

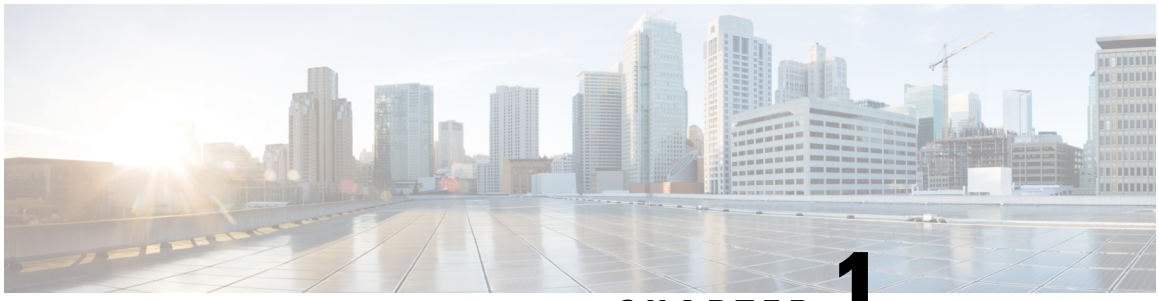
This document uses the following conventions:

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

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

PART I

Preparation



CHAPTER 1

System Requirements

Note By default, Windows Defender is enabled on Windows Server 2016. For more information on Windows Defender antivirus compatibility, see https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/windows-defender-antivirus-compatibility.

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.

Solution Components

Cisco Packaged CCE components are:

The Cisco Unified CCE Rogger functions as the call router and makes all routing decisions. The Unified CCE Rogger also functions as the logger.

The Cisco Unified CCE PG contains the Peripheral Gateways (PG) that connect to Unified Communications Manager, the Media Routing (MR) peripherals, and the Voice Response Unit (VRU). The VRU in this case is a Cisco Unified Customer Voice Portal (CVP).

The Cisco Unified CCE AW-HDS-DDS stores contact center configuration data and reporting data.

The Cisco Unified Communications Manager Server functions as the call processing component. The Publisher stores the read-write database. Devices such as phones and gateways register to the Subscribers.

The Cisco Unified Customer Voice Portal (CVP) Server provides prompting, queuing, and call control. The Unified CVP Server combines the Call Server, Media Server, and VXML server functionality. This guide refers to the server as the Unified CVP Server.

The Cisco Unified CVP Operations Console (CVP OAMP) Server functions as the administrative and management component of the Unified CVP cluster.

The Cisco Unified CVP Reporting Server collects information from Unified CVP components and makes that information available to Cisco Unified Intelligence Center.

Cisco Unified Intelligence Center is a web-based reporting application that generates real-time and historical reports for Unified Contact Center Enterprise and Cisco Unified CVP. Unified Intelligence Center includes the Live Data VOS services. Live Data is a stream processing system that aggregates and processes the events in-stream and publishes the information. Unified Intelligence Center subscribes to the message stream to receive real time data and continuously update the Live Data reports.

The Unified Intelligence Center installation includes Cisco Identity Service (Cisco IdS) on the same VM. Cisco IdS is used to generate authentication and authorization requests for Single Sign-On.

Cisco Finesse is a browser-based agent and supervisor desktop.

Enterprise Chat and Email is an optional application that provides chat and email functionality to the contact center.

The VMs for these applications must be on the Side A and Side B servers as indicated in the following table.

SIDE A Required VMs	SIDE B Required VMs
Unified CCE Rogger	Unified CCE Rogger
Unified CCE PG	Unified CCE PG
Unified CCE AW-HDS-DDS	Unified CCE AW-HDS-DDS
Unified CVP Server	Unified CVP Server
Unified CVP OAMP Server	—
Unified Intelligence Center Publisher (with Live Data and Cisco IdS)	Unified Intelligence Center Subscriber (with Live Data and Cisco IdS)
Finesse Primary	Finesse Secondary

Unified Communications Manager Publisher and Subscribers must be part of the deployment. They can be VMs on Side A and Side B, or they can be configured as external machines.

The Unified CVP Reporting Server and Enterprise Chat and Email (ECE) Data server VMs are optional.

ECE Data Server can be installed as a VM on Side B or configured as an external machine.

Note On-box installation for ECE is supported only on the B200 M4, C240 M4 and the C240 M5 servers.

SIDE A Other VMs	SIDE B Other VMs
Unified Communications Manager Publisher	Unified Communications Manager Subscriber 2
Unified Communications Manager Subscriber 1	Unified CVP Reporting Server (optional)
—	Enterprise Chat and Email (optional)

Platform Requirements

Server selection for Packaged CCE in a virtualized environment involves several factors, including:

- The server and all related hardware must be supported for use in a virtualized Packaged CCE system
- Minimum specifications for processing, memory, and storage
- Whether you want a packaged and tested Cisco configuration (Tested Reference Configuration or TRC) or a configuration that you base on Cisco-defined minimum requirements (Specs-based Configuration)
- Compatibility requirements for all hardware, and Cisco and third-party software including the VMware required to run and manage a virtual environment

Confirm that your hardware selection is supported for Packaged CCE and meets all minimum specifications:

Server	VMware required	For detailed requirements information, see
UCS B- or C-series (TRC):	• VMware vSphere ESXi • VMware vCenter (Optional)	*Virtualization for Cisco Packaged CCE* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html
UCS B- or C-series (Specs-based):	• VMware vCenter • VMware vSphere ESXi	
Third-party (Specs-based)	• VMware vCenter • VMware vSphere ESXi	

In addition to confirming that your servers meet minimum specifications, confirm that your server choice is compatible with all Cisco and third-party software.

Note You cannot have any additional VMs on the Packaged CCE VMware hosted on Tested Reference Configuration (TRC), even if you are using an external Unified Communications Manager cluster.

VMware Hosting and Hardware Support

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

Software Compatibility

See the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for version compatibility information for the following:

- Cisco Systems Contact Center required and optional components
- Endpoints for agents and callers
- Cisco gateway hardware and software
- Third-party software

Software Licenses

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

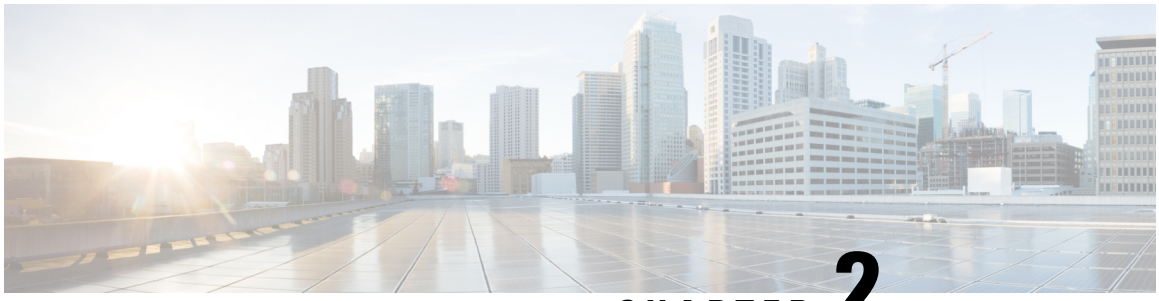
Components	License requirements
Cisco Packaged Contact Center Enterprise	One server license for each of the voice applications. One agent license for each concurrent user with different feature tiers.
Cisco Unified Communications Manager	One license for each Cisco Unified Communications Manager node, plus device licenses for connected devices.
Cisco Unified Customer Voice Portal (CVP)	One CVP software license with CVP Call server ports for each server that runs Call Server and VXML Server software ports for each server that runs CVP VXML server. One CVP reporting license for each Reporting Server. No license required for Operations Console. Redundant port licenses required for each redundant port. One license for each developer machine running Call Studio.
Cisco Unified Intelligence Center	One license for each server.
Cisco Finesse	Cisco Finesse: User licenses included with selected tiers of Cisco Unified Contact Center Enterprise user licenses. One license for each server pair. One license for each Media Kit.
Cisco SocialMiner	User license included with Packaged CCE Agent License. One server license for each SocialMiner server.

Third-Party Products

Note For detailed information about the software editions and versions supported for this release, see the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html.

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

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



CHAPTER 2

Prepare Customer Site Servers

Prepare Customer Site Servers

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

Prepare Cisco UCS C-Series Customer Site Servers

Configure RAID for the C240 M3S TRC#1

For each array created using this procedure, use the following settings:

- Stripe size: 128KB
- Read Policy: Read Ahead Always
- Write Policy: Write Back with BBU

Procedure

Step 1 Power on the UCS server, making sure that Quiet Boot is disabled in BIOS.

Step 2 Press **Ctrl-H** during the initial startup sequence to enter the MegaRAID BIOS configuration utility.

Step 3 Click **Start**.

Step 4 Select **Configuration Wizard** on the left panel. Click **New Configuration**. Then click **Next**.

Step 5 At the prompt to clear the configuration, click **Yes**.

Step 6 Select **Manual Configuration**. Then click **Next**.

Step 7 On the next screen, in the left panel, add the first eight drives to create Drive Group0 as follows:

a) Select drives 1 - 8.
b) Click **Add to Array**.
c) Click **Accept DG**.

Step 8 Add the remaining eight drives to create Drive Group1 as follows:

a) On the left panel, select drives 9 - 16.
b) Click **Add to Array**.
c) Click **Accept DG**.
d) Click **Next** to accept the Drive Group.

Step 9 Add Drive Group0 to a span as follows:

a) Select **Drive Group0**.
b) Click **Add to Span**.
c) Click **Next**.

Step 10 Configure RAID for Drive Group0 as follows:

a) For RAID Level, select **RAID 5**.
b) For Stripe Size, select **128KB**.
c) For Read Policy, select **read ahead = always**.
d) For Write Policy, select **write back with bbu**.
e) Click **Update Size** to finalize the RAID volume and to determine the size of the resulting volume. It resolves to 1.903TB
f) Click **Accept** to accept the virtual drive definition, VD0.
g) Click **Next**.
h) Click **Back** to add the second RAID 5 array.

Step 11 Click **Back** to add the second RAID 5 array as follows:

a) Select **Drive Group1**.
b) Click **Add to Span**.
c) Click **Next**.

Step 12 At the **RAID Selection** screen:

a) For RAID Level, select **RAID 5**.
b) For Stripe Size, select **128KB**.
c) For Read Policy, select **read ahead = always**.
d) For Write Policy, select **write back with bbu**.
e) Click **Update Size**. The size resolves to 1.903TB.
f) Click **Accept** to accept the virtual drive definition, VD1.

Step 13 Click **Yes** at the BBU warning screen.

Step 14 Click **Next** at the Virtual Live Definition screen to indicate that you have finished defining virtual drives.

Step 15 Click **Accept** at the Configuration Preview screen to accept the RAID configuration.

Step 16 Click **Yes** to save the configuration.

Step 17 Click **Yes** to start drive configuration.

Step 18 Click **Home** to exit the Wizard when both drives report their status as Optimal.

Step 19 Click **Exit**.

After RAID configuration is complete on the drives, the system may try to initialize (format) the new RAID array. In this event, the current initialization progress can be seen from the **Web BIOS** screen. Wait for the

background initialization to complete before proceeding with any of the subsequent server configuration steps such as installing ESXi.

You can check background initialization progress on either the **Web BIOS Home** screen or **Virtual Drives** screen.

Configure RAID for C240 M4SX

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

Procedure

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

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

For more information regarding RAID configuration for C240 M4SX in Configure RAID with GUI (UCS C-Series M4 Servers) section, see *Cisco Collaboration on Virtual Servers* Guide at: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/virtual/CHCS_BK_C7C7ED05_00_cisco-collaboration-on-virtual-servers/CHCS_BK_C7C7ED05_00_cisco-collaboration-on-virtual-servers_chapter_01.html#CUCM_TK_C2DC4F2D_00.

Configure RAID for C240 M5SX

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

Procedure

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

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

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

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/virtual/chcs_b_cisco-collaboration-on-virtual-servers.html

Install VMware vSphere ESXi

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

For Packaged CCE, you must install the ESXi on the first drive as the default boot drive for the server. Packaged CCE has no unique requirements.

Add the Datastores to the Host Server

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

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

Add the Customer ESXi Host to the vCenter

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

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

Run the RAID Config Validator Utility

After you set up RAID configuration and add the datastores, run the RAID Config Validator utility to ensure that your datastore configuration is correct.

Before you begin

To run the utility, Java 7 (any update) must be installed. Java 8 and later releases are not supported.

Procedure

Step 1 Download the Packaged CCE RAID Config Validator utility from the **Packaged CCE Download Software** > **Deployment Scripts page** at https://software.cisco.com/download/type.html?mdfid=284360381&i=rm. Extract the zip file locally.

Step 2 Open the Windows command prompt and change to the directory where you downloaded the file.

Step 3 Enter this command to run the tool: **java -jar PackagedCCEraidConfigValidator-<version>.jar <IP Address of the Side A ESXi host> <username> <password>**

For example:

```
C:\Users\Administrator\Desktop>java -jar PackagedCCEraidConfigValidator-11.0.jar xx.xx.xxx.xxx
 userName password
```

Messages appear on the monitor to show that the validation is starting. You then see an indication of a valid or invalid configuration.

Step 4 If your configuration is valid, repeat step 2. Enter the IP address of the Side B server instead of the Side A server.

What to do next

If the utility reports an invalid configuration, you must recreate the RAID configuration. To do this, reset the RAID configuration, re-install ESXi, and then re-run the RAID Config Validator utility to re-validate the configuration.

RAID configuration errors include:

- Non-supported server found or used.
- Incorrect number of datastores found.
- Incorrect sizes set for the datastores.

Prepare Cisco UCS B-Series Customer Site Servers

Before you complete the configuration steps in this section, the customer site UCS B-Series must be installed, configured, and operational.

For additional information and guidance on UCS B-Series installation and configuration, refer to the UCS B-Series documentation (https://www.cisco.com/c/en/us/products/servers-unified-computing/product-listing.html) or your Cisco Data Center Unified Computing Authorized Technology Provider.

This section includes only specific configuration requirements for Packaged CCE deployments on the UCS B-Series platform. Customers may have varying design and configuration needs due to their data center requirements and infrastructure. However, all configurations must meet the Packaged CCE requirements for high availability. For example, the design must not create the potential for a single point of failure, which can adversely impact the operation of Cisco call processing applications.

UCS B-Series may have a variable number of LUNs on the SAN provisioned to meet Packaged CCE IOPS requirements.

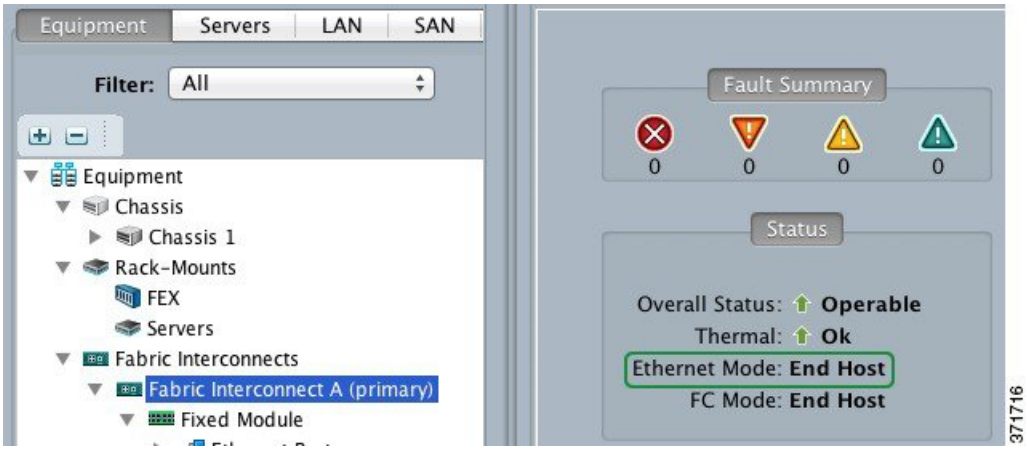
See the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html for IOPs requirements.

Note All UCS hardware configuration examples in this section use the Cisco UCS Manager GUI. You can also use the UCS Manager CLI or API.

Fabric Interconnect Requirements

Ethernet Mode

The Fabric Interconnects' Ethernet Mode must be set to End Host.



Ethernet Uplinks

Cisco UCS Fabric Interconnect Ethernet uplinks (Uplink Ports) for Packaged CCE are required to be 10G, with each Fabric Interconnect cross-connected to two common-L2 data center switches. The uplinks can be in a single-link, Port-Channel (EtherChannel), vPC or VSS (MEC) uplink topology.

If any Port-Channel uplink are used, corresponding Port-Channel must be created in UCS Manager, where the ID of the Port-Channel matches that on the data center switch.

If Port-Channel uplinks to data center switches are used, the UCS B Series Fabric Interconnects support only Link Aggregation Control Protocol (LACP). Ensure that the data center switch and Port-Channels are configured for, and support, LACP. This requirement also applies to vPC and VSS Port-Channels.

FC Mode

Both End Host and Switching modes are supported. End Host is the default for FC and FCoE NPIV with a supported FC Switch. Switching mode requires FC Zoning to be configured in the Fabric Interconnects. Refer to UCS Fabric Interconnect documentation for more information on these modes and use cases, and to specific SAN switch and SAN controllers vendor documentation as necessary. UCS Fabric Interconnect documentation is available at https://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-6200-series-fabric-interconnects/index.html.

FC Storage Port and FCoE Uplinks

Packaged CCE supports all FC and FCoE connected SAN topologies as supported by the UCS Fabric Interconnects, provided that all storage redundancy, latency, IO and bandwidth requirements are met.

Note If direct-attach SAN is used, qualified direct-attach FC and FCoE storage vendors are currently limited to EMC, Hitachi Data Systems, and NetApp. Please refer to the latest Cisco UCS hardware compatibility list for the most current qualified vendors and models, at https://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html.

QoS System Class and QoS Policy

Unified CM and CCE applications set L3 QoS DSCP (AF/CS), which is not handled by the Fabric Interconnects; Fabric Interconnects are not L3 aware. Packaged CCE does not require specific QoS System Class or QoS Policy settings for VMware vSwitches.

Cisco UCS B-Series Blade Requirements

Cisco UCS Manager uses Pools, Policies and Templates which are collected in a Service Profiles Template and applied to a blade as a Service Profile.

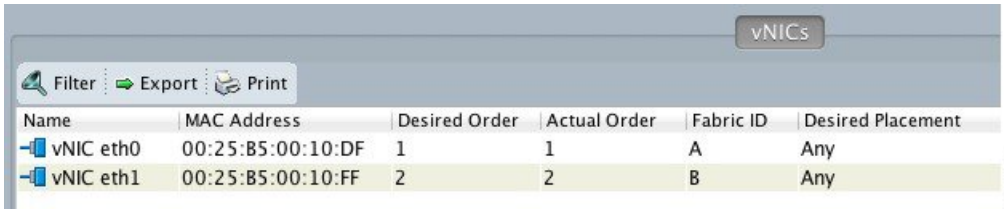
Packaged CCE does not have any specific requirements for the blade Service Profile or Service Profile Templates, other than the vNIC and vHBA requirements to conforming to network VLAN and FC/FCoE VSAN requirements (see vNIC Requirements, on page 13 and vHBA Requirements, on page 14).

For consistent and verifiable configuration and conformance of server configurations, use vNIC, vHBA and Service Profile Templates.

For more detail on UCS blade configuration and service profiles and templates, refer to the appropriate Cisco UCS Manager documentation.

vNIC Requirements

Packaged CCE requires that you configure a minimum of two vNIC Ethernet interfaces on the UCS B-series blade. You must assign each of these two interfaces to alternate Fabric Interconnects for redundancy.



Do **not** enable Fabric Failover for any Packaged CCE host vNIC interfaces.

The VMware VMKernel and Management interface is allowed to share the same vNICs with Packaged CCE.

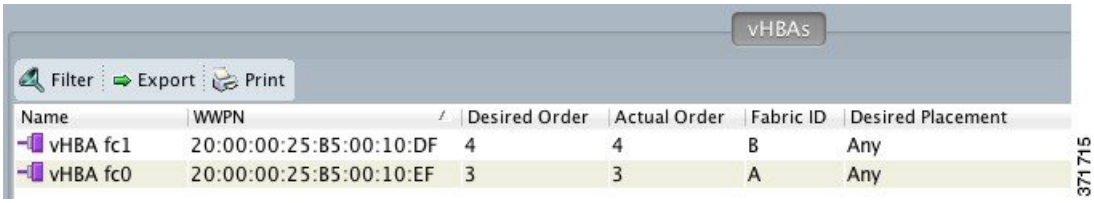
This table is an example of collapsed vNIC interfaces for all VLANs:

vNIC	VLANS	Fabric	Notes
eth0	PCCE Visible (Active) PCCE Private (Standby) VMware Kernel & Management (Active) Default VLAN (Active) Other Management (Active)	A	Active and Standby are denoted to show the reference design for traffic flow through these vNICs as aligned to Fabric Interconnects as controlled in the VMware layer. See the UCS B Series Networking section for more details.
eth1	PCCE Visible (Standby) PCCE Private (Active) VMware Kernel & Management (Standby) Default VLAN (Standby) Other Management (Standby)	B	

Note Networks other than the Packaged CCE Visible and Private networks are not required to be set to Active/Standby, as shown in the table. They can be set to Active/Active (no override), or assigned as needed to distribute load evenly across the infrastructure.

vHBA Requirements

You must configure a minimum of two vHBA FC interfaces on the UCS B-series blade. You must assign each of these two interfaces to alternate Fabric Interconnects for redundancy.



These FC vHBAs can be used for either FC or FCoE connected SAN. Use a different VSAN for each Fabric Interconnect (A/B) path to the SAN, but common VSAN is also supported.

Common (as depicted) or separate vHBA interfaces may be used for Packaged CCE datastores and ESXi Boot from SAN storage path.

Packaged CCE UCS B-Series Fabric Interconnects Validation Tool

This tool performs checks on currently deployed UCS B-Series Fabric Interconnect clusters to determine compliance with Packaged CCE requirements. If Packaged CCE will be deployed on two separate UCS B Series Fabric Interconnect clusters, run the tool for each cluster.

Note To run this tool, the Java version applicable to the version of the tool you are using must be installed.

Java 7 (any update) or Java 8 (any update) must be installed.

In addition to running this tool, see *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html and the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html to ensure full compliance.

To begin, download this file:

`UCSValidatorTool-<version>.zip`

Where <version> indicates the version of the tool you intend to install.

Once downloaded, follow these instructions to run the tool:

1. Unzip the UCSValidatorTool zip file to create a UCSValidatorTool directory.
2. Change to the UCSValidatorTool directory.
3. Run "java -jar UCSValidatorTool.jar".

The tool requests the following information:

- Company name (Required to generate the PDF filename using Company Name)
- IP Address of UCS Manager
- HTTPS (yes/no)
- Port (defaults to 80 for HTTP/443 for HTTPS)
- Username: Read-only credentials to UCS Manager
- Password

The following shows an example of the prompts.

```
Welcome to the Unified Computing System Verification Utility (version 11.6.1.0).
This tool will validate the UCS Fabric Interconnects for Packaged CCE requirements.
Enter company name: Cisco Systems Inc.
Enter UCS Manager cluster IP address: <ip-address-of-UCS-manager>
Use HTTPS? Yes/No: > (n[o]=80; y[es]=443)y
Port: [443]<port-number>
Enter UCS Manager access information with read privilege:
Username: <your-username>
Password: ****
Processing ........
```

After the validation process is complete, a summary of the pass/fail test results is displayed on the console, and output as both a log file (results/ucsValidation.log) and as a PDF file (Company-Name-date.pdf).

The following table provides a detailed explanation of each tool validation rule check run against the UCS B-Series Fabric Interconnects.

Table 1: Requirement Validation Rules

Category	Type	Requirements
Fabric Interconnect	Count	Two matching Fabric Interconnects (HA)
	Ethernet Mode	Mode must be End Host
	UCS Manager	Version 2.2(1) or later. A higher version than this may be required depending on the version of ESXi that you installed. Use the UCS Hardware and Software Compatibility tool to help you select the appropriate version. The tool can be found here: https://ucshcltool.cloudapps.cisco.com/public/

Category	Type	Requirements
	Ethernet Uplinks	

Category	Type	Requirements

		The Fabric Interconnect rule:
		Checks all Ethernet uplinks for one set that passes the following requirement validation rules.
		• Uplink Ethernet interface speed must be 10, 20, or 40 Gbps
		• For Uplink Eth Interfaces:
		  • Two or more (even, by two's) per Fabric Interconnect with common VLAN(s) (for grouping of ports across Fabric Interconnects - differentiate grouping if disjoint-L2)
		  • Four or more (even, by four's) per Fabric Interconnect pair grouped by common VLAN(s)
		• For Port Channels:
		  • One or more Port Channels per Fabric Interconnect
		  • Two or more Port Channels (even by two's) per Fabric Interconnect pair matched by common VLAN(s)
		  • Two or more member Ethernet ports (even, by two's) per Port Channel
		  • VLAN matched Port Channel pairs must have 4 or more (even, by four's) member Ethernet interfaces in total
		Caveats:
		• Even though Packaged CCE does not support splitting the Public and Private VLANs over disjoint-L2 uplinks, this tool examines each disjoint-L2 uplink set and provides pass/fail results. If any one set of uplinks is found to meet the requirements, the rule will pass even if others fail. In this case (as the tool is pre-deployment), if an uplink set that failed the rule is intended for Packaged CCE VLANs, it must be corrected to meet requirements for support.
		• The tool does not connect to or inspect the upstream data center switches to confirm the following requirements:
		  • Fabric Interconnect pair cross-connected to upstream data center switch pair
		  • Data center switch pair Ethernet interface ports properly configured for standard, EtherChannel,

Category	Type	Requirements
		vPC, or VSS uplink designs • Data center switch pair Ethernet interface ports properly configured for Virtual Switch VLAN Tagging (802.1q)

IO Model (Fabric Extender)	Count	The IO Model (Fabric Extender) rule:
		• Checks for two matching IO Modules on each blade chassis (minimum one required).
		Caveats:
		• This rule does not validate whether or not the two IO Modules are correctly connected to different Fabrics Interconnects (one to A and the other to B). However, the tool and output PDF does include the connection information for each IO Module (as shown in the following example).
		`Rule: IO Module count and models should match design. Result: Pass`
		`Details: --- Supported Chassis Configuration --- Chassis 1 PID`
		`N20-C6508 Serial FOX1721GCRG IO Module 1 PID UCS-IOM-2208XP Fabric`
		`ID A IO Module 2 PID UCS-IOM-2208XP Fabric ID B`
		• This rule does not validate that each IO Module has a minimum of two ports connected to its paired Fabric Interconnect as required.

Category	Type	Requirements

SAN Hardware and Transport	Type and Data Rate	The SAN Hardware and Transport rule:
		Checks all FC uplink types for one set of FC uplinks that pass the following requirement validation rules.
		• FC port speed must be 2, 4, or 8 Gbps
		• FCoE port speed must be 10, 20, or 40 Gbps
		• For FC ports:
		  • One or more per Fabric Interconnect
		• For FCoE ports:
		  • Two or more (even, by two's) per Fabric Interconnect
		• Number of FC and/or FCoE port channels must match on Fabric Interconnect pair (must be symmetrical)
		  • Two or more FC member ports per Fabric Interconnect
		  • Two or more FCoE member ports (even, by two's) per Fabric Interconnect
		Caveats:
		• This rule does not match FC or FCoE port counts between Fabric Interconnects (though this may be required for a given SAN design).
		• It does not validate any specific Cisco UCS and SAN switch and SAN controller supported designs.
		• It does not inspect FC or FCoE VSAN memberships for uplink grouping.
		• It does not inspect the FC Mode to validate uplinks for internal versus external NPV/NPIV designs.

The following table provides a detailed explanation of the UCS B-Series requirements not validated by this tool.

Table 2: Requirements Not Validated by the Tool

Category	Requirement
UCS Blade Server	UCS blade specification must match one of the following: • B200 M3 TRC#1: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-hardware.html • B200 M4 TRC#1: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-hardware.html Note: B200 M4 TRC#1 is supported for Release 11.0(1) and later only. Storage and Ethernet interface requirements: • Two vHBAs, alternately pinned to Fabric A and B • Two vNICs, alternately pinned to Fabric A and B • No Fabric Failover enabled on vNICs
UCS SAN HCL	The following SAN components (as applicable) must be on the UCS HCL for the version of UCS Manager firmware used: • FC SAN switch • SAN controller
SAN LUN	SAN LUNs must: • Meet the IOPS requirements • Meet the storage latency requirement
VMware vSphere ESXi	The tool does not connect to or check any vSphere ESXi specific requirements.

For more UCS HCL resources, see:

- https://www.vmware.com/resources/compatibility/search.php
- https://www.cisco.com/c/en/us/support/servers-unified-computing/unified-computing-system/products-technical-reference-list.html

NTP and Time Synchronization

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

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

For Cisco UCS B-series servers, you also must set the time zone and NTP Time Server using the UCS Manager. See Set Time Zone and NTP Time Server for Cisco UCS B-Series Servers, on page 23 for more information.

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

Windows Active Directory Domain

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

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

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

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

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

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

Windows Components in the Domain

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

Windows Components Not in the Domain

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

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

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

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

Cisco Integrated Service Routers

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

VOS Components

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

CLI commands for NTP Servers

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

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

ESXi Hosts

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

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

Set Time Zone and NTP Time Server for Cisco UCS B-Series Servers

Set the time zone and NTP Time server for UCS B-series server in the UCS Manager.

Procedure

Step 1 From the **Admin** tab in UCS Manager, select **Stats Mangement** > **Time Zone Management**.

Step 2 Select the **Time Zone** from the down-down menu.

Step 3 Click **Add NTP Time Server.**

Step 4 Enter the IP address of the NTP Time Server, and click **OK**.

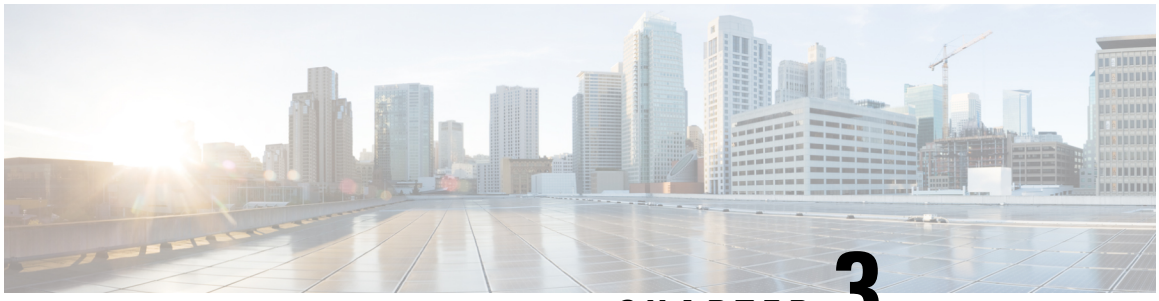
Step 5 Click **Save**.

Global Catalog Requirements

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

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

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



CHAPTER 3

Network Design Considerations

Network Design Considerations

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

Bandwidth Provisioning and Network QoS Considerations

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

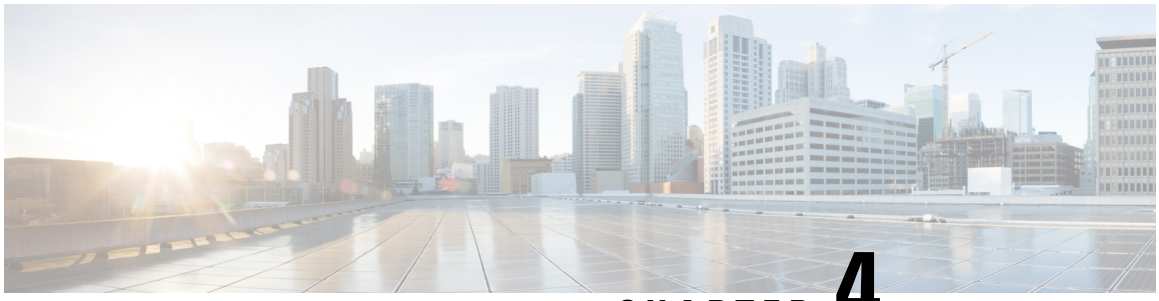
For bandwidth provisioning information for video calls, refer to the "Cisco Collaboration Solutions Design and Deployment Sizing Considerations" chapter of the *Cisco Collaboration System Solution Reference Network Designs*, at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home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

For bandwidth provisioning information for Cisco MediaSense video playback, refer to the "Scalability and Sizing" chapter of the *Cisco MediaSense Design Guide*, at https://www.cisco.com/c/en/us/support/customer-collaboration/mediasense/tsd-products-support-series-home.html.

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

PART II

Installation



CHAPTER 4

Create Virtual Machines for Components

About Creatings VMs

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

The sequence is:

1. Download the OVA files. See Open Virtualization Files, on page 37.
2. Create VMs (this chapter)..
3. After you create all the VMs, perform initial configuration. See Configuration, on page 67.

Create VM for Unified CCE PG

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

Sequence	Task
1	Using Packaged-CCE-UCCE.ova, Create a Virtual Machine from the OVA, on page 38. Select **Medium PG** from the drop-down list.
2	Install Microsoft Windows Server, on page 45

Sequence	Task
3	Install VMware Tools, on page 47
4	Configure Network Adapters for Unified CCE Rogger and Unified CCE PG, on page 47
5	Add Machine to Domain, on page 49
6	Install Antivirus Software, on page 43
7	Set Persistent Static Routes, on page 49
8	Run Windows Updates, on page 50
9	Install Cisco Unified Contact Center Enterprise, on page 54
10	Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55

Create VM for Unified CCE Rogger

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

Sequence	Task
1	Using Packaged-CCE-UCCE.ova, Create a Virtual Machine from the OVA, on page 38. Select **Rogger** from the drop-down list.
2	Install Microsoft Windows Server, on page 45
3	Install VMware Tools, on page 47
4	Configure Network Adapters for Unified CCE Rogger and Unified CCE PG, on page 47
5	Add Machine to Domain, on page 49
6	Install Antivirus Software, on page 43
7	Configure Database Drive, on page 41
8	Set Persistent Static Routes, on page 49
9	Run Windows Updates, on page 50
10	Install Microsoft SQL Server, on page 50
11	Install Cisco Unified Contact Center Enterprise, on page 54
11	Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55

Create VM for Unified CCE AW-HDS-DDS

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

Sequence	Task
1	Using Packaged-CCE-UCCE.ova, Create a Virtual Machine from the OVA, on page 38. Select **AW-HDS-DDS** from the drop-down list.
2	Install Microsoft Windows Server, on page 45
3	Install VMware Tools, on page 47
4	Configure Network Adapter for Unified CCE AW-HDS-DDS, AW-HDS, HDS-DDS , on page 49
5	Add Machine to Domain, on page 49
6	Install Antivirus Software, on page 43
7	Configure Database Drive, on page 41
8	Run Windows Updates, on page 50
9	Install Microsoft SQL Server, on page 50
10	Install Cisco Unified Contact Center Enterprise, on page 54
11	Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55

Create VMs for the Cisco Unified Customer Voice Portal Servers

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

- The Unified CVP Servers are deployed as two virtual machines—one on Side A and one on Side B.
- The Unified CVP OAMP Server is deployed as one virtual machine on Side A.

This process is similar for the Unified CVP Servers and the Unified CVP OAMP Servers—the differences are selections you make from the OVA drop-down list and in the Select Packages options during the installation.

Sequence	Task
1	Using Packaged-CCE-CVP.ova, Create a Virtual Machine from the OVA, on page 38. From the drop-down list: • Select **Cisco Unified CVP Call Server-VXML Server** from the drop-down list when you create the Unified CVP Server VM. • Select **Cisco Unified CVP Operations Console** from the drop-down list when you create the Unified CVP OAMP Server VM.
2	Install Microsoft Windows Server, on page 45 NTP configuration is required if this machine is not in the same domain as the Unified CCE Roggers, AWs, and PGs. See NTP and Time Synchronization, on page 21.
3	Install VMware Tools, on page 47
4	Configure Network Adapters for Cisco Unified CVP, on page 55
5	Add Machine to Domain, on page 49
6	Install Antivirus Software, on page 43
7	Run Windows Updates, on page 50
8	Install Cisco Unified CVP Server, on page 56

Create VM for Cisco Unified CVP Reporting Server

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

Sequence	Task
1	Using the Packaged-CCE-CVP.ova template, create a virtual machine. For more information, see Create a Virtual Machine from the OVA, on page 38. Select **Cisco Unified CVP Reporting Server** from the drop-down list.
2	Install Microsoft Windows Server, on page 45 NTP configuration is required if this machine is not in the same domain as the Unified CCE Roggers, AWs, and PGs. See NTP and Time Synchronization, on page 21.
3	Install VMware Tools, on page 47
4	Configure Network Adapters for Cisco Unified CVP, on page 55
5	Install Antivirus Software, on page 43
6	Configure Database Drive, on page 41
7	Run Windows Updates, on page 50
8	Install Cisco Unified CVP Reporting Server, on page 56

Sequence	Task
9	Add Machine to Domain, on page 49

Create VM for Cisco Unified Communications Manager Publisher

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

Note For the UCS C240 M4 Server, the Unified Communications Manager (CUCM) 12.5 and above installation must be off-box.

Sequence	Task
1	Using Packaged-CCE-CUCM.ova. Create a Virtual Machine from the OVA, on page 38. Select **CUCM 10000 user node** from the drop-down list.
2	Configure DNS Server, on page 41
3	Install the Unified Communications Manager Publisher. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 57.
4	Install VMware Tools, on page 47
5	Configure the Cluster for Cisco Unified Communications Manager, on page 60
6	Create a Unified Communications Manager AXL User Account, on page 60
7	Generate and install the Unified Communications Manager License, on page 64.
8	Activate Services, on page 64

Create VM for Cisco Unified Communications Manager Subscriber

Sequence	Task
1	Using Packaged-CCE-CUCM.ova, Create a Virtual Machine from the OVA, on page 38. Select **CUCM 7500 user node** from the drop-down list.
2	Configure DNS Server, on page 41

Sequence	Task
3	Install the Unified Communications Manager Subscriber. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 62.
4	Install VMware Tools, on page 47
5	Generate and install the Unified Communications Manager License, on page 64.
6	Activate Services, on page 64

Create VM for Cisco Finesse Primary

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

Sequence	Task
1	Using the Packaged-CCE-Finesse.ova, Create a Virtual Machine from the OVA, on page 38. Select **2000 HTTP or 2000 HTTPS Agent** from the drop-down list.
2	Configure DNS Server, on page 41
3	Install the Cisco Finesse Primary node. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 57.
4	Install VMware Tools, on page 47
5	Configure the Cluster for Cisco Finesse, on page 61

Create VM for Cisco Finesse Secondary

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

Sequence	Task
1	Using Packaged-CCE-Finesse.ova, Create a Virtual Machine from the OVA, on page 38. Select **2000 HTTP or 1500 HTTPS Agent** from the drop-down list. Select **2000 HTTP or 2000 HTTPS Agent** from the drop-down list.
2	Configure DNS Server, on page 41
3	Install the Cisco Finesse Secondary node. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 62.
4	Install VMware Tools, on page 47

Create VM for Cisco Unified Intelligence Center Publisher

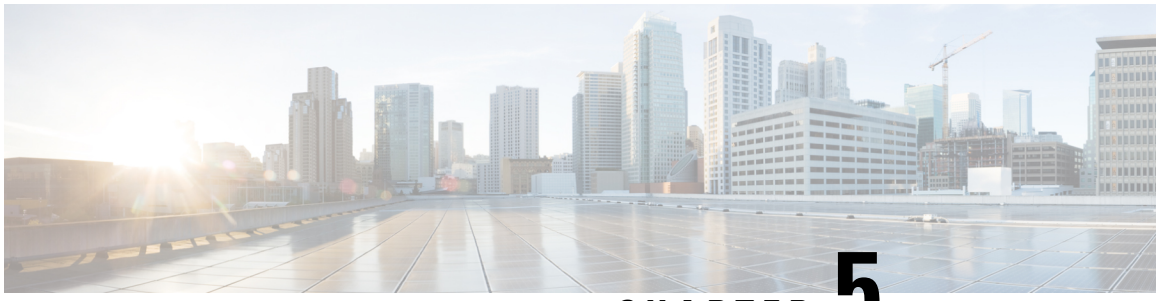
Follow this sequence of tasks to create the virtual machine for the Unified Intelligence Center Publisher. Live Data and the Cisco Identity Service are also installed on the same VM.

Sequence	Task
1	Using Packaged-CCE-CUIC.ova, Create a Virtual Machine from the OVA, on page 38. Select **Co-Resident** from the drop-down list.
2	Configure DNS Server, on page 41
3	Install the Cisco Unified Intelligence Center Publisher. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 57.
4	Install VMware Tools, on page 47
5	Acquire and upload the license. See Cisco Unified Intelligence Center License, on page 59.
6	Configure the Cluster for Cisco Unified Intelligence Center, on page 61

Create VM for Cisco Unified Intelligence Center Subscriber

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

Sequence	Task
1	Using Packaged-CCE-CUIC.ova, Create a Virtual Machine from the OVA, on page 38. Select **Co-Resident** from the drop-down list.
2	Configure DNS Server, on page 41
3	Install the Cisco Unified Intelligence Center Subscriber. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 62.
4	Install VMware Tools, on page 47



CHAPTER 5

Tasks Common to Virtual Machines

Open Virtualization Files

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

OVA files for Packaged CCE are contained in the **Packaged-CCE-OVA** zip file at Cisco.com.

1. Go to https://cisco.com/en/US/products/ps12586/tsd_products_support_series_home.html. Click **Download Software**. Then select Packaged Contact Center Enterprise Virtual Machine Templates.
2. Go to Download Software page on Cisco.com.
3. Select the required release version.
4. Download and extract the file and save the OVAs to your local drive.

Mount and Unmount 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 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. Uncheck **Connect at power on** (Device status panel, upper right).

Create a Virtual Machine from the OVA

Procedure

Step 1 Select the Host in the vSphere client.

Step 2 Choose **File** > **Deploy OVF Template**.

Step 3 Browse to the location on your local drive where you stored the OVA. Click **Open** to select the file. Click **Next.**

Step 4 Click **Next** at the OVF Template Details page.

Note For Cisco Unified CVP ova, an End User License Agreement displays. Click **Agree** and then click **Next**.

Step 5 Enter the virtual machine name. Click **Next**.

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

Step 6 On the Deployment Configuration page, use the drop-down to select the appropriate configuration. Then click **Next**.

Step 7 Choose a datastore on which to deploy the new virtual machine. Then click **Next.**

For each datastore, the following tables describe the RAID group, the ESXi Host, and the virtual machines for the C240 M3S, C240 M4SX and C240 M5SX servers.

RAID configuration for the C240 M3S

RAID Group	VM Datastore	ESXi Host	Virtual Machines
VD0	datastore1	A	ESXi operating system Unified CCE AW-HDS-DDS Side A
VD1	datastore2	A	Unified CCE PG Side A Unified CCE Rogger Side A Unified CVP Server Side A Unified Intelligence Center Server Publisher Unified CVP OAMP Server Unified Communications Manager Publisher Unified Communications Manager Subscriber 1 Cisco Finesse Primary
VD0	datastore1	B	ESXi operating system Unified CCE AW-HDS-DDS Side B
VD1	datastore2	B	Unified CCE PG Side B Unified CCE Rogger Side B Unified CVP Server Side B Unified Intelligence Center Server Subscriber Unified Communications Manager Subscriber 2 Unified CVP Reporting Server (optional) Cisco Finesse Secondary

RAID configuration for the C240 M4SX and C240 M5SX

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

RAID Group	VM Datastore	ESXi Host	Virtual Machines
VD1	datastore 2	A	Unified CCE AW-HDS-DDS Side A
VD2	datastore 3	A	Unified Communications Manager Subscriber 1 Unified CVP OAMP Server Unified CVP Server Side A
VD3	datastore 4	A	Unified Intelligence Center Server Publisher Unified CCE PG Side A
VD0	datastore 1	B	ESXi operating system Unified CCE Rogger Side B Unified CCE Router Side B Unified CCE Logger Side B Unified Communications Manager Subscriber 2 Cisco Finesse Secondary
VD1	datastore 2	B	Unified CCE AW-HDS-DDS Side B
VD2	datastore 3	B	Unified Customer Voice Portal Reporting Server (optional) Unified CVP Server Side B
VD3	datastore 4	B	Unified Intelligence Center Server Subscriber Unified CCE PG Side B Enterprise Chat and Email Server (optional)

Step 8 On the Disk Format page, keep the default virtual disk format: **Thick provisioned Lazy Zeroed format**. Click **Next.**

Step 9 Confirm that the Network Mapping page is correct for the Unfied CCE Rogger and PG:

a) For the Unifed CCE Rogger and PG:

b)
- Map Public to UCCE Public Network
- Map Private to UCCE Private Network

c) For all other servers, map Public to UCCE Public Network.

Step 10 At the Successfully Completed message, click **Close**.

Note Do not make any changes to the VM configurations once the VMs are created.

Configure DNS Server

This procedure is for Windows DNS server.

Note If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs in order to work properly.

Procedure

Step 1 Log in to the DNS server.

Step 2 In Windows, navigate to **Administrative Tools** > **DNS**. This opens the DNS Manager.

Step 3 In the Forward lookup zone, navigate to your deployment's domain name.

Step 4 Right-click the domain name and select **New Host (A or AAAA)**.

Step 5 In the New Host dialog box, enter the computer name and IP address (IPv4) of VOS components.

Configure Database Drive

Note Complete this procedure to create a virtual drive, if the virtual drive was not automatically created in the VM.

Procedure

Step 1 Add a virtual drive as follows:

Using Vsphere client:

a) Right-click the virtual machine and click **Edit Settings**.
b) In the **Hardware** tab, click on **Add**.

The **Add Hardware** window appears.

c) You can select the type of device you wish to add. Select **Hard Disk**, and then click **Next**.
d) Select the **Create a new virtual disk** option, and then click **Next**.
e) In the **Capacity** section, use the **Disk Size** box to assign the desired disk space, and then click **Next**.

Note Virtual machine templates for Logger, Rogger, AW, and HDS servers do not have a SQL database drive preprovisioned. The following reference table must be used to assign disk space to the virtual machine based on the type of validation errors will occur:

Virtual Machine Template	Default Second Disk Size
Logger	500 GB
Rogger	150 GB
AW-HDS-DDS	750 GB
AW-HDS	500 GB
HDS-DDS	500 GB
CVP Reporting Server	438 GB

You can custom size the SQL database disk space to meet the data retention requirements on an external AW-HDS-DDS server only, as calculated by the Database Estimator tool.

f) On the **Disk Provisioning** section choose **Thick provision Lazy Zeroed format**. Click **Next**.
g) In the **Advanced Options** section, retain the default options and then click **Next**.
h) In the **Ready to Complete** section, click **Finish** to create the hard disk.
i) Click **OK** to confirm the changes.

The Recent Tasks window at the bottom of the screen displays the progress.

Step 2 Choose **Start** > **Windows Administrative Tools** > **Computer Management**.

Step 3 In Windows, navigate to **Disk Management**.

Step 4 Right-click on the **Disk 1** box and select **Online**.

Step 5 Initialize Disk 1 as follows:

a) Right-click on the **Disk 1** box and select **Initialize Disk**.
b) Check the **Disk 1** checkbox.
c) Select the **MBR (Master Boot Record)** radio button.
d) Click **OK**.

Step 6 Create a new disk partition as follows:

a) Right-click the graphic display of **Disk 1** and select **New Simple Volume**.
b) Click **Next** on the first page of the **New Simple Volume Wizard**.
c) On the **Specify Volume Size** page, retain the default volume size. Click **Next**.
d) On the **Assign Drive Letter or Path** page, assign drive letter (E). Click **Next**.
e) On the **Format Partition** page, format the partition as follows:

1. Select the **Format this volume with the following settings** radio button.
2. Click **Format Disk**.
3. Select File System as **NTFS** and click **Start**.
4. Select **Default** from the **Allocation unit size** drop-down menu.
5. Enter a value in the **Volume label** field.

6. Check the **Perform a quick format** checkbox.
7. Click **Next**.

f) Click **Finish**.

The format is complete when the status changes to Healthy.

A popup window displays a message that you need to format the disk before you can use it.

Step 7 Format the disk.

a) Click **Format disk**.
b) Click **Start**.
A popup displays a warning that formatting will erase all data on the disk.
c) Click **OK**.
d) When the format is complete, click **OK** to close the popup window.

Install Antivirus Software

Install one of the supported antivirus software products.

See the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for the list of supported products.

Important Disable automatic updates. Update antivirus software manually.

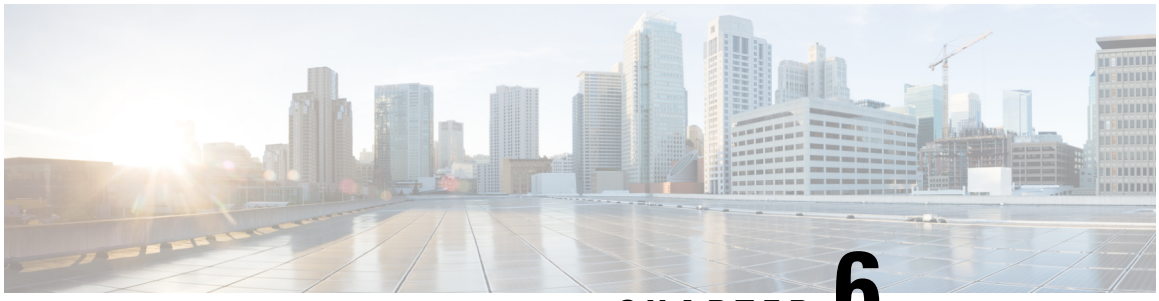
Tip To allow required access to installation program files or folders, perform file-blocking exclusions in the antivirus product file-and-folder protection rules. To do this in McAfee VirusScan:

1. Launch the VirusScan console.
2. Right-click **Access Protection** and select **Properties.**
3. In the Anti-virus Standard Protection category, make sure that the rule Prevent IRC communication is unchecked in the Block column.

For more information about changing settings, see the documentation for your antivirus software.

For more information on security guidelines, refer the **General Antivirus Guidelines** section in the *Security Guide for Cisco Unified ICM/Contact Center Enterprise Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Important The firewall component of Symantec Endpoint Protection 12.1, the Network Threat Protection feature, must be disabled. If the feature remains enabled, which is the default, both sides of a duplexed router come up in simplex mode, thus blocking communication between each side of a router. This blocking impacts all deployment types.



CHAPTER 6

Software Installations for Components

Install Microsoft Windows Server

Complete the following procedure to install Microsoft Windows Server on the virtual machines deployed.

Procedure

Step 1 Mount the Microsoft Windows Server ISO image to the virtual machine.

Check the **Connect at power on** check box when mounting the ISO.

Step 2 Power on the VM.

Step 3 Enter the Language, Time and Currency Format, and Keyboard settings. Click **Next**.

Step 4 Click **Install Now**.

Step 5 If prompted, enter the product key for Windows Server and click **Next**.

Step 6 Select the Desktop Experience option for the Windows Server and click **Next**.

Step 7 Accept the license terms and click **Next**.

Step 8 Select **Custom: Install Windows only (advanced)**, select **Drive 0** to install Microsoft Windows Server, and then click **Next**.

The installation begins. After the installation is complete, the system restarts without prompting.

Step 9 Enter and confirm the password for the administrator account, and then click **Finish**.

Step 10 Enable Remote Desktop connections as follows:

a) Navigate to **Control Panel** > **System and Security** > **System**.
b) Click **Remote Settings**.
c) Click the **Remote** tab.
d) Select the **Allow remote connections to this computer** radio button. The Remote Desktop Connection dialog displays a notification that the Remote Desktop Firewall exception is enabled. Click **OK**.

Step 11 Install VMWare tools. See Install VMware Tools, on page 47.

Step 12 Open the **Network and Sharing Center**, and in the View your basic network info and set up connections section, click **Ethernet**.

Step 13 In the Ethernet Status window, click **Properties**.

Step 14 In the **Ethernet Properties** dialog box, configure the network settings and the Domain Name System (DNS) data:

a) Uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
b) Select Internet Protocol Version 4 (TCP/IPv4) and click **Properties**.
c) Select **Use the following IP Address**.
d) Enter the IP address, subnet mask, and default gateway.
e) Select **Use the following DNS Server Address**.
f) Enter the preferred DNS server address, and click **OK**.

Microsoft Windows Server is installed. In addition, Internet Explorer 11 is installed automatically.

Note If you want to install Unified CCE on a multilingual version of Windows Server, run the Multilingual User Interface (MUI) language pack. See https://software.cisco.com/download/release.html?mdfid=268439622&flowid=46046&softwareid=280840583.

If Unified CCE language pack is applied on Chinese Windows OS machine, set the screen resolution to 1600 x 1200.

Related Topics

Mount and Unmount ISO Files, on page 37

Install VMware Tools

Use this procedure to install and upgrade VMware tools from the VMware vSphere Client.

To install or upgrade VOS for Cisco Finesse, Cisco Unified Intelligence Center, and Cisco Unified Communications Manager:

1. Ensure that your virtual machine is powered on.
2. Right-click the VM in the virtual machine menu. Select **Guest** > **Install / Upgrade VMware tools**
3. Choose the automatic tools update and press **OK**.

The process takes a few minutes. When the process is complete, the tools are listed as Running (Current) on the VM's Summary tab in vSphere.

To install or upgrade VMs with Windows guest operating system:

1. Ensure that your Windows virtual machine is powered on.
2. Right click the VM in the virtual machine menu. Select **Guest** > **Install / Upgrade VMware tools**. Click **OK** on the popup window.
3. Log in to the VM as a user with administrative privileges.
4. Run VMware tools from the DVD drive.

   The installation wizard starts.
5. Follow the prompts in the wizard to complete the VMware Tools installation. Choose the **Typical** installation option.
6. When the VMware Tools installation has finished, restart the virtual machine for the changes to take effect.

When the process is complete, the tools are listed as Running (Current) on the VM's Summary tab in vSphere.

Configure Network Adapters for Unified CCE Rogger and Unified CCE PG

The Unified CCE Rogger and the Unified CCE PG each have two network adapters. You must identify them by MAC address and Network Label, rename them, configure them, and set the interface metric value.

Procedure

Step 1 Identify the MAC addresses and labels for the network adapters as follows:

a) From vSphere, select and right-click the VM.

b) Select **Edit Settings**. In the **Hardware** tab, click **Network adapter 1**. In the right panel, write down the last few digits of MAC addresses and note whether the label is PCCE Public or PCCE Private. For example, Network adapter 1 may have a MAC address that ends in 08:3b and the network label PCCE Public.

c) Repeat for Network adapter 2, noting its MAC address and label.
d) From the VM console, type **ipconfig /all** from the command line. This displays the adapter names and physical addresses.
e) Note the adapter names and physical addresses and match them with the MAC addresses and labels that you noted in VMware. For example, in ipconfig/all, Local Area Connection 2 may have a physical address that ends in 08-3b.
f) Match the MAC address of the network adapter that VMware identified as PCCE Public with the corresponding physical address of Local Area Connector. In this example, the physical address of Local Area Connection 2 (08-3b) matches the MAC address (08-3b) of Network adapter 1. This means that Local Area Connection 2 is PCCE Public.

Note Adapters may have a different name than Local Area Connection.

Step 2 Locate and rename the network adapters in Windows as follows:

a) In Windows, open the **Control Panel** > **Network and Sharing Center** and click **Change adapter settings**.
b) Right-click **Local Area Connection** and select **Rename**. Rename it to **PCCE Public** or **PCCE Private**, based on the matching you did above.
c) Right-click **Local Area Connection 2** and select **Rename**. Rename it to **PCCE Public** or **PCCE Private**, based on the matching you did above. In the example above, **Local Area Connection 2** is renamed to PCCE Public.

Step 3 Set the Properties for PCCE Public as follows:

a) Right-click **PCCE Public** and select **Properties**.
b) In the **Networking** tab, uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
c) Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
d) In the **General** tab for Internet Protocol Version 4, select **Use the following IP address** and enter **IP address**, **Subnet mask**, **Default gateway**, and DNS servers.
e) Click **OK** and **Close** to exit.

Step 4 Set the Properties for PCCE Private as follows:

a) Right-click **PCCE Private** and select **Properties**.
b) In the **Networking** tab, uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
c) Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
d) In the **General** tab for Internet Protocol Version 4, select **Use the following IP address** and enter **IP address** and **Subnet mask**.
e) Click **Advanced**.
f) Click the **DNS** tab and uncheck *Register this connection's addresses in DNS*.
g) In the DNS server, add a new A record that resolves to the private IP address. Also, create an associated pointer record for reverse lookups.

Note For hostnames in A records, append the letter p to indicate that it is a private address.

h) Click **OK** to exit.

Configure Network Adapter for Unified CCE AW-HDS-DDS, AW-HDS, HDS-DDS

Procedure

Step 1 Locate and rename the network adapter in Windows as follows:

a) In Windows, open the **Network and Sharing Center** and click **Change Adapter Settings** .
b) Right-click **Local Area Connection** and select **Rename**. Rename it to **UCCE Public**.

Step 2 Set the Properties for UCCE Public as follows:

a) Right-click **UCCE Public** and select **Properties**.
b) In the Networking dialog box, uncheck Internet Protocol Version 6 (TCP/IPv6).
c) In the Networking dialog box, select Internet Protocol Version 4 (TCP/IPv4) and select **Properties**.
d) In the General dialog box for Internet Protocol Version 4, select **Use the following IP address** and enter the IP address, the Subnet mask, the default gateway, and DNS servers.
e) Click **OK** and **Close** to exit.

Add Machine to Domain

Procedure

Step 1 Navigate to **Control Panel** > **System and Security** > **System**.
Step 2 Click **Change Settings**.
Step 3 In the **Computer Name** tab, click **Change**.
Step 4 Change the name of the computer from the name randomly generated during Microsoft Windows Server installation. The name does not contain underscores or spaces.
Step 5 Select the **Domain** radio button to change the member from Workgroup to Domain.
Step 6 Enter qualified domain name and click **OK**.
Step 7 In the **Windows Security** dialog, enter the domain credentials and click **OK**.
Step 8 On successful authentication, click **OK**.
Step 9 Reboot the server and sign in with domain credentials.

Set Persistent Static Routes

For geographically distributed Central Controller sites, redundant Rogger, and Peripheral Gateway components typically have a Private IP WAN connection between Side A and Side B. Windows only allows one default

gateway for each VM (which sends the Private Network traffic to the Public Network). So, you add a Static Route to all the VMs running the Rogger, and PG applications.

For geographically distributed Central Controller sites, redundant Rogger, logger, router, and Peripheral Gateway components typically have a Private IP WAN connection between Side A and Side B. Windows only allows one default gateway for each VM (which sends the Private Network traffic to the Public Network). So, you add a Static Route to all the VMs running the Rogger, logger, router, and PG applications.

To create a persistent static route with the **route add** command, you need the destination subnet, the subnet mask, the local gateway IP, and the interface number of the local Private Network interface:

```
route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p
```

You must launch the DOS prompt as an administrator to run the commands in this procedure.

Procedure

Step 1 On each Rogger, or PG VM, run `ipconfig /all`.
Record the `IPv4 Address`, `Subnet Mask`, and `Physical Address` (MAC address) for the Private Network interface.

Step 2 On each of these VMs, run `route print -4`.
Record the `Interface` for the Private Network. You can identify the correct interface by looking for its `Physical Address` (MAC address).

Step 3 On each of these VMs, run `route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p` to add a persistent static route for the remote Private Network.

On Side A VMs, use the gateway IP for Side B. On Side B VMs, use the gateway IP for Side A.

Run Windows Updates

Procedure

Go to **Settings** > **Update & Security** and run Microsoft Windows Update.

After the update is complete, click **Do not enable automatic updates**.

Install Microsoft SQL Server

Install Microsoft SQL Server, and store the SQL Server log and temporary files on the same physical disk as the operating system.

Note For information about supported editions, see the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html.

Before you begin

Enable Microsoft .NET Framework 3.5 SP1 before installing SQL Server 2014. In the Windows Server, Server Manager, use the Add Roles and Features Wizard to enable the .NET Framework 3.5 SP1. See the Microsoft documentation at https://technet.microsoft.com/en-au/library/dn482071.aspx for detailed instructions.

Note If your computer has no internet connection to get the updates, download and install Microsoft .NET Framework 3.5 SP1 manually.

Add the virtual machine to a domain before installing SQL Server.

Procedure

Step 1 Mount the Microsoft SQL Server ISO image to the virtual machine. For more information, see Mount and Unmount ISO Files, on page 37.

Step 2 Run **setup.exe**.

Step 3 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 4 On the **Product Key** page, enter the product key and then click **Next**.

Step 5 Accept the **License Terms** and then click **Next**.

Step 6 On the Feature Selection page, select on of the following; and then click **Next**.

- Database Engine Services
- Clients Tool Connectivity
- Documentation Components
- Management Tools - Basic
- Management Tools - Complete
- SQL Client Connectivity SDK

Step 7 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** check box, click **Next** on the **Product Updates** page.

Step 8 On the **Instance Configuration** page, select **Default Instance** and click **Next.**

Step 9 For the remaining services, accept the default values.

Step 10 In the **Start Up Type** column, for the **SQL Server Agent service** account, select **Automatic** from the list.

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) 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)
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. Shared Memory
2. Named Pipes
3. 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 releases the memory only when other processes request it, which can cause unnecessary memory monitoring tool alerts.

Cisco supports the Microsoft guideline 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 limit of the memory with the maximum memory usage settings in the SQL Server Properties menu.

For more information on SQL Server memory settings and 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 Unified CCE 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**.

Set Users as System Administrators

Any users who are involved in installing or upgrading a Unified ICM/CCE & Hosted solution must be added as part of SQL Server Security login and associated with the System Administrator role. Complete the following steps to set a user as a System Administrator:

Procedure

Step 1 Open the Microsoft SQL Server Management Studio using the System Administrator login credentials.

Step 2 In the Object Explorer pane, click the **Security** folder.

The **Security** folder expands.

Step 3 Right-click the **Logins** folder, and then click **New Login**.

The Login-New view appears.

Step 4 In the **Login name** field, enter the Domain login name of the user whom you want to associate with the System Administrator role.

Use the following format:

```
<domain>\<username>
```

Step 5 In the Object Explorer pane, click the **Server Roles** folder.

The Server Roles view appears.

Step 6 Check the **sysadmin** check box.

Note This step is mandatory.

System administrator is a predefined fixed server-level role in the Microsoft SQL Server. The system administrator performs operations on a site-level. System administrators manage jobs, role definitions, and shared schedules that are used to run reports.

You must be a system administrator to create, modify, and delete individual records in the Configuration Manager tool.

For details about the **sysadmin** role, see the *Microsoft SQL* documentation.

Step 7 Click **OK**.

The user is now a part of the SQL Security login and is also associated with the System Administrator role.

Collation and Locale Settings for Localization

Microsoft SQL Server Collation Settings for Languages

You select a collation when you install Microsoft SQL Server, and it must be the collation that maps to the customer's language display.

Remember If your initial collation selection is incorrect, you must uninstall Microsoft SQL Server and reinstall it with the correct collation configuration.

For the languages supported by Packaged CCE and the SQL Server Collation setting for each language, see the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html.

Windows System Locale

The Windows system locale must match the display language; otherwise some characters appear incorrectly in the user interface and are saved incorrectly to the database. For example, if the system locale is English and you are working in Spanish, characters such as the *acute a* appear incorrectly.

Perform this procedure at both CCE Roggers, both CCE PGs, both CCE AWs, and any external HDS systems.

1. Open **Control Panel > Clock, Language, and Region > Language**.
2. Add the required language in the **Change your language preferences** page.
3. In the left pane, select **Advanced settings**.
4. Select the language for the **Override for Windows display language** option.
5. Select the language for the **Override for default input method** option.
6. Save your work and restart the virtual machine.

Install Cisco Unified Contact Center Enterprise

Install the Unified Contact Center Release 11.0 12.0 software on your Unified CCE virtual machines. Install Unified Contact Center Release 11.0(1) before you install the Release 11.6(1) software.

Procedure

Step 1 Login as a user with administrative privileges.

Step 2 Mount the Cisco Unified CCE ISO image to the virtual machine. See Mount and Unmount ISO Files, on page 37.

Step 3 Run setup.exe from the D:\ICM-CCE-CCH Installer directory.

Step 4 Follow the InstallShield procedures to install Cisco Unified CCE.

Step 5 When the installation completes, restart the computer when prompted.

Step 6 Before applying any ES, you must run the mandatory update for Packaged CCE, if a fresh install is being performed on Windows Server 2016. You can download the `CCE 12.0 Mandatory Update for Fresh Install/Tech Refresh` from https://software.cisco.com/download/home/268439622/type/280840583/release/12.0(1).

Step 7 Unmount the ISO image.

Install Cisco Unified Contact Center Enterprise Release 11.6(1)

Procedure

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

Step 2 After either downloading the installer or placing the media in the drive, start the Cisco ICM Minor Release ICM Installer.

Step 3 Follow the on-screen instructions to install Unified CCE Release.

Step 4 After the installation is complete, unmount the ISO image.

Configure Network Adapters for Cisco Unified CVP

Unified CVP has only one network adapter to configure. You must rename it and set its properties.

Procedure

Step 1 Navigate to **Control Panel** > **Network and Internet** .

Step 2 Click **Network and Sharing Center**, and then click **Change adapter settings** in the left panel.

Step 3 Right-click the adapter and select **Rename**. Change the name to UCCE Public.

Step 4 Right-click UCCE Public and select **Properties**.

Step 5 In the Networking dialog box, de-select Internet Protocol Version 6 (TCP/IPv6).

Step 6 In the Networking dialog box, select Internet Protocol Version 4 (TCP/IPv4) and select **Properties**.

Step 7 In the General dialog box for Internet Protocol Version 4 , select **Use the following IP address** and enter the IP address, the Subnet mask, the default gateway and DNS servers.

Step 8 Click **OK** and **Close** to exit.

Install Cisco Unified CVP Server

Procedure

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

Step 2 Mount the Unified CVP ISO image to the virtual machine. For more information, see Mount and Unmount ISO Files, on page 37.

Step 3 Run setup.exe from the D:\ CVP\Installer_Windows directory.

Step 4 Follow the InstallShield wizard to Run setup.exe from the D:\CVP\Installer_Windows directory:

a) Accept the license agreement.

b) In the **Select Packages** screen, check the type you are adding. Options are CVP Server, Operations Console, and Reporting Server.

Note Select Operations Console when creating the Unified CVP OAMP server VM.

c) Click **Next**.

d) On the **Voice Prompt Encode Format** screen, select the codec according to your requirement.

e) In the **Choose Destination Location** screen, accept the default. Click **Next**.

f) In the **X.509 certificate** screen, enter the information that you want to include in the certificate.

g) In the **Ready to Install** screen, click **Install**.

h) For the OAMP Server only, enter and confirm a password. Click **Next**.

i) Select the option to restart the computer after installation. Click **Finish**.

Step 5 If Unified CVP Engineering Specials are available, copy them to the local drive. Follow the InstallShield wizard to install them.

Step 6 Unmount the ISO image.

Unified CVP Server installation automatically creates a default user for the Unified CVP Ops Console Server Web Services manager CLI, with the following credentials:

- **Username:** wsmadmin
- **Password:** password you entered for the OAMP Server

You can create and manage additional Web Services manager CLI users using the Unified CVP Operations Console, if needed.

Install Cisco Unified CVP Reporting Server

This task is required for the installation of the optional Unified CVP Reporting server.

The IBM Informix database server is installed as part of the Unified CVP Reporting Server.

Before installing the Unified CVP Reporting Server, you must configure a database drive. For more information .

Complete the following procedure to install the Unified CVP Reporting server:

Procedure

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

Step 2 Mount the Unified CVP ISO image to the virtual machine. For more information, see Mount and Unmount ISO Files, on page 37.

Step 3 Run setup.exe from the DVD drive located at the `CVP\Installer_Windows` directory.

Step 4 Follow the InstallShield wizard to Run setup.exe from the `D:\CVP\Installer_Windows` directory:

a) Accept the license agreement.
b) In the **Select Packages** screen, check **Reporting Server**.
c) In the **Choose Destination Folder** screen, select the folder location for the CVP installation folder.
d) In the **X.509 certificate** screen, enter the information that you want to include in the certificate.
e) In the **Choose the database data and backup drive** screen, enter the drive letter (typically, E).
f) In the **Database size selection** screen, select Premium (438 GB).
g) In the **Ready to Install** screen, click **Install**.
h) Enter the Reporting Server password when prompted.
i) Select the option to restart the computer after installation. Click **Finish**.

Step 5 If Unified CVP Engineering Specials are available, copy them to the local drive. Follow the InstallShield wizard to install them.

Step 6 Unmount the ISO image.

What to do next

Repeat this procedure if your deployment requires a second, external Unified CVP Reporting Server.

Ensure that you generate a license file and add the license file to `C:\Cisco\CVP\conf\license`. For more information, see Generate a License, on page 80. Shut down and then start each of the CVP Reporting Servers for the new license to take effect.

You may see the following error:

```
CVP_12_0_Infrastructure-2-LICENSING: Evaluation license already expired on
```

Manually rename license file and extension to `cvp.license`.

Ensure you place it in the `C:\Cisco\CVP\conf\license` filepath.

Install Publishers/Primary Nodes of VOS-Based Contact Center Applications

This task is required for the publisher/primary nodes of the three VOS-based contact center applications: Cisco 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, Cisco Finesse and Cisco Identity Service (IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Procedure

Step 1 Create a virtual machine for your VOS-based contact center application using the OVA.

Step 2 Mount the ISO image for the software to the virtual machine.

Step 3 Select the virtual machine, power it on, and open the console.

Step 4 Follow the Install wizard, making selections as follows:

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.

b) In the **Success** screen, select **OK**.

c) In the **Product Deployment Selection** screen:

- If you are installing Finesse or Unified Communications Manager, select **OK**.
- If you are installing Unified Intelligence Center, select **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center with Live Data, and Cisco Identity Service (IdS) on the same server.

d) In the **Proceed with Install** screen, select **Yes**.

e) In the **Platform Installation Wizard** screen, select **Proceed**.

f) In the **Apply Patch** screen, select **No**.

Finesse does not have this step.

g) In the **Basic Install** screen, select **Continue**.

h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

Note For Live Data servers, use the same timezone for all the nodes.

i) In the **Auto Negotiation Configuration** screen, select **Continue**.

j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.

k) In the **DHCP Configuration** screen, select **No**.

Finesse does not have this step.

l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.

m) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.

n) Enter your DNS client configuration. Select **OK**.

Important DNS client configuration is mandatory for Finesse. If you do not perform this step, agents cannot sign in to the desktop and you must reinstall Finesse.

o) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.

p) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
q) In the **First Node Configuration** screen, select **Yes**.
r) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.

Important Proper NTP configuration is essential.

s) In the **Security Configuration** screen, enter the security password and select **OK**.
t) In the **SMTP Host Configuration** screen, select **No**.

Finesse does not have this step.

u) Unified Communications Manager only: On the **Smart Call Home Enable** screen, select **Disable All Call Home on System Start**.
v) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
w) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

Step 5 Unmount the ISO image.

Cisco Unified Intelligence Center License

Acquire License

Procedure

Step 1 Go to the following URL:

https://software.cisco.com/download/home/282163829/type/282377062/release/11.5%25281%2529

Step 2 Download the **CUIC_Premium.lic** file.
Step 3 Save the license file in a location where the System Application User can access it.

Configure the Cluster for Cisco Unified Communications Manager

Procedure

Step 1 Launch Unified Communications Manager Publisher in a browser (https://<IP Addr of CUCM Publisher>/ccmadmin).

Step 2 Select **System** > **Server** > **Add New**.

Step 3 On the Server Configuration page, select **CUCM Voice/Video** for the **Server Type**. Click **Next**.

Step 4 On the Server Configuration page, enter the IP Address of the subscriber.

Step 5 Click **Save.**

Create a Unified Communications Manager AXL User Account

Create a Unified Communications Manager AXL user in Unified Communications Manager Administration. First create an Access Control Group with Standard AXL API Access, and then create an Application User with permission for that Access Control Group.

Procedure

Step 1 Launch Unified Communications Manager Administration in a browser (`https://<IP Address of Unified Communications Manager Publisher>/ccmadmin`).

Step 2 Create an Access Control Group, as follows:

a) Navigate to **User Management** > **User Settings** > **Access Control Group**.
b) Click **Add New**.
c) Enter a name for the Access Control Group.
d) Click **Save**.

The **Access Control Group Configuration** page opens.

e) From the **Related Links** drop-down menu, select **Assign Role to Access Control Group** and click **Go**.
f) Click **Assign Role to Group**.

The **Find and List Roles** popup window opens.

g) Click **Find**.
h) Check the **Standard AXL API Access** check box.
i) Click **Add Selected**.
j) Click **Save**.

Step 3 Create an Application User, as follows:

a) Navigate to **User Management** > **Application User**.

b) Click **Add New**.
c) Enter a name and password for the Application User.
d) In the **Permissions Information** section, click **Add to Access Control Group**.

The **Find and List Access Control Group** popup window opens.

e) Click **Find**.
f) Check the check box for the Access Control Group you created.
g) Click **Add Selected.**
h) Click **Save**.

Configure the Cluster for Cisco Unified Intelligence Center

Procedure

Step 1 Direct a browser to the URL `https://<hostmame>:8443/oamp`, where <*hostname*> is the hostname of your Cisco Unified Intelligence Center publisher.

Step 2 Sign in using the system application user ID and password that you defined during installation.

Step 3 From the section in the left, select **Device Configuration**.

Step 4 Click **Add Member**.

Step 5 On the Device Configuration fields for the Subscriber, enter a name, the hostname or IP address , and a description for the device.

Note All CUIC Subscribers must be entered here before you can install the software.

Step 6 After you complete the cluster configuration, restart the publisher.

Note For 2000 Agents deployment, the system updates the Live Data failover settings.

Configure the Cluster for Cisco Finesse

Procedure

Step 1 Launch the Cisco Finesse primary node in a browser (`https://<FQDN of Finesse Primary node>/cfadmin`).

If you are using an IPv6 client, you must include the port number in the URL (https://<*FQDN of Finesse Primary node*>:8445/cfadmin).

Step 2 Go to **Home > Cluster Settings**. (This path is based on the default configuration and assumes that you have not changed the page for the Cluster Settings gadget.)

Step 3 Add the hostname for the Cisco Finesse secondary node.

Step 4 Click **Save**.

Step 5 Restart Cisco Finesse Tomcat as follows:

a) To stop the Cisco Finesse Tomcat service, enter this CLI command: **utils service stop Cisco Finesse Tomcat** .

b) To start the Cisco Finesse Tomcat service, enter this CLI command: **utils service start Cisco Finesse Tomcat** .

Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications

Note This task is required for installation of the subscriber/secondary nodes of the three VOS-based contact center applications: Cisco 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 you are installing Finesse or Unified Communications Manager, select **OK**.
- If you are installing Unified Intelligence Center, select **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center, Live Data, and Cisco Identity Service (IdS) on the same server.

Step 5 Follow the Install wizard, making selections as follows:

a) In the **Proceed with Install** screen, select **Yes**.

b) In the **Platform Installation Wizard** screen, select **Proceed**.
c) In the **Apply Patch** screen, select **No**.

Finesse does not have this step.

d) In the **Basic Install** screen, select **Continue**.
e) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

Note For Live Data servers, use the same timezone for all the nodes.

f) In the **Auto Negotiation Configuration** screen, select **Continue**.
g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.

Finesse does not have this step.

i) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
j) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.

Important DNS client configuration is mandatory for Finesse. If you do not perform this step, agents cannot sign in to the desktop and you must reinstall Finesse.

k) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
l) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
m) In the **First Node Configuration** screen, select **No**.
n) In the warning screen, select **OK**.
o) In the **Network Connectivity Test Configuration** screen, select **No**.
p) In the **First Node Access Configuration** screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select **OK**.
q) In the **SMTP Host Configuration** screen, select **No**.

Finesse does not have this step.

r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

- There is a reboot in the middle of the installation.
- For Cisco Unified Intelligence Center, you see a **Product Licensing** screen that shows the URL for obtaining the license and the Media Access Control (MAC) address. Write down the MAC address. You need this information for the license application.
- The installation ends at a sign-in prompt.

Step 6 Unmount the ISO image.

Unified Communications Manager License

Generate and Register License

Procedure

Step 1 Launch Unified Communications Manager in a browser (`https://<IP Address of Unified CM Publisher>`).

Step 2 Click **Cisco Prime License Manager** and navigate to **Licenses** > **Fulfillment**.

Step 3 Under **Other Fulfillment** options, click **Generate License Request**.

Step 4 When the **License Request and Next Steps** window opens, copy the text (PAK ID).

Step 5 Click the **Cisco License Registration** link.

Step 6 Sign in and click **Continue to Product License Registration**.

Step 7 In the **Enter a Single PAK or Token to fulfill** field, paste your PAK ID and click **Fulfill Single PAK/Token**.

You receive the license file in an email message.

Install License

Procedure

Step 1 Unzip the license file from the email message.

Step 2 Under Other Fulfillment Options, select **Fulfill Licenses from File**.

Step 3 Click **Browse** and locate your license file.

Step 4 Click **Install** and close the popup window.

Step 5 Navigate to **Product Instances**. Then click **Add**.

Step 6 Fill in the name, hostname/IP address, username, and password for your Cisco Unified Communications Manager Publisher.

Step 7 Select Product type of Unified CM.

Step 8 Click **OK**.

Step 9 Click **Synchronize Now**.

Activate Services

Complete the following procedure to activate services.

Procedure

Step 1 Open Cisco Unified CM Administration at `https://<IP Address of the CUCM Publisher>/ccmadmin`.

Step 2 Select Cisco Unified Serviceability from the **Navigation** menu and click **Go**.

Step 3 Select **Tools** > **Service Activation**.

Step 4 From the Server drop-down list, choose the server on which you want to activate the service, and then click **Go**.

Step 5 For the Publisher, check the following services to activate and click **Save**:

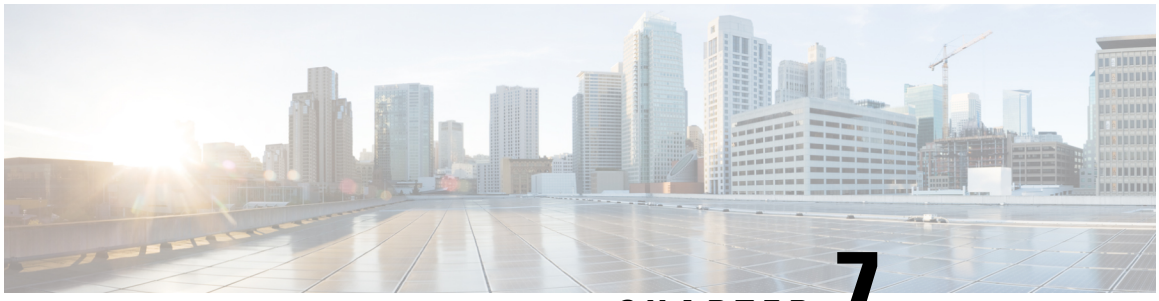
- Cisco CallManager
- Cisco IP Voice Media Streaming App
- Cisco CTIManager
- Cisco Tftp
- Cisco Bulk Provisioning Service
- Cisco AXL Web Service
- Cisco Serviceability Reporter
- Cisco CTL Provider
- Cisco Certificate Authority Proxy Function
- Cisco Dialed Number Analyzer Server

Step 6 For the Subscribers, check the follow services to activate and click **Save**:

- Cisco CallManager
- Cisco IP Voice Media Streaming App
- Cisco CTIManager
- Cisco AXL Web Service
- Cisco CTL Provider
- Cisco Dialed Number Analyzer Server

PART III

Configuration



CHAPTER 7

Configure Cisco Unified Contact Center Enterprise Rogger and Cisco Unified Contact Center Enterprise AW-HDS-DDS

Configure SQL Server for CCE Components

Configure SQL Server on both the Unified CCE Rogger and the Unified CCE AW-HDS-DDS.

Procedure

Step 1 Click the **Windows Start** icon, and then select the Downward Arrow icon to display all applications.

Step 2 Open **Microsoft SQL Server Management Studio**.

Step 3 Log in.

Step 4 Expand **Security** and then **Logins**.

Step 5 If the BUILTIN\Administrators group is not listed:

a) Right-click **Logins** and select **New Login**.
b) Click **Search** and then **Locations** to locate BUILTIN in the domain tree.
c) Type **Administrators** and click **Check Name** and then **OK**.
d) Double-click **BUILTIN\Administrators**.
e) Choose **Server Roles**.
f) Ensure that **public** and **sysadmin** are both checked.

Configure the Domain Manager

DO THIS ONCE on the first Unified CCE Rogger that you configure.

Important You must create the Cisco Root OU in the same domain to which the Unified CCE servers belong.

Procedure

Step 1 Log in to the system as a user who has permissions to create organizational units (OUs) in the domain.

Step 2 Click the **Windows Start** icon, and then select the Downward Arrow icon to display all applications.

Step 3 Select the **Domain Manager** icon from the list of applications.

Step 4 In the section on the left, expand the domain.

Step 5 Add the Cisco root as Cisco_ICM:

a) Under the Cisco root, click **Add**.
b) Select the **OUs** under which you want to create the Cisco root OU and click **OK**.

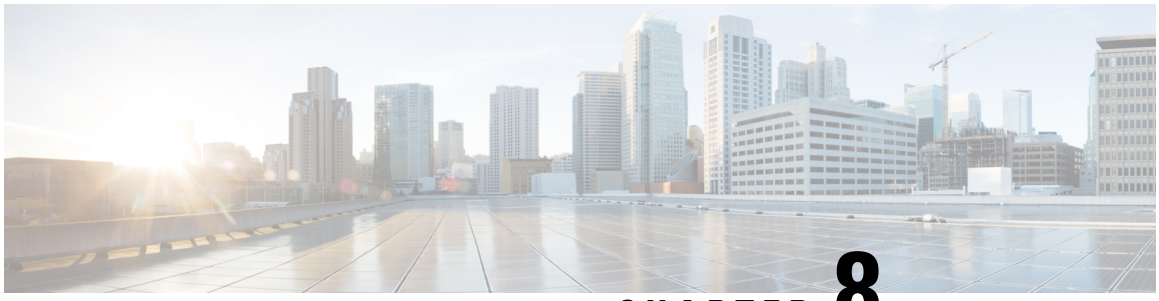
Step 6 Add the facility organizational unit (OU):

a) In the right section, under **Facility**, click **Add**.
b) Enter the name for the **Facility** and click **OK**.

Step 7 Add the Instance OU:

a) In the right section, under , click **Add**.
b) Enter the instance name and click **OK**.

Step 8 Click **Close**.



CHAPTER 8

Initialize Cisco Packaged Contact Center Enterprise Deployment

Initialize the Packaged CCE 2000 Agents Deployment Type

When you sign into Unified CCE Administration for the first time, you are prompted to enter information and credentials for the components in your deployment. Packaged CCE uses this information to configure the components and build the System Inventory.

Note After a Packaged CCE deployment is initialized, you cannot switch to another deployment type.

Note The system does not support IP address change. This is applicable for all the **Hostname/ IP Address** fields.

Procedure

Step 1 Sign into **Unified CCE Administration** using the Active Directory username (*user@domain*) and password (`https://<IP Address>/cceadmin`, where <IP Address> is the address of the Side A Unified CCE AW-HDS-DDS).
The **Configure your deployment** popup window opens automatically.

Step 2 On the **Deployment** page , select a **Deployment Type** and an **Instance** from the respective drop-down lists. You must be a member of the Setup security group for the instance you select. Click **Next**.

Step 3 On the **VM Host** page, enter the IP address, Username, and Password for the VMware hosts for Side A and Side B.

The VMware hosts are the two servers on which ESXi is installed. The username and password fields are the host login names and passwords configured in ESXi.

- If you do not want to use the "root" user credentials. You can create user with the following permissions:

Users must have *Read* and *Reboot* permissions on the hosts. To enable these permissions in the VMware Host Client, set the following in **Manage Permissions**:

- *Anonymous*, *View*, and *Read* in **Root** > **System** (enabled by default).
- *Reset* in **Root** > **VirtualMachine** > **Interact**.

Note If you update the ESXi root password in Packaged CCE 2000 agent deployment, be sure to reinitialize the deployment in the Inventory page.

Note The following step is applicable only if you have installed Packaged CCE 11.6(1) ES27 patch. Else, click **Next** to continue on the **Credentials** page.

Step 4 Select the hardware layout type as **M3/M4 Tested Reference Configuration** or **M5 Tested Reference Configuration / Specification Based Configuration** and click **Next**.

Packaged CCE validates the hosts in your deployment.

- If you select **M3/M4 Tested Reference Configuration**, the system checks if the hardware is supported UCS hardware and verifies if the VMs are configured as per the reference design. If the validation is successful, the **Credentials** page opens.
- If you select **M5 Tested Reference Configuration / Specification Based Configuration**, the system validates the hardware specifications of the VMware host and verifies if the VMs are configured as per the reference design. If the validation is successful, click **Next** to open the **Credentials** page. See the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html for hardware specifications.

Note

- Datastores used by Cisco VMs should not be shared or used by other third-party VMs.
- Packaged CCE core components include:
  - Unified CCE Rogger
  - Unified CCE AW/HDS/DDS
  - Unified CCE PG
  - Unified CVP Server
  - Unified CVP OAMP Server
  - Unified Intelligence Center Publisher
  - Finesse

  VM annotations are used to identify Packaged CCE core component VMs. Do not change the default annotations of any of the core component VMs. The following terms are reserved for core component annotations: Cisco, Finesse, CUIC, and CVP. Do not use these reserved terms in the annotations of any of the non-core component VMs.
- Core components must be on-box, all other components have to be added as external machines. For more information, see the *Add External Machines* topic in the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide, Release 11.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html
- All other non-core components are required to be added as an external machine in the Packaged CCE Inventory.

- If the validation fails, click **Update Hosts** to go back to the **VM Hosts** page and edit the values. Click **Retry** to run the validation with existing values.

Step 5 On the **Credentials** page, enter the specified information for each component in your deployment. After entering information for a component, click **Next**.

The system validates the credentials you entered before prompting you for the next component's information.

Component	Information Required
Unified CM	Either: • The Unified CM Publisher for an on-box Unified Communications Manager deployment. • The Unified CM Publisher Name and IP address for an external Unified Communications Manager deployment. **Note** • Only a single Unified CM cluster can be integrated to a single site of Packaged CCE deployment. AXL username and password.

Component	Information Required
Unified CVP	Unified CVP Web Services manager CLI username and password. Unified CVP Operations Console username and password.
Unified CCE AW-HDS-DDS	Unified CCE Diagnostic Framework Portico domain, username, and password. These credentials must be of a domain user who is a member of the Config security group for the instance, and valid on all Unified CCE components in your deployment (the Side A and Side B Unified CCE Roggers, PGs, and AW-HDS-DDSs). **Note** Every time the Active Directory credentials are updated, the credentials configured here must be updated as well.
Unified Intelligence Center	Unified Intelligence Center Administration application username and password. Identity Service Administration username and password.
Finesse	Finesse Administration username and password.

Step 6 On the **Settings** page, select the following:

- Select the codec used for Mobile Agent calls from the **Mobile Agent Codec** drop-down menu. The codec you select must match the codec specified on the voice gateways.
- If you have an external Unified Communications Manager, select the Unified CM Subscribers to which the Side A and Side B Unified CCE PGs connect from the **Side A Connection** and **Side B Connection** drop-down menus.
- Enter the username and password for an existing Active Directory user in the same domain as the Packaged CCE servers. This account will be added to the Service group.

Click **Next**.

The deployment is initialized. The **Details** dialog box displays the status of the automated initialization tasks.

See Automated Initialization Tasks for Components, on page 75 for more information.

Step 7 After the automated initialization tasks complete, click **Done**. The **System Inventory** opens.

If one of the automated initialization tasks fails, correct the errors and then click **Retry**.

If the retry is successful, the automated initialization continues.

For some task failures, all completed tasks must be reverted before the task can be retried. You see a message informing you that the system needs to be reverted to a clean state.

Click **OK**, and then after the system is in a clean state, click **Start Over**.

Note The System Inventory displays alerts for some machines when it opens after initialization completes and you click **Done**. These alerts will be cleared after you configure Unified Communications Manager.

Related Topics

Create a Unified Communications Manager AXL User Account, on page 60
Configure Cisco Unified Communications Manager, on page 97

Automated Initialization Tasks for Components

Packaged CCE performs the following tasks during initialization.

Component	Automated Initialization Tasks
Unified CCE Rogger	• Creates the Logger. • Creates the Router.
Unified CCE PG	• Downloads JTAPI from the Unified Communications Manager, and installs it on the Unified CCE PG. • Creates the CUCM Peripheral Gateway (PG) with the CUCM PIM. • Creates the Media Routing PG (MR PG). • Creates the VRU PG with two VRU PIMs. • Creates the CTI Server.
Unified CCE AW-HDS-DDS	• Creates the AW-HDS-DDS. • Creates the Cisco Unified Intelligence Center SQL user account that is used for Unified Intelligence Center data sources. • Creates the Cisco Finesse SQL user account that is used for Cisco Finesse data sources.
Unified Communications Manager	• Creates the Application User that is used to configure the Unified CCE PG.
Unified Customer Voice Portal	• Configures the Unified CVP Call Servercomponents. • Configures the Unified CVP VXML Server components. • Configures the Unified CVP Media Server components. • Configures the Unified CVP Reporting Server components, if used.
Unified Intelligence Center	• Creates the historical and real-time data sources.
Cisco Finesse	• Configures the CTI Server settings. • Configures the connection to the AW database. • Disables the **Reasons** gadget in Finesse Administration.

Set System-Level Settings

After you have configured the Packaged CCE deployment, you can specify system-level settings. For example, you can enter labels for Unified Communications Manager, Unified CVP, and outbound calls.

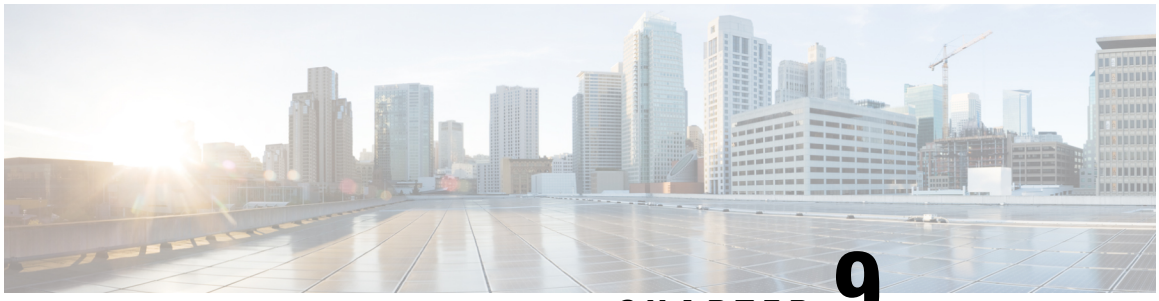
See the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-maintain-and-operate.html for more information about system settings.

Procedure

Step 1 In Unified CCE Administration, navigate to **System** > **Settings**.

Step 2 Specify system-level settings on the **General**, **Agents**, **Call Reporting**, and **Labels** tabs.

Step 3 Click **Save**.



CHAPTER 9

Configure Cisco Unified Contact Center Enterprise PG

Cisco Unified Contact Center Enterprise PG Configuration

This chapter contains the configuration procedures you must perform for the Unified CCE PGs on Side A and Side B.

Add PIMs to the Media Routing Peripheral Gateway

The Media Routing Peripheral Gateway (MR PG) is created during automated initialization.

Creating PIMs for the MR PG is optional. You can create up to four PIMs on the Media Routing Peripheral Gateway:

- Outbound PIM
- Multichannel PIM for SocialMiner
- Multichannel PIM for Enterprise Chat and Email (ECE)
- Multichannel PIM for a third-party multichannel application

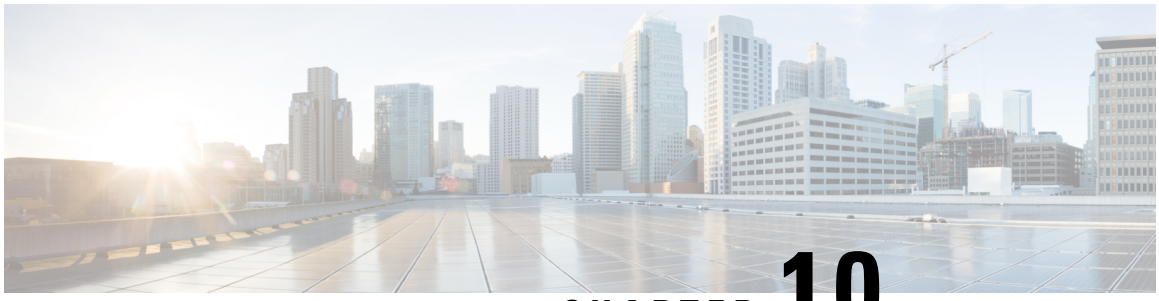
To create Dialed Numbers associated with the Multichannel PIMs, first do the following:

- Create the PIM using Peripheral Gateway Setup.
- Add an external machine in the Solution Inventory using the Unified CCE Administration System. Navigate to **System** > **Deployment** . Scroll down and click **Add Machine** .

Note If ECE is deployed on box, you do not need to create a Dialed Number associated with the PIM.

Note Refer to the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/en/US/products/ps12586/prod_maintenance_guides_list.html for directions on adding the Outbound PIM and the Multichannel PIMs.

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



CHAPTER 10

Configure Cisco Unified Customer Voice Portal

Cisco Unified Customer Voice Portal Configuration

This chapter explains the procedures you must perform to configure the Cisco Unified CVP servers and OAMP servers.

Sign in to your Unified CVP Operations console with your Unified CVP administrator account (https://<ServerIP>:9443/oamp), where ServerIP is the IP address or hostname.

Configure Gateways

Note If you are using Internet Explorer 11, you must add the Unified CVP Operations Console URL to Internet Explorer's list of Compatibility View websites in order to use the Operations Console. Compatibility View settings are available from Internet Explorer's **Tool** menu.

Procedure

Step 1 In the Unified CVP Operations Console, navigate to **Device Management** > **Gateway**.

Step 2 Click **Add New**.

Step 3 On the General tab, configure as follows:

a) Enter the IP address.

b) Enter the hostname.

c) Choose the Device Type.
d) In the Username and Passwords pane, enter the username, password, and enable password.

Step 4 Click **Test Sign-in** to verify that a connection with the gateway can be established and that the credentials are correct.

Step 5 Click **Save**.

Step 6 Repeat for every gateway.

Transfer Unified CVP Scripts and Media Files

Create the notification destination and deploy to all of the Unified CVP devices.

Procedure

Step 1 Log in to the Operations Console and select **Bulk Administration** > **File Transfer** > **Scripts and Media**.

Step 2 In the **Select device type** field, select the Gateway.

Step 3 Move all Gateways to **Selected**.

Step 4 Select **Default Gateway files**.

Step 5 Select **Transfer**, and then select **OK** on the popup window.

If you have separate Ingress and VXML gateways, you must select the appropriate files and script for each component.

Step 6 Click **File Transfer Status** to monitor transfer progress.

Unified Customer Voice Portal Licenses

Generate a License

Before you begin

Access the product authorization key (PAK) that you received with the Unified CVP software.

Procedure

Step 1 Sign in to the Product License Registration Portal at https://tools.cisco.com/SWIFT/LicensingUI/Home.

Step 2 Click **Continue to Product License Registration**.

Step 3 In the **Get New Licenses** field, enter your PAK.

You can enter up to 10 PAKs, separated by commas.

Step 4 Click **Fulfill**.

Step 5 Select your features and enter the quantity.

Step 6 In the **Serial Number** field, enter the following:

- For a Unified CVP Server or Unified CVP Reporting Server, enter the IP address.
- For Unified Call Studio, enter the MAC address.

Step 7 Click **Next**.

Step 8 Accept the terms of the License Agreement, enter your Recipient Information, and click **Submit**.

Your request is processed.

Step 9 Click **Download** to download your license.
Your license is also sent to you by email.

What to do next

Ensure that the license file is named as `cvp.license`.

Copy the license file to `C:\Cisco\CVP\conf\license`. Shut down gracefully and then restart each of the Call Server components for the new license to take effect.

Transfer License Files for Unified CVP Server

Procedure

Step 1 In the Unified CVP Operations Console, navigate to **Bulk Administration** > **File Transfer** > **Licenses**.

Step 2 Click **Browse** to choose your license file to upload.

Step 3 Click **Transfer**. Then click **OK** at the message asking if you are sure.

Step 4 Click **File Transfer Status**.

Step 5 Confirm that each of the File Transfers shows "Success" in the Status column.

Step 6 Navigate to **System** > **Control Center**.

Step 7 Shut down gracefully and then start each of the Call Server components in the list.

This allows the new licensing to take effect.

Configure SNMP

Note This is optional. For more information, see Configure SNMP, on page 81

Procedure

Step 1 In the Unified CVP Operations Console, navigate to **SNMP** > **V1/V2c** > **Community String** .

Step 2 Click **Add New**.

a) On the **General** tab, name the community string.
b) On the **Devices** tab, select the required device from the list of available devices.
c) Click **Save and Deploy**.

Step 3 Create the notification destination and deploy to all of the Unified CVP devices.

a) Navigate to **SNMP** > **V1/V2c** > **Notification Destination**.
b) Click **Add New**.
c) Complete the fields.
d) Select the **Devices** tab and assign the SNMP notification destination to a device.
e) Click **Save and Deploy**.

Configure SIP Server Groups

SIP Server Groups are required for Cisco Unified Communications Manager and Gateways.

Procedure

Step 1 In the Unified CVP Operations Console, navigate to **System** > **SIP Server Group**.

Step 2 Create a server group for the Cisco Unified Communications Manager devices:

a) On the General tab, click **Add New**.
b) Fill in the **SRV Domain Name FQDN** field with a value that will also be used in the Cluster FQDN setting in Enterprise Parameters in Communications Manager. For example, cucm.cisco.com.
c) In the **IP Address/Hostname** field, enter an IP address or hostname for a Unified Communications Manager subscriber.
d) Click **Add**.
e) Repeat Steps c and d for each Unified Communications Manager subscriber. Click **Save**.

Note Do not put the Publisher node in the server group.

SIP server group for Communications Manager is not required for Small Contact Center (SCC) deployment as there is no direct SIP trunk created from Communications Manager to CVP in SCC model.

The FQDN should match the FQDN configured in the Cluster FQDN setting that will be configured in Enterprise Parameters on the Cisco Unified Communications Manager. See Configure Fully Qualified Domain Name, on page 97

Step 3 Create a server group for the gateway devices:

a) On the General tab, click **Add New**.
b) In the **SRV Domain Name FQDN** field, enter the SRV Domain Name FQDN. For example vxmlgw.cisco.com.

c) In the **IP Address/Hostname** field, enter an IP address or hostname for a VXML gateway in the deployment.
d) Click **Add**.
e) Repeat Steps c and d for each VXML gateway as appropriate for the deployment and branches. Click **Save**.

Adding all VXML gateways to the server group will load balance calls across all the member server group gateways.

Step 4 Associate these server groups to all Unified CVP Call Servers:

a) On the **Call Server Deployment** tab, move all Unified CVP Call Servers from the **Available** list to the **Selected** list.
b) Click **Save and Deploy**.

Configure Dialed Number Patterns

Dialed number patterns are required for:

- Agent Device
- Network VRU
- Ringtone
- Error

Procedure

Step 1 In the Unified CVP Operations Console, navigate to **System** > **Dialed Number Pattern**.

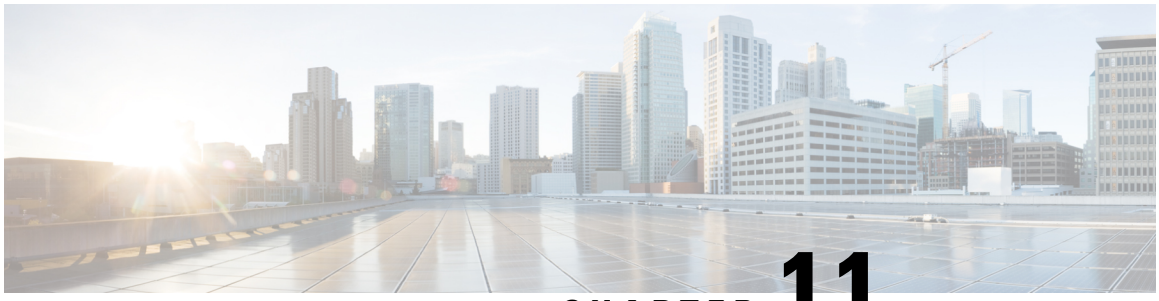
Step 2 For each dialed number pattern in the following table:

a) Click **Add New**.
b) In the **Dialed Number Pattern** field, enter the dialed number pattern.
c) In the **Description** field, enter a description for the dialed number pattern.
d) In the **Dialed Number Pattern Types** pane, check the specified dialed number pattern types.
e) Click **Save**.

Step 3 After you configure all dialed number patterns, click **Deploy**.

Step 4 Click **Deployment Status** to make sure that you applied the configuration.

Dialed number pattern	Description	Dialed number pattern types
91*	Ringtone	Check **Enable Local Static Route**. Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example, vxmlgw.cisco.com). Check **Enable Send Calls to Originator**. **Note** You must use 91* for the Ringtone dialed number pattern. Packaged CCE does not support using a different Ringtone dialed number pattern.
92*	Error	Check **Enable Local Static Route**. Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example, vxmlgw.cisco.com). Check **Enable Send Calls to Originator**. **Note** You must use 92* for the Error dialed number pattern. Packaged CCE does not support using a different Error dialed number pattern.
The agent extension pattern. For example, enter 500* where the range of agent extensions is 5001 to 500999.	Agent Device.	Check **Enable Local Static Route**. Route to SIP Server Group and IP Address/Hostname/Server Group Name are both the Unified Communications Manager gateway. Check **Enable RNA Timeout for Outbound Calls**. The default timeout value is 60 seconds.
777*	Network VRU Label	Check **Enable Local Static Route**. Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example vxmlgw.cisco.com). Check **Enable Send Calls to Originator**.



CHAPTER 11

Cisco Unified Customer Voice Portal Reporting Server Configuration

This chapter contains the configuration procedures you must perform to configure the optional Unified Customer Voice Portal Reporting Server on Side B.

The Unified CVP Reporting VM is required for customers who use Courtesy Callback and who want to run Unified CVP call and application reports.

Transfer License File for the Unified CVP Reporting Server

Before you begin

You must generate a license file before transferring the file to the Unified CVP Reporting Server. See Generate a License, on page 80.

Procedure

Step 1 In the Operations Console, navigate to **Device Management** > **Unified CVP Reporting Server**.

Step 2 Click the link for the Unified CVP Reporting Server.

Step 3 From the toolbar, click **File Transfer** > **Licenses**.

The File Transfer page appears listing the Host name and IP address for the selected Unified CVP Reporting Server.

Step 4 From **Select From Available License Files**, select the license file, and then click **Select**.

Note If the license file is not listed in the **Select From Available License Files** text box, click **Select a License File from Your Local PC** and enter the filename in the text box or click **Browse** to search the license file on the local file system.

Step 5 Click **Transfer**.

Step 6 Select and restart the Unified CVP Reporting Server through the Operations Console (**System** > **Control Center**).

Step 7 If you have installed a second Unified CVP Reporting Server, repeat this procedure for that component.

Obtain Cisco Unified Customer Voice Portal Report Templates

To import Unified CVP report templates complete the following:

Procedure

Step 1 On the Unified CVP Reporting Server, click **Start**.

Step 2 In the search box, type **%CVP_HOME%\CVP_Reporting_Templates** and press **Enter**.

Step 3 Compress the reports into a zip folder and copy it to the system from which you will run Unified Intelligence Center Administration.

Create Data Source for Cisco Unified CVP Report Data

Perform the following procedure to create a data source.

Procedure

Step 1 Log in to the Unified Intelligence Center at `https://<hostname/ IP address of CUIC Publisher>:8444/cuicui`.

Step 2 Select the **Data Sources** drawer to open the Data Sources page.

Step 3 Click **New** to open New Data Source window.

Step 4 Complete fields on this page as follows:

Field	Value
Name	Enter the name of this data source. Report Designers and Report Definition Designers do not have access to the Data Sources page but can see the list of Data Sources when they create custom reports. To benefit those users, give a new Data Source a meaningful name.
Description	Enter a description for this data source.
Data Source Type	Choose **Informix**. **Note** Type is disabled in Edit mode.
Host Settings	

Field	Value
Database Host	Enter the IP address or hostname for the Unified CVP Reporting server.
Port	Enter the port number. Typically, the port is 1526. You may have to open this port in the CVP Reporting Server firewall (Windows Firewall > Advanced Settings > Inbound rules > new rule).
Database Name	Enter the name of the reporting database on the Unified CVP reporting server. The database name can be `cvp_data` or `callback`.
Instance	Specify the instance name of the desired database. By default, this is `cvp`.
Timezone	Choose the correct time zone for the data stored in the database. In locations that change from Standard Time to Daylight Savings Time, this time zone is updated automatically. **Note** Set CVP datasource timezone configuration to UTC on CUIC.
Authentication Settings	
Database User ID	Enter the user ID of the Reporting User who is configured in the Operations Console to access the Unified CVP reporting database. (The cvp_dbuser account is created automatically during Unified CVP Reporting server installation.)
Password and Confirm Password	Enter and confirm the password for the database user.
Charset	Choose UTF-8.
Default Permissions	View or edit the permissions for this datasource for My Group and for the All Users group.
Max Pool Size	Select the maximum pool size. Value ranges from 5-200. The default Max Pool Size value is 100 and is common for both the primary and secondary data source tabs.

Step 5 Click **Test Connection**.

If the status is not Online, review the error message to determine the cause and edit the data source accordingly.

Step 6 Click **Save** to close the Add Data Source window.

The new data source appears on the Data Sources list.

Import Unified CVP Report Templates in Unified Intelligence Center

You can import a report (XML) and the associated template help file (ZIP format) into Cisco Unified Intelligence Center.

Procedure

Step 1 Launch the Unified Intelligence Center web application at `https://<Hostname/IP Address of CUIC Publisher>:8444/cuic`

Step 2 From the left navigation pane, click **Reports**.

Step 3 On the Reports toolbar, click **New** > **Import**.
You will be redirected to the legacy interface.

Step 4 Navigate to the folder where you want to import the report.

Note If you are importing a stock report bundle from Cisco.com, it must be placed at the Reports folder level.

Step 5 Click **Import Report**.

Step 6 In the **File Name (XML or ZIP file)** field, click **Choose File**.

Step 7 Browse to and select the XML or the compressed report file, and click **Open**.

Step 8 From the **Data source for ReportDefinition** drop-down list, select a data source used by the report definition.

Note This field appears only if the Report Definition for the report being imported is not currently defined in Unified Intelligence Center.

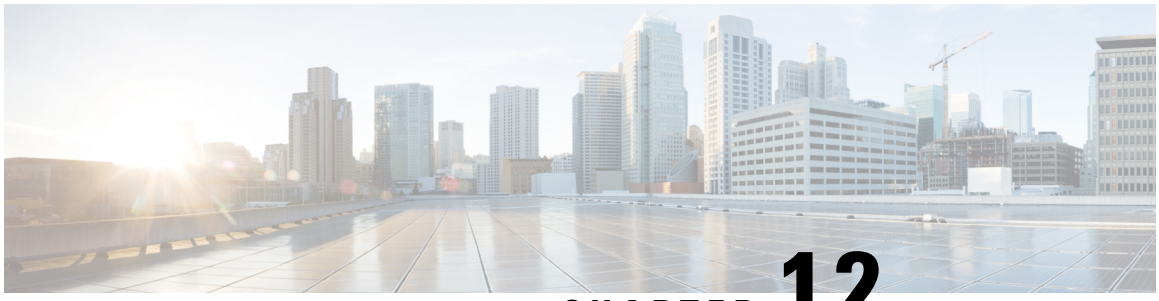
Step 9 From the **Data Source for ValueList** drop-down list, select the data source used by the value lists defined in the report definition.

Note You have to select a data source for the value list only if it does not use the same data source as the Report Definition. For Report Definitions of Real Time Streaming, it is mandatory to select a data source for the Value Lists.

Step 10 In the **Save To** field, browse to the folder where you want to place the imported report. Use the arrow keys to expand the folders.

Step 11 Click **Import**.

Note Importing a report to a different version of Unified Intelligence Center is not supported. However, when you upgrade Unified Intelligence Center, report templates continue to work in the upgraded version.



CHAPTER 12

Configure Cisco IOS Enterprise Voice Gateway

About Ingress and VXML Gateway Configuration

Complete the following procedures to configure the Ingress Gateway and VXML Gateway. Instructions are applicable to both TDM and Cisco Unified Border Element (CUBE) Voice gateways, unless otherwise noted.

You may also have Cisco Virtualized Voice Browser (Cisco VVB) as part of your deployment. For information about Cisco VVB, see Install and Configure Cisco Virtualized Voice Browser, on page 137.

Note Complete all configuration steps in **enable** > **configuration terminal** mode.

Common Configuration for the Ingress Gateway and VXML Gateway

```
logging buffered 2000000 debugging
no logging console
service timestamps debug datetime msec localtime
ip routing
ip cef
ip source-route
interface GigabitEthernet0/0
     ip route-cache same-interface
     duplex auto
     speed auto
     no keepalive
     no cdp enable

voice service voip
          ip address trusted list
```

```
     ipv4 0.0.0.0 0.0.0.0 # OR an explicit Source IP Address Trust List
allow-connections sip to sip
signaling forward unconditional
```

Configure Ingress Gateway

Procedure

Step 1 Configure global settings.

```
voice service voip
  allow-connections sip to sip
 signaling forward unconditional
 # If this gateway is being licensed as a Cisco UBE the following lines are also required
 mode border-element
 ip address trusted list
  ipv4 0.0.0.0 0.0.0.0               # Or an explicit Source IP Address Trust List
sip
  rel1xx disable
  header-passing
  options-ping 60
  midcall-signaling passthru
```

Step 2 Configure voice codec preference:

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

Step 3 Configure default services:

```
#Default Services
application
     service survivability flash:survivability.tcl
```

Step 4 Configure gateway and sip-ua timers:

```
gateway
 media-inactivity-criteria all
 timer receive-rtp 1200

sip-ua
 retry invite 2
 retry bye 1
 timers expires 60000
 timers connect 1000
 reason-header override
```

Step 5 Configure POTS dial-peers:

```
# Configure Unified CVP survivability
dial-peer voice 1 pots
     description CVP TDM dial-peer
     service survivability
     incoming called-number .T
     direct-inward-dial
```

Note This is required for TDM gateways only.

Step 6 Configure the switch leg:

```
#Configure the Switch leg where
# preference is used to distinguish between sides.
# max-conn is used prevent overloading of Unifed CVP
# options-keepalive is used to handle failover
# Note: the example below is for gateways located on the A-side of a geographically
#distributed deployment
# Note: Ensure that you configure switch dial-peers for each Unified CVP server.

dial-peer voice 70021 voip
     description Used for Switch leg SIP Direct
     preference 1
     max-conn 225
     destination-pattern xxxx..... #Customer specific destination pattern
     session protocol sipv2
     session target ipv4:###.###.###.###     #IP Address for Unified CVP, SideA
     session transport tcp
     voice-class codec 1
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     no vad

dial-peer voice 70022 voip
     description Used for Switch leg SIP Direct
     preference 2
     max-conn 225
     destination-pattern xxxx..... #Customer specific destination pattern
     session protocol sipv2
     session target ipv4:###.###.###.###    #IP Address for Unified CVP, SideB
     session transport tcp
     voice-class codec 1
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     no vad
```

Step 7 Configure the hardware resources (transcoder, conference bridge, and MTP):

Note This configuration section is unnecessary for virtual CUBE or CSR 1000v Gateways. They do not have physical DSP resources.

```
#For gateways with physical DSP resources, configure Hardware resources using
#Unified Communications Domain Manager.

# Configure the voice-cards share the DSP resources located in Slot0
voice-card 0
     dspfarm
     dsp services dspfarm
voice-card 1
     dspfarm
     dsp services dspfarm
voice-card 2
     dspfarm
     dsp services dspfarm
voice-card 3
     dspfarm
     dsp services dspfarm
voice-card 4
     dspfarm
     dsp services dspfarm

# Point to the contact center call manager
sccp local GigabitEthernet0/0
     sccp ccm ###.###.###.### identifier 1 priority 1 version 7.0 # Cisco Unified CM sub 1
```

```
     sccp ccm ###.###.###.### identifier 2 priority 2 version 7.0 # Cisco Unifed CM sub 2

# Add a SCCP group for each of the hardware resource types
sccp ccm group 1
     associate ccm 1 priority 1
     associate profile 2 register <gatewaynamemtp>
     associate profile 1 register <gatewaynameconf>
     associate profile 3 register <gatewaynamexcode>

# Configure DSPFarms for Conference, MTP and Transcoder

dspfarm profile 1 conference
     codec g711ulaw
     codec g711alaw
     codec g729r8
     maximum sessions 24
     associate application SCCP

dspfarm profile 2 mtp
     codec g711ulaw
     codec g711alaw
     codec g729r8
     maximum sessions software 500
     associate application SCCP

dspfarm profile 3 transcode universal
     codec g711ulaw
     codec g711alaw
     codec g729r8
     maximum sessions 52
     associate application SCCP
```

Step 8 Optional, configure the SIP Trunking:

```
# Configure the resources to be monitored
voice class resource-group 1
     resource cpu 1-min-avg threshold high 80 low 60
     resource ds0
     resource dsp
     resource mem total-mem
     periodic-report interval 30

# Configure one rai target for each CVP Server
sip-ua
     rai target ipv4:###.###.###.### resource-group1 # CVPA
     rai target ipv4:###.###.###.### resource-group1 # CVPB
     permit hostname dns:%Requires manual replacement - ServerGroup Name defined in
CVP.System.SIP Server Groups%
```

Step 9 Configure incoming PSTN SIP trunk dial peer:

```
dial-peer voice 70000 voip
     description Incoming Call From PSTN SIP Trunk
     service survivability
     incoming called-number xxxx……    # Customer specific incoming called-number pattern
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     session protocol sipv2
     voice-class codec 1
     no vad
```

Note This is required for CUBE only.

Configure VXML Gateway

Before you begin

Note If you have configured VVB, it is not mandatory to configure VXML Gateway. You may configure either VVB or VXML Gateway, or configure both.

Procedure

Step 1 Configure global settings:

```
voice service voip
  allow-connections sip to sip
 signaling forward unconditional
 # If this gateway is being licensed as a Cisco UBE the following lines are also required
 mode border-element
 ip address trusted list
  ipv4 0.0.0.0 0.0.0.0               # Or an explicit Source IP Address Trust List
sip
  rel1xx disable
  header-passing
  options-ping 60
  midcall-signaling passthru
```

Step 2 Configure default Unified CVP services:

```
#Default Unified CVP Services
application
     service new-call flash:bootstrap.vxml
     service CVPSelfService flash:CVPSelfServiceBootstrap.vxml
     service ringtone flash:ringtone.tcl
     service cvperror flash:cvperror.tcl
     service bootstrap flash:bootstrap.tcl
     service handoff flash:handoff.tcl
```

Step 3 Configure dial-peers:

Note While configuring VXML gateway voice class codec must not be used. G711ulaw may be used in general for the dial-peers, but still depending on the implementation the other codec may be used.

```
# Configure Unified CVP Ringtone
dial-peer voice 919191 voip
     description CVP SIP ringtone dial-peer
     service ringtone
     incoming called-number 9191T
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad
```

```
# Configure Unified CVP Error
dial-peer voice 929292 voip
     description CVP SIP error dial-peer
     service cvperror
     incoming called-number 9292T
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad
```

Step 4 Configure default Unified CVP HTTP, ivr, rtsp, mrcp and vxml settings:

```
http client cache memory pool 15000
http client cache memory file 1000
http client cache refresh 864000
no http client connection persistent
http client connection timeout 60
http client connection idle timeout 10
http client response timeout 30
ivr prompt memory 15000

vxml tree memory 500
vxml audioerror
vxml version 2.0
```

Step 5 Configure VXML leg where the incoming called-number matches the Network VRU Label:

```
dial-peer voice 7777 voip
     description Used for VRU leg
     service bootstrap
     incoming called-number 777T
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad
```

Step 6 Exit configuration mode and use the Cisco IOS CLI command **call application voice load <service_Name>** to load the transferred Unified CVP files into the Cisco IOS memory for each Unified CVP service:

- call application voice load new-call
- call application voice load CVPSelfService
- call application voice load ringtone
- call application voice load cvperror
- call application voice load bootstrap
- call application voice load handoff

Configure Codec for Ingress and VXML Gateways

Configure Ingress Gateway

Procedure

Step 1 Add the voice class codec 1 to set the codec preference in dial-peer:

Example:

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

dial-peer voice 70021 voip
     description Used for Switch leg SIP Direct
     preference 1
     max-conn 225
     destination-pattern xxxx...... # Customer specific destination
     session protocol sipv2
     session target ipv4:###.###.###.### # IP Address for Unified CVP
     session transport tcp
     voice class codec 1
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     no vad
```

Step 2 Modify the dial-peer to specify the codec explicitly for a dial-peer:

```
dial-peer voice 9 voip
     description For Outbound Call for Customer
     destination-pattern <Customer Phone Number Pattern>
     session protocol sipv2
     session target ipv4:<Customer SIP Cloud IP Address>
     session transport tcp
     voice-class sip rel1xx supported "100rel"
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 10 voip
     description ***To CUCM Agent Extension For Outbound***
     destination-pattern <Agent Extension Pattern to CUCM>
     session protocol sipv2
     session target ipv4:<CUCM IP Address>
     voice-class sip rel1xx supported "100rel"
     dtmf-relay rtp-nte
     codec g711alaw
```

Configure VXML Gateway

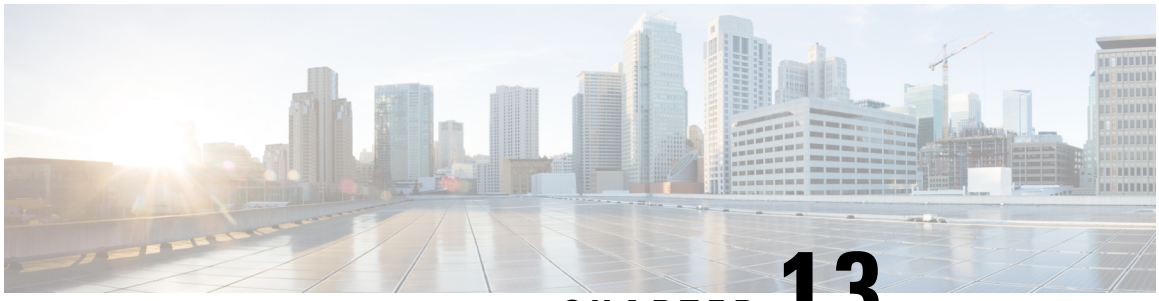
Procedure

Modify the following dial-peer to specify the codec explicitly for a dial-peer:

```
dial-peer voice 919191 voip
     description Unified CVP SIP ringtone dial-peer
     service ringtone
     incoming called-number 9191T
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 929292 voip
     description CVP SIP error dial-peer
     service cvperror
     incoming called-number 9292T
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 7777 voip
     description Used for VRU leg #Configure VXML leg where the incoming called
     service bootstrap
     incoming called-number 7777T
     dtmf-relay rtp-nte
     codec g711alaw
     no vad
```



CHAPTER 13

Configure Cisco Unified Communications Manager

Cisco Unified Communications Manager Configuration

This chapter contains the configuration procedures you must perform to configure Unified Communications Manager. Perform the procedures on the Unified Communications Manager Publisher.

Configure Fully Qualified Domain Name

Procedure

Step 1 Open Cisco Unified Communications Manager and log in.

Step 2 Navigate to **System** > **Enterprise Parameters**.

Step 3 Fill in **Clusterwide Domain Configuration** > **Cluster Fully Qualified Domain Name** with the Fully Qualified Domain Name of your cluster.

Example:

ccm.hcscc.icm

Note The Cluster Fully Qualified Domain Name is the name of the Unified Communications Manager Server Group defined in Unified CVP.

Step 4 Click **Save**.

Configure Cisco Unified Communications Manager Groups

Complete the following procedure to add a Cisco Unified Communications Manager to the Unified Communications Manager Group.

Procedure

Step 1 Select Cisco Unified CM Administrator from the **Navigation** menu and click **Go**.
Step 2 Select **System > Cisco Unified CM Group**.
Step 3 Click **Find**. Then click **Default**.
Step 4 Move the two subscribers from the Available panel to the Selected panel.
Step 5 Click **Save.**
Step 6 Click **Reset.**
Step 7 On the **Device Reset** popup, click **Reset**.
Step 8 Click **Close**.

Configure Conference Bridges

Perform this procedure for each gateway in the deployment.

Procedure

Step 1 Select **Media Resources** > **Conference bridge**.
Step 2 Click **Add New**.
Step 3 Select Conference Bridge Type of **Cisco IOS Conference Bridge**.
Step 4 In the **Conference Bridge name** field, enter a unique identifier for the conference bridge name that matches the configuration on the gateway.

In the example, this is gw70conf.

```
# Add a SCCP group for each of the hardware resource types
sccp ccm group 1
associate ccm 1 priority 1
associate profile 2 register gw70mtp
associate profile 1 register gw70conf
associate profile 3 register gw70xcode
```

Step 5 Select a Device Pool.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

Related Topics

Configure Cisco IOS Enterprise Voice Gateway, on page 89

Configure Media Termination Points

Complete this procedure for each gateway in the deployment.

Procedure

Step 1 Select **Media Resources** > **Media Termination Point**.

Step 2 Click **Add New**.

Step 3 In the Media Termination Point Name field, enter a unique identifier for the media termination that coincides with the configuration on the gateway.

In the example, this is gw70mtp.

```
# Add a SCCP group for each of the hardware resource types
sccp ccm group 1
associate ccm 1 priority 1
associate profile 2 register gw70mtp
associate profile 1 register gw70conf
associate profile 3 register gw70xcode
```

Step 4 Select a Device Pool.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Related Topics

Configure Cisco IOS Enterprise Voice Gateway, on page 89

Transcoder Configuration in Unified CM and IOS Gateway

A transcoder is required for multicodec scenarios to convert a stream from a G.711 codec to a G.729 codec.

For more information about transcoder configuration in Unified Communications Manager and gateway, see the section "Configure Transcoders and Media Termination Points" in the *System Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Configure Transcoders

Perform this procedure for each gateway in the deployment.

Procedure

Step 1 In Unified Communications Manager Administration, select **Media Resources** > **Transcoder.**

Step 2 Click **Add New**.

Step 3 For Transcoder Type, select **Cisco IOS enhanced media termination point**.

Step 4 In the **Device Name** field, enter a unique identifier for the transcoder name that coincides with the configuration on the gateway.

In the following example, this is gw70xcode.

```
# Add a SCCP group for each of the hardware resource types
sccp ccm group 1
associate ccm 1 priority 1
associate profile 2 register gw70mtp
associate profile 1 register gw70conf
associate profile 3 register gw70xcode
```

Step 5 In the **Device Pool** field, select the appropriate device pool.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

Related Topics

Configure Cisco IOS Enterprise Voice Gateway, on page 89

Configure the CVP Call Server Dial Peers in Ingress Gateway

The Ingress Gateway to Unified CVP outbound dial peer configuration uses the IPv4 address of Unified CVP as the session target.

Configure Media Resource Groups

Procedure

Step 1 Select **Media Resources** > **Media Resource Group**.

Step 2 Add a Media Resource Group for Conference Bridges.

a) Click **Add New**.
b) Enter a Name.
c) From the Available list, select all the Cisco IOS conference bridge resources configured for each ingress/VXML combination gateway in the deployment and add them to the group.
d) Click **Save**.

Step 3 Add a Media Resource Group for Media Termination Point.

a) Click **Add New**.
b) Enter a Name.
c) From the Available list, select all the hardware media termination points configured and add them to the group.

d) Click **Save**.

Step 4 Add a Media Resource Group for Transcoder.

a) Click **Add New**.
b) Enter a Name.
c) From the Available list, select all the transcoders configured and add them to the group.
d) Click **Save**.

Step 5 Click **Save.**

Configure and Associate Media Resource Group List

Procedure

Step 1 Select **Media Resources** > **Media Resource Group List**.
Step 2 Click **Add New** and enter a Name.
Step 3 Add a Media Resource Group list and associate all of the media resource groups. Click **Save**.
Step 4 Select **System** > **Device Pool**. Click **Find**. Select the appropriate device pool.
Step 5 From the Media Resource Group List drop-down list, choose the media resource group list added in Step 2.
Step 6 Click **Save**. Click **Reset**.

Configure CTI Route Point

Complete the following procedure to add a computer telephony integration (CTI) route point for agents to use for transfers and conferences.

Procedure

Step 1 In Cisco Unified CM Administration, select **Device** > **CTI Route Point**.
Step 2 Click **Add New**.
Step 3 Set a device name; for example, **PCCEInternalDNs**.
Step 4 For Device Pool, select **Default**.
Step 5 Select a Media Resource Group List from the list.
Step 6 Click **Save.**
Step 7 Click on Line [1] to configure the directory number associated with this route point.

This directory number will be a pattern that is intended to match any of the internal Dialed Numbers you configure in Packaged CCE for internally routed calls. (For instance, for Transfers and Conferences).

Important Define a pattern that is flexible enough to match all your internal dialed numbers yet restrictive enough not to inadvertently intercept calls intended for other Route Patterns you may have defined for other parts of your dial plan. Use a unique prefix for internal calls. For example, if you have internal dialed numbers 1230000 and 1231111, then an appropriate line number to enter for the cti route point would be 123XXXX.

Step 8 Select **User Management** > **Application User**.

Step 9 Select *pguser* created during Packaged CCE automated initialization.

Step 10 Select the CTI Route Point from the list of **Available Devices**, and add it to the list of **Controlled Devices**.

Step 11 Click **Save.**

Configure Ingress Gateways for Locations-based Call Admission Control

Locations-based call admission control (CAC) is used in the Unified CCE branch-office call flow model (also known as the Centralized Model). This means that all servers (Unified CVP, Unified CCE, Unified Communications Manager, and SIP Proxy server) are centralized in one or two data centers, and each branch office.

Configure Unified Communications Manager to use the Ingress gateway instead of Unified CVP as the originating location of the call. This configuration ensures that CAC can be properly adjusted based on the locations of the calling endpoint and the phone.

Important Do not define Unified CVP as a gateway device in Unified Communications Manager.

Procedure

In Cisco Unified CM Administration, define the Ingress gateways as gateway devices. Assign the correct location to the devices.

Configure Route Group

Complete the following procedure to create a route group.

Procedure

Step 1 In Unified Communications Manager, select **Call Routing** > **Route Hunt** > **Route Group**.

Step 2 Click **Add New**.

Step 3 Enter a name for the route group; for example, **CVP Route Group**.

Step 4 Using the Add to Route Group button, add all CVP Trunks as Selected Devices.

Step 5 Click **Save**.

Configure Route List

Complete the following procedure to add a route list to the route group.

Procedure

Step 1 In Unified Communications Manager, select **Call Routing** > **Route Hunt** > **Route List**.

Step 2 Click **Add New**.

Step 3 Enter a name for the route list; for example, **CVP Route List**.

Step 4 Select a Cisco Unified Communications Manager Group.

Step 5 Add the route group you created.

Step 6 Click **Save**.

Configure Route Pattern

Complete the following procedure to add a route pattern to the route list.

Procedure

Step 1 In Unified Communications Manager, select **Call Routing** > **Route Hunt** > **Route Pattern**.

Step 2 Click **Add New**.

Step 3 Enter a route pattern of **8881111000XXXX**.

Step 4 Select the route list that you created.

Step 5 Keep all defaults in all panels

Step 6 Click **Save**.

Step 7 Click **OK** at the message about the Forced Authorization Code. You do not want a Forced Authorization Code.

Add a SIP Profile in Unified CM

This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. Perform this procedure for IPv6-enabled deployments only.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Device Settings** > **SIP Profile**.

Step 2 Click **Add New** and enter the name of the SIP profile.

Step 3 Check the **Enable ANAT** check box on the SIP Profile.

Step 4 Save your changes.

Configure Trunk

There are two Unified CVP Servers and each must be associated with a SIP trunk in Unified Communications Manager. The following procedure explains how to configure the SIP trunks, each targeting a different Unified CVP Server.

Actual site topology may necessitate the use of alternate SIP trunk plans, which are supported as long as both Unified CVP Servers are targeted by the configured SIP trunks.

Procedure

Step 1 In Unified Cisco CM Administration, select **Device** > **Trunk.**

Step 2 Click **Add New**.

Step 3 From the Trunk Type drop-down list, choose **SIP Trunk**, and then click **Next**.

Step 4 Enter the following in the **Device Information** section:

a) In the **Device Name** field, enter a name for the SIP trunk, for example, **`sipTrunkCVPA`**.
b) In the **Device Pool** drop-down list, select the device pool that the customer has defined.
c) Select a Media Resource Group List from the list.
d) Make sure that the **Media Termination Point Required** check box is not checked.

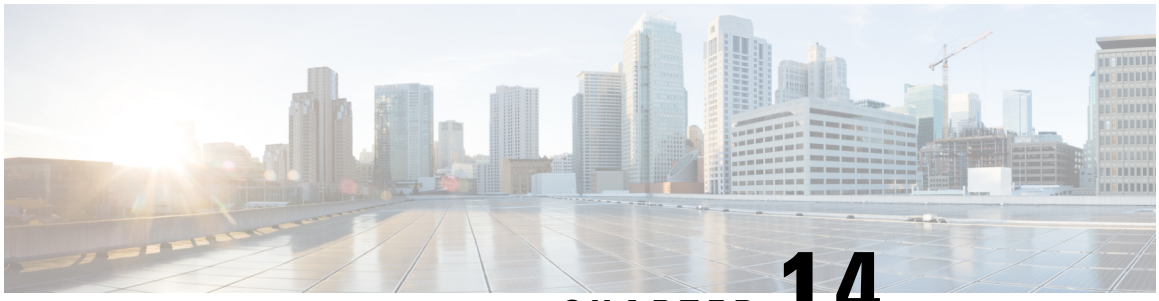
Step 5 Scroll down to the **SIP Information** section:

a) In Row 1 of the **Destination** table, enter the IP address of a CVP server. Accept the default destination port of 5060.
b) In the **SIP Trunk Security Profile** drop-down list, select **Non Secure SIP Trunk Profile**.
c) In the **SIP Profile** drop-down list, select **Standard SIP Profile**.
d) In the **DTMF Signaling Method** drop-down list, select **RFC 2833**.

Step 6 Click **Save**.

Step 7 Click **Reset**.

Step 8 Repeat for all the remaining Unified CVP servers in the deployment.



CHAPTER 14

Configure Cisco Unified Intelligence Center

Follow this sequence to configure the Cisco Unified Intelligence Center for Packaged CCE 2000 Agentsdeployment

Sequence	Task
1	Configure Unified Intelligence Center Data Sources for External AW-HDS-DDSHDS, on page 105
2	Download Report Bundles, on page 106
3	Import Report Bundles, on page 107
4	Configure Unified Intelligence Center Administration, on page 108

Cisco Unified Intelligence Center Configuration

This chapter contains the configuration procedures you must perform to configure Unified Intelligence Center on Side A and Side B.

Configure Unified Intelligence Center Data Sources for External AW-HDS-DDSHDS

Perform this procedure only if your deployment includes an external HDS and you wish to have a longer retention period.

Before you begin

Configure the Unified Intelligence Center SQL user for the External AW-HDS-DDSHDS databases before configuring the data sources (applicable for 4000 Agents and 12000 Agents). For more information, see Configure Unified Intelligence Center SQL User Account on the External HDS, on page 144

Procedure

Step 1 Sign in to Unified Intelligence Center with your Cisco Intelligence Center administrator account (https://<hostname/ IP address of CUIC Publisher>:8444/cuicui).

Step 2 Select **Configure** > **Data Sources**.

Step 3 Click **Data Sources** in the left panel.

Step 4 Select the **UCCE Historical** data source. Click **Edit**.

a) In the **Datasource Host** field, enter the IP Address of the external HDS server.
b) In the **Port** field, enter **1433**.
c) In the **Database Name** field, enter **{instance}_hds**.
d) Leave the **Instance** field blank.
e) Select the **Timezone**.
f) In the **Database User ID**, enter the user name that you configured for the Cisco Unified Intelligence Center SQL Server user account.
g) Enter and confirm the SQL Server User **password**.
h) Select the **Charset** based on the collation of SQL Server installation.
i) Click **Test Connection**.
j) Click **Save**.

Step 5 Click the **Secondary** tab to configure Unified CCE Historical Data Source.

a) Check the **Failover Enabled** checkbox.
b) In the **Datasource Host** field, enter the IP address of the second external HDS server.
c) In the **Port** field, enter **1433**.
d) In the **Database Name** field, enter **{instance}_hds**.
e) Complete other fields as in the Primary tab.
f) Click **Test Connection**.
g) Click **Save**.

Step 6 Repeat this procedure for the **UCCE Realtime** datasource .

The **Database Name** for the Realtime Data Source is **{instance}_hds** .

Related Topics

Configure Unified Intelligence Center SQL User Account on the External HDS, on page 144

Download Report Bundles

The following Cisco Unified Intelligence Center report bundles are available as downloads from Cisco.com https://software.cisco.com/download/type.html?mdfid=282163829&catid=null. Click the **Intelligence Center Reports** link to view all available report bundles:

- Realtime and Historical Transitional templates - Introductory templates designed for new users. These templates are simplified versions of the All Fields templates, and are similar to templates available in other contact center solutions.
- Realtime and Historical All Fields templates - Templates that provide data from all fields in a database. These templates are most useful as a basis for creating custom report templates.
- Live Data templates - Templates that provide up to the moment data for contact center activity.
- Realtime and Historical Outbound templates - Templates for reporting on Outbound Option activity. Import these templates if your deployment includes Outbound Option.
- Realtime and Historical SocialMiner templates - Templates for reporting on SocialMiner activity. Import these templates if your deployment includes SocialMiner.
- Cisco Unified Intelligence Center Admin Security templates - Templates to report on Cisco Unified Intelligence Server audit trails, permissions, and template ownership.

Some of the templates in these bundles are not applicable in Cisco Packaged CCE deployment. See the *Cisco Packaged Contact Center Enterprise Reporting User Guide* at https://www.cisco.com/en/US/products/ps12586/tsd_products_support_series_home.html for more information about the templates used in Packaged CCE deployments.

Additionally, sample custom report templates are available from Cisco DevNet (https://developer.cisco.com/site/reporting/documentation/) and include templates for:

- Enterprise Chat and Email
- Cisco Unified Customer Voice Portal (Unified CVP)

When downloading report template bundles, select bundles for the version of software deployed in your contact center.

Import Report Bundles

Procedure

Step 1 Sign in to Unified Intelligence Center at https://<hostname/ IP address of CUIC Publisher>:8444/cuicui, and click **Reports** in the left pane.

Step 2 Click **New** > **Import**.
You wll be redirected to the legacy interface.

Step 3 Navigate to the folder where you want to import the report and click **Import Report**.

Step 4 In the **File Name (XML or ZIP file)** field, click **Browse**.

Step 5 Browse to and select the report bundle zip file, and click **Open**.

Select a report bundle for the version of software deployed in the contact center.

Step 6 Select the location where you want to save the file.

Step 7 Click **Import**.

Step 8 Choose one:

- If the report or reports do not yet exist, you must provide the data source. From the **Data Source for ValueList** drop-down list, select the data source used. Then click **Import**.

  Note You have to select a data source for the value list only if it does not use the same data source as the report definition. For LiveData reports, the Data Source for ReportDefinition is LiveData Streaming and the Data Source for ValueList is UCCE Realtime. For real time reports, the Data Source is UCCE Realtime. For historical reports, the Data Source is UCCE Historical.

- If the report or reports do exist, a message appears asking you if you want to replace the existing report (which overwrites any report definition changes associated to it). Click **Yes**, **Yes to All**, **No**, or **No to All**.

Configure Unified Intelligence Center Administration

Procedure

Step 1 Sign in to the **Cisco Unified Intelligence Center Administration Console** (`https://<hostname>:8443/oamp`).

Step 2 Configure the Active Directory tab under **Cluster Configuration** > **Reporting Configuration**.

a) Enter the Host Address for the Primary Active Directory Server.
b) Leave the default value for Port.
c) Complete the **Manager Distinguished Name** fields.
d) Enter and confirm the password with which the Manager accesses the domain controller.
e) For User Search Base, specify the Distinguished Name or Organization Unit of the domain you want to search.
f) For Attribute for User ID, select the required option.

Note If the Windows domain name and the NETBIOS names are different, do the following: in the **Cisco Unified Intelligence Center Administration Console**, under **Active Directory Settings**, in the field **Attribute for User ID**, ensure to select *sAMAccountName*, and add the *NETBIOS* value to set it as default value.

g) Add at least one domain for the UserName Identifier. Do not type the @ sign before the domain name.
h) Set a domain as the default.
i) Click **Test Connection**.
j) Click **Save**.

Note For more details, see the online help.

Step 3 Configure syslog for all devices.

a) Choose **Device Management** > **Logs and Traces Settings**.
b) For each host address:

- Select the associated servers and click the arrow to expand.
- Select the server name.

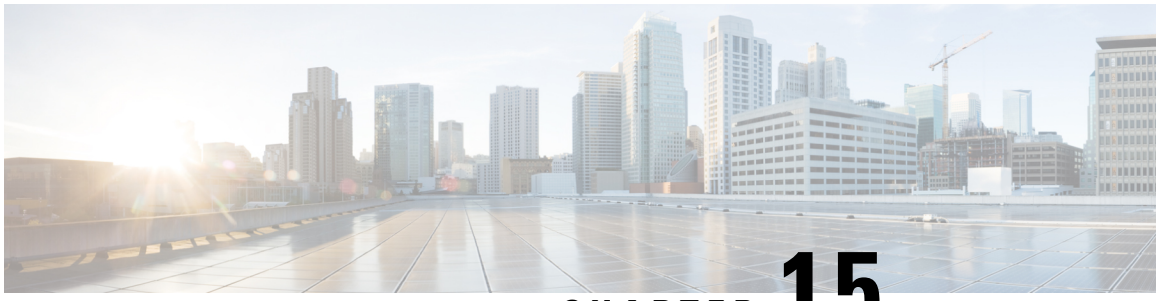
- In the **Edit Serviceability Settings** screen **Syslog Settings** pane, configure the Primary and Backup Host. Click **Save**.

Step 4 Configure SNMP for all devices, if used.

a) Select **Network Management** > **SNMP**.

b) Navigate to SNMP and for each server add the following:

- V1/V2c Community Strings.
- Notification Destination.



CHAPTER 15

Configure Cisco Finesse

Cisco Finesse Configuration

This chapter contains the configuration procedures you must perform to configure Cisco Finesse. Perform the procedures on the Cisco Finesse Primary node.

Configure Contact Center Agents and Routing for Live Data Reports

In order to test the Live Data reports in the Finesse desktops, configure the following in Unified CCE Administration (`https://<Side A/B Unified CCE AW-HDS-DDS IP address>/cceadmin`):

- Agents
- Skill groups or precision queues
- Call types
- Dialed numbers
- Network VRU scripts
- Routing scripts

Note Routing scripts are configured in Script Editor, which you can open from Unified CCE Administration Tools.

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

Live Data Reports

Cisco Unified Intelligence Center provides Live Data real-time reports that you can add to the Finesse desktop.

Prerequisites for Live Data

Before you add Live Data reports to the desktop, you must meet the following prerequisites:

- Download the Live Data reports from Cisco.com and import them into Cisco Unified Intelligence Center. Verify that the reports are working in Unified Intelligence Center.
- Ensure that user integration synchronization is enabled for Cisco Unified Intelligence Center. For more information, see *Administration Console User Guide for Cisco Unified Intelligence Center* https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.
- For HTTPS, you must upload security certificates to the Finesse and Cisco Unified Intelligence Center servers. Both Finesse and Cisco Unified Intelligence Center are installed with self-signed certificates. However, if you use the self-signed certificates, agents and supervisors must accept certificates in the Finesse desktop when they sign in before they can use the Live Data gadget. To avoid this requirement, you can provide a CA certificate instead. You can obtain a CA certificate from a third-party certificate vendor or produce one internal to your organization.

Related Topics

Download Report Bundles, on page 106
Import Report Bundles, on page 107
Certificates for Live Data, on page 222

Add Live Data Reports to Finesse

The following sections describe how to add the Live Data reports to the Finesse desktop. The procedure that you follow depends on several factors, described in the following table.

Procedure	When to use
Add Live Data reports to default desktop layout	Use this procedure if you want to add Live Data reports to the Finesse desktop after a fresh installation or after an upgrade if you have not customized the default desktop layout.
Add Live Data reports to custom desktop layout	Use this procedure if you have customized the Finesse desktop layout.
Add Live Data reports to team layout	Use this procedure if you want to add Live Data reports to the desktop layout for specific teams only.

Add Live Data Reports to Default Desktop Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to the default desktop layout. Use this procedure after a fresh installation of Finesse. If you upgraded Finesse but do not have a custom desktop layout, click **Restore Default Layout** on the Manage Desktop Layout gadget and then follow the steps in this procedure. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

Procedure

Step 1 Sign in to the Finesse administration console (`https://FQDN of Finesse server:Port Number(8445)/cfadmin`), in which FQDN refers to the fully qualified domain name.

Step 2 Click the **Desktop Layout** tab.

Step 3 Remove the comment characters (<!-- and -->) from each report that you want to add to the desktop layout. Make sure you choose the reports that match the method your agents use to access the Finesse desktop (HTTP or HTTPS).

Step 4 Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 5 Optionally, change the gadget height.

Example:

The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows, replacing 310 with 400:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=400&viewId_1=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
        </gadget>
```

To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

Step 6 Click **Save**.

Note After you add a gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without needing to scroll down.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

Add Live Data Reports to Custom Desktop Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to a custom desktop layout. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

Procedure

Step 1 Sign in to the Finesse administration console.

Step 2 Click the **Desktop Layout** tab.

Step 3 Click **Finesse Default Layout XML** to show the default layout XML.

Step 4 Copy the XML code for the report you want to add from the Finesse default layout XML.

Example:

To add the Agent Report for HTTPS, copy the following:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&
        viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
</gadget>
```

Step 5 Paste the XML within the tab tags where you want it to appear.

Example:

To add the report to the home tab of the agent desktop:

```
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
              gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
              filterId_1=agent.id=CL%20teamName&
              viewId_2=9AB7848B10000141000001C50A0006C4&
              filterId_2=agent.id=CL%20teamName
      </gadget>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
  </tabs>
</layout>
```

Step 6 Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 7 Optionally, change the gadget height.

Example:

The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=400&viewId_1=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
        </gadget>
```

To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

Step 8 Click **Save**.

Note After you add a gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without needing to scroll down.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

Add Live Data Reports to Team Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to the desktop layout of a specific team. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

Procedure

Step 1 Copy the XML code for the report you want to add from the Finesse default layout XML.

Example:

To add the Agent Report for HTTPS, copy the following:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
        </gadget>
```

Step 2 Click the **Team Resources** tab.

Step 3 Select the team from the list of teams for which you want to add the report.

Step 4 In the Resources for <team name> area, click the **Desktop Layout** tab.

Step 5 Check the **Override System Default** check box.

Step 6 Paste the XML within the tab tags where you want it to appear.

Example:

To add the report to the home tab of the agent desktop:

```
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
              gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
              filterId_1=agent.id=CL%20teamName&
              viewId_2=9AB7848B10000141000001C50A0006C4&
              filterId_2=agent.id=CL%20teamName
      </gadget>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
  </tabs>
</layout>
```

Step 7 Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 8 Optionally, change the gadget height.

Example:

The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=400&viewId_1=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
        </gadget>
```

To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

Step 9 Click **Save**.

Note After you add a gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without needing to scroll down.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

Modify Live Data Stock Reports for Finesse

This procedure describes how to modify the Live Data stock reports in Cisco Unified Intelligence Center and add the modified report to the Finesse desktop layout. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

Note To make sure the modified gadget renders in the Finesse desktop, you must give the appropriate permission for that report in Cisco Unified Intelligence Center.

Procedure

Step 1 Copy the gadget URL for the report you want to modify from the Finesse default layout XML and paste it into a text editor.

Example:

If you want to modify the Agent Report for HTTPS, copy the following URL and paste it into a text editor:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
        </gadget>
```

Step 2 In Cisco Unified Intelligence Center, in Edit view of the report, select the view for which you want to create a gadget URL and then click **Links**.

The HTML Link field displays the permalink of the customized report.

Step 3 Copy the permalink of the customized report from the **HTML Link** field, and paste it in a text editor. Then copy the viewId value from this link into the desired view.

Example:

Copy the viewId, which is underlined in this example, from the permalink for the report.

```
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid
```

Step 4 Replace the desired viewId value in the gadget URL with the viewId value from the permalink of the customized report.

Step 5 Replace my-cuic-server with the FQDN of the Cisco Unified Intelligence Center Server.

Step 6 Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click **Save**.

Note After you add the gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without the need to scroll.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

Configure Live Data Reports with Multiple Views

Cisco Unified Intelligence Center allows you to display multiple Live Data reports or views on a single gadget. Agents can select the desired view to display from a drop-down list on the gadget toolbar, which lists up to five report views in *Report Name - View Name* format.

This procedure describes how to add multiple Live Data views to the Finesse desktop layout using the viewId_n and filterId_n keys. You can specify up to five report views to appear in your gadget. The first view among the five is the default view. There is no defined order for how the remaining views are displayed.

Finesse still supports the display of a single gadget using a single viewId. However, if you specify the single viewId along with multiple viewId_n keys, the multiple views are used and the single viewId is ignored.

Note To make sure the modified gadget renders in the Finesse desktop, you must give the appropriate permission for that report in Unified Intelligence Center.

Procedure

Step 1 For each report or view that you want to include in the gadget, obtain the associated viewId from the permalink for the view:

a) In Unified Intelligence Center, in Edit view of the report, select the desired view then click **Links**.

The HTML Link field displays the permalink of the customized report.

b) Copy the permalink of the customized report from the **HTML Link** field, and paste it in a text editor, and then copy the viewID value from the permalink and save it.

Example:

Copy the viewId, which is underlined in this example, from the permalink for the report.

```
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid
```

Step 2 From the Finesse default layout XML, copy the gadget URL for one of the Live Data reports and paste it into a text editor.

Example:

Copy the URL for the Agent Skill Group for HTTPS from the default layout XML and paste it into a text editor:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=9AB7848B10000141000001C50A0006C4&filterId_1=agent.id=CL%20teamName</gadget>
```

Step 3 To update the URL to refer to a different report view, populate the viewId_1 value (after the equal sign) with the desired viewId obtained in step 1.

Example:

The following shows the URL updated with the example viewId copied from step 1.

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName</gadget>
```

Step 4 For each additional view you want to include:

a) At the end of the URL, copy and paste the viewId_1 and agentId_1 strings with a leading ampersand.

Example:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName</gadget>
```

b) Update the copied viewId_1 and filterId_1 in the URL to the next available integer (in this example, viewId_2 and filterId_2).

Example:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&
viewId_2=5C90012F10000140000000830A4E5B33&filterId_2=agent.id=CL%20teamName</gadget>
```

c) Populate the copied viewId value (after the equal sign) with the value defined in the permalink for the desired report (in this example, `99E6C8E210000141000000D80A0006C4`).

Example:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&
viewId_2=99E6C8E210000141000000D80A0006C4&filterId_2=agent.id=CL%20teamName</gadget>
```

d) Make sure that the filterId value matches the type required by the report type, as follows:

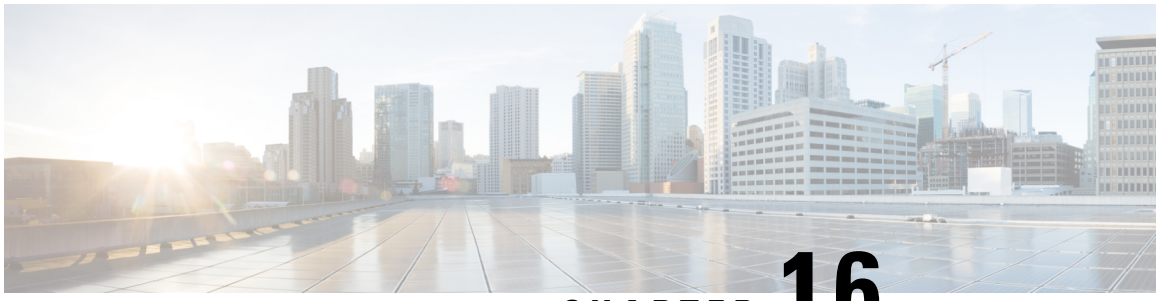
- Agent Reports: filterId_*N*=agent.id=CL%20teamName
- Agent Skill Group Reports: filterId_*N*=agent.id=CL%20teamName
- Skill Group Reports: filterId_*N*=skillGroup.id=CL%20teamName
- Precision Queue Reports: filterId_*N*=precisionQueue.id=CL%20teamName

Step 5 Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 6 Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click **Save**.

Note After you add the gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without the need to scroll.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.



CHAPTER 16

Configure IPv6

IPv6 Configuration

Packaged CCE can support IPv6 connections for agent and supervisor Finesse desktops and phones. An IPv6-enabled deployment can use either all IPv6 endpoints or a mix of IPv4 and IPv6 endpoints. Servers that communicate with these endpoints can accept both IPv4 and IPv6 connections. Communication between servers continues to use IPv4 connections.

This chapter contains the configuration procedures that you perform for IPv6-enabled deployments.

Set Up IPv6 for VOS-Based Contact Center Applications

By default, only IPv4 is enabled for Unified Communications Manager, Cisco Finesse, and Unified Intelligence Center.

If you choose to enable IPv6 on these applications, you must enable it on both the publisher/primary nodes and subscriber/secondary nodes for those applications.

You can use Cisco Unified Operating System Administration or the CLI to enable IPv6.

See the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html for more information about IPv6 support in Packaged CCE deployments.

Set Up IPv6 Using Cisco Unified Operating System Administration

To set up IPv6 using Cisco Unified Operating System Administration, perform the following procedure on the primary and secondary VOS servers.

Procedure

Step 1 Sign into Cisco Unified Operating System Administration on the Publisher/Primary node:.

- Unified Communications Manager and Unified Intelligence Center: `https://<host or IP address of the Publisher or Primary node>/cmplatform`
- Finesse: `https://FQDN of the Primary node:8443/cmplatform`

Step 2 Navigate to **Settings** > **IP** > **Ethernet IPv6**.

Step 3 Check the **Enable IPv6** check box.

Step 4 Enter values for **IPv6Address**, **Prefix Length**, and **Default Gateway**.

Step 5 Check the **Update with Reboot** check box.

Step 6 Click **Save**.
The server restarts.

Step 7 Repeat this procedure on the subscriber/secondary node.

Set Up IPv6 for VOS-Based Applications Using the CLI

To set up IPv6 using the CLI, perform the following procedure on both the primary and secondary VOS servers.

Procedure

Step 1 Access the CLI on the VOS server.

Step 2 To enable or disable IPv6, enter:
set network ipv6 service {enable | disable}

Step 3 Set the IPv6 address and prefix length:
set network ipv6 static_address *addr mask*

Example:

```
set network ipv6 static_address 2001:db8:2::a 64
```

Step 4 Set the default gateway:
set network ipv6 gateway *addr*

Step 5 Restart the system for the changes to take effect.
utils system restart

Step 6 To display the IPv6 settings, enter:
show network ipv6 settings

Configure NAT64 for IPv6-Enabled Deployment

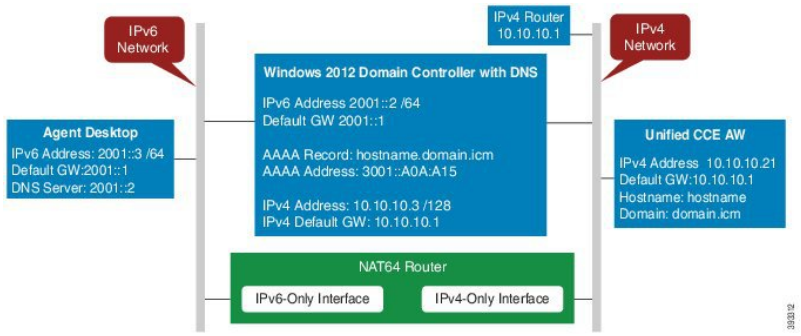
NAT64 allows communication between IPv6 and IPv4 networks. For IPv6-enabled deployments, you must set up NAT64 so that supervisors on an IPv6 network can access Unified CCE Administration web tools on an IPv4 network.

You can use either Stateful and Stateless NAT64. To read more about which translation type is the most appropriate for your deployment see Table 2. Comparison Between Stateless and Stateful NAT64 here: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

Note NAT64 is NOT supported on M train IOS. T train is required.

For more information, see the Compatibility Matrix for Packaged Contact Center Enterprise at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html.

The following example network diagram and interface configuration demonstrates Stateful NAT64 translation between an IPv6 network and an IPv4 network.




```
interface GigabitEthernet0/0
description ipv4-only interface
 ip address 10.10.10.81 255.255.255.128
 duplex auto
 speed auto
 nat64 enable
 no mop enabled

interface GigabitEthernet0/1
description ipv6-only interface
 no ip address
 duplex auto
 speed auto
 nat64 enable
 ipv6 address 2001::1/64
 ipv6 enable

ipv6 unicast-routing
ipv6 cef
!
nat64 prefix stateful 3001::/96
nat64 v4 pool POOL1 10.10.10.129 10.10.10.250
```

```
nat64 v6v4 list V6ACL1 pool POOL1 overload
ipv6 router rip RIPv6
!
ipv6 router rip RIP

!
ipv6 access-list V6ACL1
 permit ipv6 2001::/64 any
```

Configure DNS for IPv6

To meet the requirement that Unified CCE Administration be accessed by FQDN, a Forward lookup AAAA record for the Unified CCE AW-HDS-DDS servers and any External HDS servers must be created in DNS.

The steps in this procedure are for a Windows DNS server.

Procedure

Step 1 In Windows, navigate to **Administrative Tools > DNS**. This opens the DNS Manager.

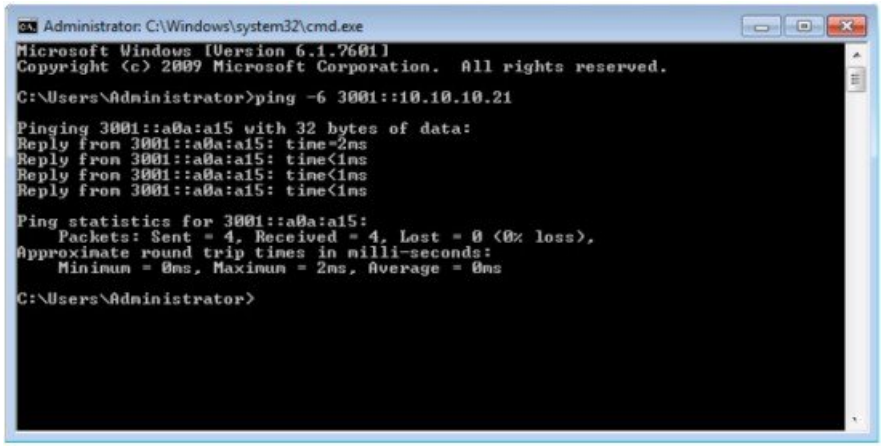
Step 2 In the Forward lookup zone, navigate to your deployment's domain name.

Step 3 Right-click the domain name and select **New Host (A or AAAA)**.

Step 4 In the New Host dialog box, enter the computer name and IP address of the Unified CCE AW-HDS-DDS servers and any External HDS servers. Click **Add Host**.

Determine IPv6 Translation of IPv4 Address for DNS Entry

You can determine the IPv6 address needed for the AAAA DNS record by running a ping command on any Windows machine using mixed notation. Type “ping -6” followed by your IPv6 Nat64 Prefix, two colons, and then the IPv4 address.



In the ping response, the IPv4 address is converted to the hexadecimal equivalent. Use this address in your static AAAA record.

Note Optionally, DNS64 can be used in place of static DNS entries. Use of DNS64 helps facilitate translation between IPv6 and IPv4 networks by synthesizing AAAA resource records from A resource records.

The *NAT64 Technology: Connecting IPv6 and IPv4 Networks* whitepaper gives an overview of DNS64 and how it is used with IPv6: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html.

Configure IPv6 on Unified CVP Call Server

For IPv6-enabled deployments, you must add an IPv6 address to your Unified CVP Call Server's existing network interface.

Perform this procedure only if you have an IPv6-enabled environment.

Procedure

Step 1 On the Unified CVP Call Server, navigate to **Control Panel** > **Network and Sharing**.

Step 2 Click **Ethernet**.

Step 3 From the **Ethernet Status** window, select **Properties**.

Step 4 Check the **Internet Protocol Version 6 (TCP/IPv6)** check box, and choose **Properties**.

Step 5 Choose **Use the following IPv6 address** radio button.

Step 6 Enter values in the **IPv6 address**, **Subnet prefix length**, and **Default gateway** fields.

Step 7 Click **OK** and restart Windows when prompted.

Configure Gateways to Support IPv6

For IPv6-enabled deployments, you must configure your Ingress and VXML gateways to enable IPv6 addressing.

Configure an Interface to Support IPv6 Protocol Stack

This procedure applies to both the Ingress and the VXML gateway.

Procedure

Configure the following on the Gateway:

```
>Enable
>configure terminal
>interface type number
```

```
>ipv6 address{ ipv6-address / prefix-length | prefix-name sub-bits / prefix-length}
>ipv6 enable
```

Enable ANAT in Ingress Gateway

Procedure

Configure the following on the Gateway:

```
>conf t
>voice service voip
>SIP
>ANAT
>bind control source-interface GigabitEthernet0/2
>bind media source-interface GigabitEthernet0/2
```

Enable Dual Stack in the Ingress Gateway

Procedure

Configure the following on the Gateway:

```
>conf t
>sip-ua
>protocol mode dual-stack preference ipv6
```

Configure IPv6 on Unified Communications Manager

In an IPv6-enabled environment, you must perform the procedures in this section to configure IPv6 on Unified Communications Manager.

Cluster-Wide Configuration in Unified CM Administration

Perform the following procedure to set IPv6 as the addressing mode preference for media and signaling cluster-wide.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **System** > **Enterprise Parameters** > **IPv6 Configuration Modes** to configure the cluster-wide IPv6 settings for each Unified Communications Manager server.

Step 2 From the **Enable IPv6** drop-down list, choose **True**.

Step 3 From the **IP Addressing Mode Preference for Media** drop-down list, choose **IPv6**.

Step 4 From the **IP Addressing Mode Preference for Signaling** drop-down list, choose **IPv6**.

Step 5 From the **Allow Auto-configuration for Phones** drop-down list, choose **Off**.

Step 6 Save your changes.

Transcoding

In an IPv6-enabled environment, a transcoder is required for the following scenarios:

- An agent logged in to an IPv6 endpoint needs to send or receive transfers from an agent logged in to an IPv4 endpoint.
- An agent logged in to an IPv6 endpoint needs to connect to a VXML Gateway for self service.

Related Topics

Transcoder Configuration in Unified CM and IOS Gateway, on page 99

Add a Common Device Configuration Profile in Unified Communications Manager

In an IPv6-enabled environment, you may have both IPv4 and IPv6 devices.

Perform the following procedure to add an IPv4, IPv6, or dual stack common device configuration profile in Unified Communications Manager.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Click **Add New** and enter the name of the new common device configuration profile.

Step 3 From the **IP Addressing Mode** drop-down list:

- To add an IPv6 common device configuration profile in Unified Communications Manager, choose **IPv6 only**.
- To add an IPv4 common device configuration profile in Unified Communications Manager, choose **IPv4 only**.
- To add a dual stack common device configuration profile in Unified Communications Manager, choose **IPv4 and IPv6**. Then choose **IPv4** from the **IP Addressing Mode Preference for Signaling** drop-down list.

Step 4 Save your changes.

Associate the Common Device Configuration Profile with Gateway Trunk

Perform the following procedure to associate the common device configuration profile with the Gateway trunk. This procedure applies to the Ingress Gateway.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Trunk**.

Step 2 Click **Find**.
Choose the trunk profile that you want to view.

Step 3 From the **Common Device Configuration** drop-down list:

- To associate the IPv6 common device configuration profile with the Gateway trunk, choose the IPv6 common device configuration profile.
- To associate the IPv4 common device configuration profile with the Gateway trunk, choose the IPv4 common device configuration profile.

Note Unified CM gateway trunk supports only an IPv4 or IPv6 trunk. You cannot associate a dual stack common device configuration profile to a Unified CM gateway trunk.

Step 4 Enter the IPv6 address in the **Destination Address IPv6** field.

Note Unified CM to Gateway trunk supports only standard SIP Profile and does not support ANAT enabled dual-stack SIP trunk.

Step 5 Save your changes.

Associate the Common Device Configuration Profile with an IPv4 or IPv6 Phone

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Phone**.

Step 2 Click **Find**.
Choose the trunk profile that you want to view.

Step 3 From the **Common Device Configuration** drop-down list: choose the IPv6 common device configuration profile.

- To associate the IPv6 common device configuration profile to an IPv6 phone, choose the IPv6 common device configuration profile.
- To associate the IPv4 common device configuration profile to an IPv4 phone, choose the IPv4 common device configuration profle.

Step 4 Save your changes.

Associate a SIP Profile in Unified CM

In an IPv6-enabled deployment, you must associate a SIP profile with the trunk you configured for Unified CVP.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Trunk**.

Step 2 Click **Find**. Choose the trunk profile that you want to view.

Step 3 From the **SIP Profile** drop-down list, choose the SIP Profile you created.

Note For more information on how to create a SIP Profile, see

Add a SIP Profile in Unified CM, on page 103.

Step 4 Save your change.

Related Topics

Configure Trunk, on page 104

Associate the Dual Stack Common Device Configuration Profile with SIP Trunk

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Trunk**.

Step 2 Click **Find**. Choose the trunk profile that you want to view.

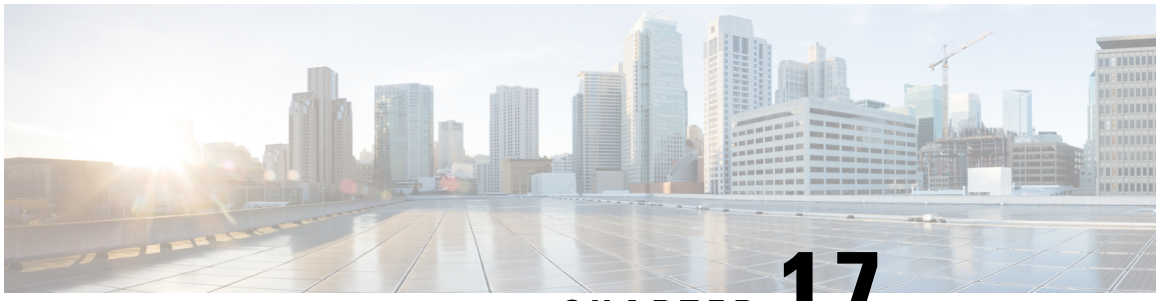
Step 3 From the **Common Device Configuration** drop-down list, choose the Dual Stack Common Device Configuration Profile.

Note For more information on how to add a Dual Stack Common Device Configuration Profile, see Add a Common Device Configuration Profile in Unified Communications Manager, on page 127.

Step 4 Save your change.

PART IV

Optional Enterprise Chat and Email



CHAPTER 17

Install and Configure Enterprise Chat and Email

Install and Configure Enterprise Chat and Email

Enterprise Chat and Email (ECE) is an optional feature that provides chat and email functionality to the contact center. On-box installation is supported on the B200 M4, C240 M4SX and C240 M5SX hardware only.

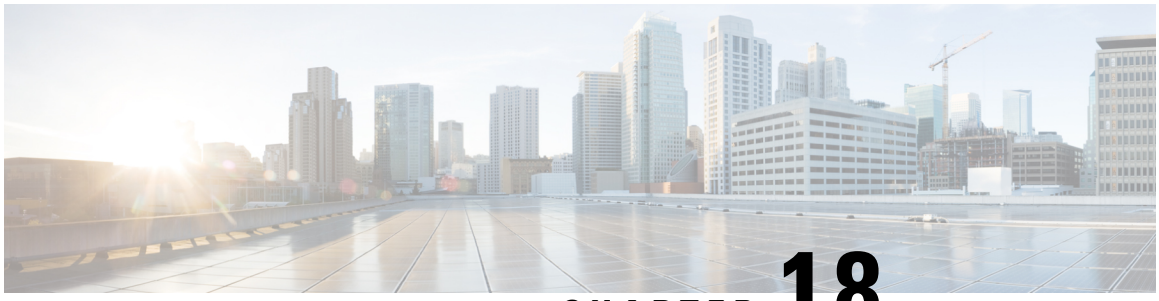
Deploy the ECE Web Server on an external server. You can place that server either in the same data center as the ECE Data Server or in a DMZ if customer chat interactions require that.

Use *Packaged-CCE-ECE.ova* OVA file to create a virtual machine for an on-box ECE. For information about creating a virtual machine, see Create a Virtual Machine from the OVA, on page 38.

For capacity information, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise*, available at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html.

PART V

Optional Cisco Virtualized Voice Browser



CHAPTER 18

Install and Configure Cisco Virtualized Voice Browser

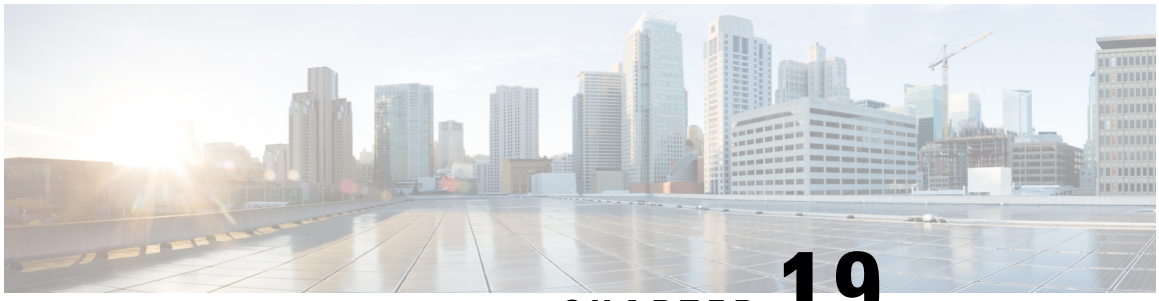
Install and Configure Cisco Virtualized Voice Browser

Cisco Virtualized Voice Browser (Cisco VVB) provides a platform for interpreting VXML documents. Cisco VVB serves as an alternative to the use of IOS Voice Browsers (VXML gateways). When an incoming call arrives at the contact center, Cisco VVB allocates a VXML port that represents the VoIP endpoint. Cisco VVB sends HTTP requests to the Unified CVP VXML server. The Unified CVP VXML server executes the request and sends back a dynamically generated VXML document.

Cisco VVB is installed off box. Installation and configuration procedures are documented in the *Installation and Upgrade Guide for Cisco Virtualized Voice Browser* at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-installation-guides-list.html.

PART VI

Optional External HDS



CHAPTER 19

Install and Configure the External HDS

Install and Configure the External HDS

The default deployment pulls data from the on-box AW-HDS-DDS on the Unified CCE AW-HDS-DDS, where Real-time, Historical and Call Detail Data are stored.

If you need a longer retention period, you can optionally install the Administration Server, Real Time and Historical Data Server, Detail Data Server (AW-HDS-DDS) on a maximum of two separate, external servers. Each external server is configured as **Central Controller Side A Preferred** or **Central Controller Side B Preferred**.

For more information about retention, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html.

Important The External HDS must be able to connect to the Packaged CCE Side A and Side B ESXi hosts.

Refer to the *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html for the requirements for the external HDS server.

Follow this sequence of tasks to install an external HDS.

Sequence	Task
1	Install Microsoft Windows Server, on page 45
2	Install Antivirus Software, on page 43
3	Install Microsoft SQL Server, on page 50
4	Install Cisco Unified Contact Center Enterprise, on page 54

Sequence	Task
5	Configure SQL Server for CCE Components, on page 69
6	Configure the database drive for the amount of data you want to keep. See Configure Database Drive, on page 41
7	Create an HDS Database for the External HDS, on page 142
8	Configure the External HDS , on page 143
9	Configure Unified Intelligence Center SQL User Account on the External HDS, on page 144
10	Configure Unified Intelligence Center Data Sources for External AW-HDS-DDSHDS, on page 105
11	If you have an IPv6 enabled deployment, configure a Forward lookup AAAA record for the External HDS in DNS. See Configure DNS for IPv6, on page 124

Create an HDS Database for the External HDS

Create the HDS database using ICMDBA.

Procedure

Step 1 Open **Unified CCE Tools** > **ICMdba**.

Note You must add instances to display in the ICMDBA. For more information, see Add a UCCE Instance, on page 177.

Step 2 Expand the instance tree view on the newly added external HDS until you can see your instance.

Step 3 Right click on the instance and select **Create**.

Step 4 In the **Select component** drop-down list, select **Administration & Data Server** and click **OK**.

Step 5 In the **Select AW type** drop-down list, select **Enterprise** and click **OK**.

Step 6 From the menu, select **Database** > **Create**. Click **Add**.

Step 7 Click the **Data** radio button, select the second disk drive, and enter the desired HDS size. Click **OK**.

Step 8 Click the **Log** radio button, select the second disk drive, and enter the desired log size. Click **OK**.

Step 9 Click **Create**.

Configure the External HDS

Procedure

Step 1 Open **Unified CCE Web Setup**.

Step 2 Choose **Component Management** > **Administration & Data Servers**. Click **Add.**

Step 3 On the Deployment page, choose the current instance.

Step 4 On the Add Administration & Data Servers page, configure as follows:

a) Click **Enterprise.**
b) Click **Small to Medium Deployment Size**.
c) Click **Next.**

Step 5 On the Server Role in a Small to Medium Deployment page, choose the option **Administration Server Real-time and Historical Data Server, and Detail Data Server (AW-HDS-DDS)**. Click **Next.**

Step 6 On the Administration & Data Servers Connectivity page:

a) Click the radio button for **Primary Administration & Data Server**.
b) In the **Secondary Administration & Data Server* field, enter the hostname for the server.
c) In the **Primary Administration & Data Server* field, enter the hostname for the server.
d) In the **Primary/Secondary Pair (Site) Name* field, enter **`CCE-AW-1`** for the first External HDS or **`CCE-AW-2`** for the second External HDS.
e) Click **Next.**

Step 7 On the Database and Options page, configure as follows:

a) In the **Create Database(s) on Drive** field, choose **C**.
b) DO NOT click the **Agent Re-skilling** web tool. Packaged CCE does not support this tool. Supervisors reskill agents using the Agent tool in Unified CCE Administration.
c) Click **Internet script editor**.
d) Click **Next.**

Step 8 On the Central Controller Connectivity page, configure as follows:

a) For Router Side A, enter the IP Address of the Unified CCE Rogger A.
b) For Router Side B, enter the IP Address of the Unified CCE Rogger B.
c) For Logger Side A, enter the IP Address of the Unified CCE Rogger A.
d) For Logger Side B, enter the IP Address of the Unified CCE Rogger B.
e) Enter the Central Controller Domain Name.
f) Click **Central Controller Side A Preferred** or **Central Controller Side B Preferred** .
g) Click **Next.**

Note The Administration & Data Server can connect to the central controller with a hostname of maximum 15 characters.

Step 9 Review the Summary page, and then click **Finish.**

Configure Unified Intelligence Center SQL User Account on the External HDS

Procedure

Step 1 Launch Microsoft SQL Server Management Studio .

Step 2 Navigate to **Security** >**Logins**, right-click **Logins** and select **New Login**.

This login is used when you configure the data sources for Cisco Unified Intelligence Center reporting.

Step 3 On the General Screen:

a) Enter the Login Name.
b) Select **SQL Server authentication**.
c) Enter and confirm the Password.
d) Uncheck **Enforce password policy**.

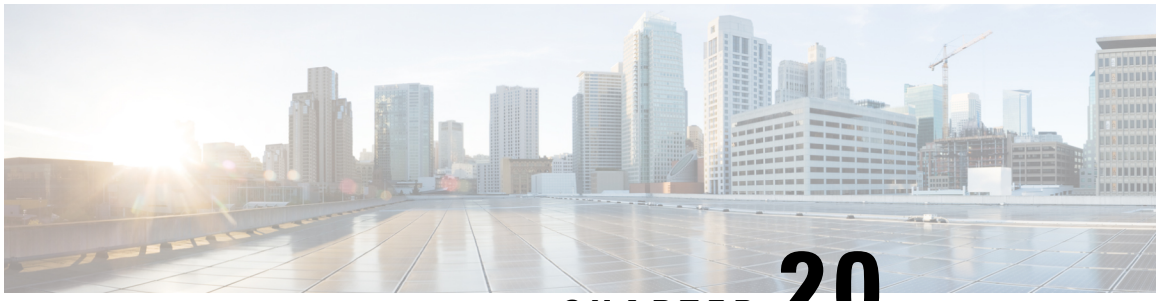
Step 4 Click **User Mapping**.

a) Check the databases associated with the AWdb.
b) Choose each database and associate it with the **db_datareader** and **public** role, and click **OK**.

Step 5 Click **OK**.

PART VII

Version Upgrade



CHAPTER 20

Upgrade System Requirements

Upgrade to Release 11.6(1)

Supported upgrade paths for Cisco Packaged CCE, Release 11.6(1):

- You can upgrade to Release 11.6(1) from Release 11.5(1) directly. For step by step procedures on how to upgrade to Release 11.6(1) from Release 11.5(x), see the *Packaged CCE 11.5 to 11.6 Upgrade* chapter.
- From the releases 11.0(x), you must migrate and upgrade to 11.6(1) . For step by step procedures on how to upgrade to Release 11.6(1) from Release 11.0(x), see the *Packaged CCE 11.0(x) to 11.6* Upgrade chapter.
- To upgrade from a release earlier than release 11.0(1), upgrade to release 11.0(1) and then upgrade to release 11.6(1).
- If there are later 11.x Maintenance Releases installed, uninstall these maintenance releases before installing Release 11.6(1). You can determine which maintenance releases you have applied, in the Programs and Features list in Control Panel.

For step by step procedures on how to upgrade to Release 11.6(1) from Release 11.5(x), see the chapters 22 through chapter 30.

Before upgrading or uninstalling Release 11.6(1), close all the open Microsoft Windows Event Viewer instances. This will prevent an installation failure with an error that the following DLLs are locked:

- icrcat.dll
- icrmsgs.dll
- snmpeventcats.dll
- snmpeventmsgs.dll

If the failure occurs, close the Event Viewer and retry the installation or uninstallation.

If the failure persists, restart the Microsoft Windows Event Log service.

COP Files Installation

Before upgrading a standalone deployment of Unified CCE (Release 10.5 or Release 11.0) or Packaged CCE with CUIC to a Release 11.6(1) co-resident `UCCE: 2000 Agents` deployment (CUIC with Live Data and IdS), install the required COP files. See the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide for more information about the installation of the COP files.

Upgrade Utilities

The EDMT, RegUtil, User Migration Tool, and DB Estimator upgrade utilities do not apply in this release. Use the Release 11.0(1) version of the EDMT, RegUtil, User Migration Tool, and DB Estimator upgrade utilities to upgrade to Release 11.0(1), as needed.

For the upgrade utilities, see https://software.cisco.com/download/type.html?mdfid=268439622

Live Data Deployments

In this release, Live Data supports only 12 Agent Peripheral Gateways (PGs). Deployment upgrades from Release 11.0(2) to Release 11.6(1) with more than 12 Agent PGs (UCM PGs and TDM PGs) are only supported if you are not using Live Data.

Remove CTIOS Server

If CTI OS Server is present in the deployment, use `\icm\CTIOS_bin\SETUP.exe` to remove it. CTI OS is no longer supported.

Microsoft Windows Patches and Updates

An upgrade to Release 11.6(1) requires the latest Microsoft Windows Server 2012 R2 and Microsoft SQL Server 2014 KB patches and Service Packs.

If you applied a Microsoft Windows update since March 2014, the Microsoft Windows Update KB2919355 (Hotfix) should be installed. To determine if this Microsoft Windows Hotfix is installed, from your Control Panel go to **Programs** > **Programs and Features**. Click **View installed updates**.

Make sure that Microsoft Windows Update is not running when you install the Release 11.6(1) patch.

Note On the Microsoft Windows 7 based administration client systems, install Microsoft Windows Update KB3080079 to ensure that the remote desktop connection over TLS v1.1 or 1.2 is supported.

Download and install the necessary Microsoft Patch updates to ensure that the ransomware Wannacry does not affect the Cisco Unified Contact Center deployment.

Supported Upgrade Paths

You can upgrade to this Packaged CCE release from any version of Packaged CCE Release 11.0(x).

Before you upgrade Packaged CCE, you must upgrade on-box or off-box Unified Communication Manager Publisher and Subscribers to a version supported by this release of Packaged CCE. For information about supported versions, see the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/

c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html.

Hardware Refresh with Common Ground Upgrade

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

- Prepare Customer Site Servers, on page 7
- *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html

After you configure the servers, you can move the VMs to the servers and complete the common ground upgrade process.

NTP Configuration Requirements

Packaged CCE relies on time synchronization. Properly configuring NTP is critical for reliability of reporting data and cross-component communication. It's important to implement the requirements outlined in NTP and Time Synchronization, on page 21.

Preupgrade System Requirements

For supported versions of all Cisco Contact Center and third-party software, see the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html.

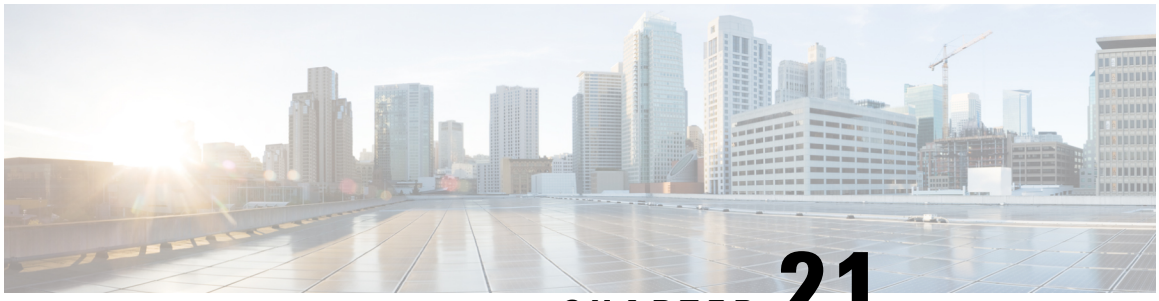
Item	Requirement
VMware Host	For supported ESXi versions, see the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html . Sides A and B must be on the same ESXi version.
Cisco Unified Communications Manager	• Unified CM 10.0(1) and later maintenance releases • Unified CM 10.5(1) and later maintenance releases • Unified CM 11.0(a) and later maintenance releases • Unified CM 11.5(1) and later maintenance releases • Unified CM 12.0 and later maintenance releases

Item	Requirement
Contact Center Software licenses	• Upgrade Unified CVP license using the Cisco Product Upgrade tool (PUT) • Upgrade the Unified Communications Manager license using the Communications Manager interface.

Item	Requirement

Third-party software licenses	• Microsoft Windows Server 2012 R2 Standard licenses & media for each Windows 2008 R2 Operating System upgrade:
	  • 10 licenses for on-box VMs, including optional Unified CVP Reporting server
	  • 1 license for optional external Unified CVP Reporting Server
	  • 1 license for each optional External AW-HDS-DDS
	• Microsoft Windows Server 2012 R2 Standard licenses and media for each of the following:
	  • 1 Virtual OS license for each of the required Unified Rogger, PG, and AW-HDS-DDS servers (6 licenses)
	  • 1 Virtual OS license for each of the required Unified CVP Servers (2 licenses)
	  • 1 Virtual OS license for each of the optional Unified CVP Reporting Servers (one on-box and one off-box—up to 2 licenses)
	  • 1 Virtual OS license for each of the optional External HDS servers (up to 2 licenses)
	  • 1 Virtual OS license for optional Enterprise Chat and Email
	• Microsoft SQL Server 2014 Standard licenses & media for SQL upgrade:
	  • 2 licenses for on-box Unified CCE Data Servers
	  • 1 license for each optional External HDS
	• Microsoft SQL Server 2014 Standard licenses and media for each of the following:
	  • 2 licenses for on-box Unified CCE AW-HDS-DDS servers
	  • 2 licenses for on-box Unified CCE Roggers
	  • 1 license for each optional External HDS
	  • 1 license for optional Enterprise Chat and Email

Note If you already have a SocialMiner added in the remote site, it is recommended to delete the SocialMiner from the remote site and add it as an External Machine in the Main site. For more information on how to delete and add an external machine, see the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.



CHAPTER 21

Packaged CCE 11.0(x) to 11.6 Upgrade

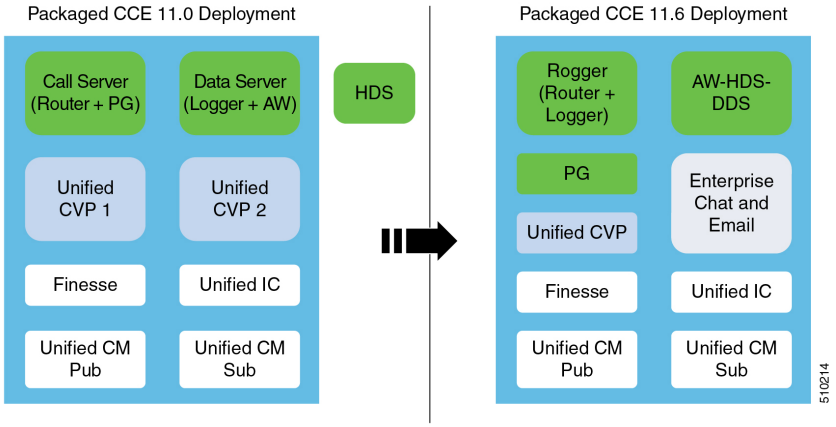
Common Ground Upgrade Process

The upgrade process for Packaged CCE is designed for minimal Contact Center downtime. While you are upgrading Side A, Side B remains operational. After you upgrade Side A, contact center activity resumes on Side A while you upgrade Side B.

In Release 11.5(1), Packaged CCE moved to a new deployment model (Packaged CCE: 2000 Agents). The upgrade process also includes steps to migrate to this new model.

The layout of the VMs on the hardware changes as shown in the following diagram.

Figure 1: Packaged CCE Deployment



Things to note include the following:

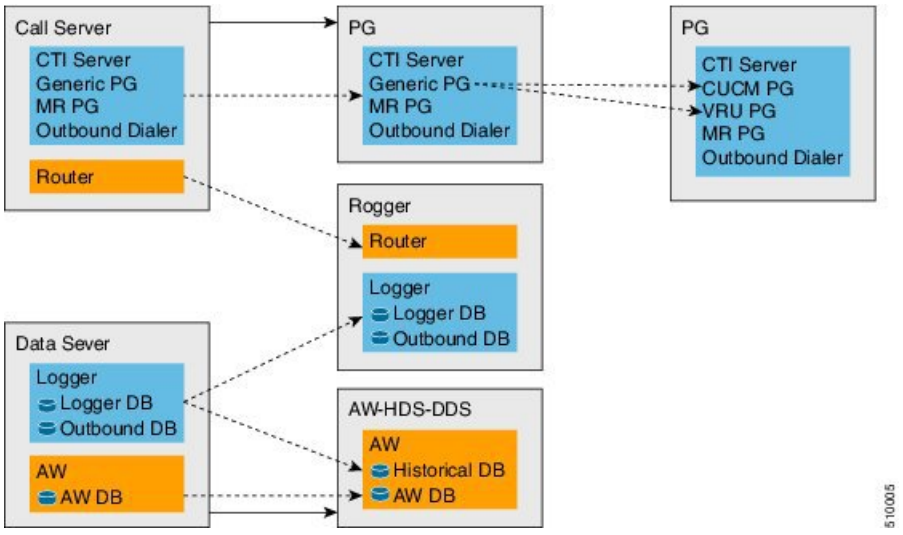
- The on-box Unified CCE Call Server and Data Server VMs change to on-box Unified CCE Rogger, PG, and AW-HDS-DDS.
- Two Unified CVP Servers are replaced with one Unified CVP Server that can support up to 3000 ports.
- Enterprise Chat and Email (ECE) can be coresident on box or deployed off box.

Note

- On-box ECE is supported on the B200 M4, C240 M4SX and C240 M5SX hardware only.

When you migrate to the Packaged CCE 2000 Agent model, the Unified CCE Call Server and Data Server are migrated as shown in the following diagram.

Figure 2: Packaged CCE Migration



Important The upgrade requires four maintenance windows:

- One maintenance window to shut down services on Side A to prepare for upgrade.
- A second maintenance window in the middle of the upgrade to cut over from Side B to Side A. You must bring down Side B before you bring up Side A.
- A third maintenance window after you upgrade Side B to synchronize Side A to Side B.
- A fourth maintenance window to finish migrating the Unified CCE Call Server to a Unified CCE PG.

This guide steps you through the upgrade and migration process for Packaged CCE, which includes the following major tasks:

- Meeting the system requirements for upgrade.
- Performing preupgrade tasks.
- Installing the Unified CCE Rogger.
- Migrating the Unified CCE Data Server to a Unified CCE AW-HDS-DDS.
- Migrating the Unified CCE Call Server to a Unified CCE PG.
- Upgrading all components on Side A.
- Cutting over from Side A to Side B, during which you bring Side B down and then bring Side A up.
- Migrating and upgrading all components on Side B.
- Synchronizing Side A and Side B.
- Performing postupgrade procedures.

Prerequisites and Important Considerations

- If your deployment includes Cisco Unified WIM and EIM, you must shut it down during the upgrade. Enterprise Chat and Email replaced Unified WIM and EIM in Release 11.5(1). Unified WIM and EIM is not supported with Packaged CCE 11.5(1) onwards. After the upgrade is complete, you can install Enterprise Chat and Email. See Install and Configure Enterprise Chat and Email, on page 133.
- Live Data does not work during the migration and upgrade.
- Outbound Option does not work while Side A is down.
- Make sure that you have backups of Side A and Side B Call Servers, Data Servers, and Unified CVP Servers before you begin your upgrade.
- Use the Disaster Recover System (DRS) application to back up Finesse and Unified Intelligence Center system data.
  - Finesse: To access the DRS application, direct your browser to `https://FQDN of Finesse server:8443/drf/`. For more information, see the online help provided with the DRS application.

- Unified Intelligence Center: To access the DRS application, direct your browser to `https://IP address of Unified Intelligence Center:8443/drf`. For more information, see the online help provided with the DRS application.

- After you begin the migration and upgrade process, you cannot back out of it. If you want to go back to the previous release, you must restore your VMs from your backup.
- Optionally, you can stage the Unified CCE Rogger off box before you begin the migration and upgrade to lessen your downtime.
- Plan out your hostnames. You may want to change the hostnames of the migrated Unified CCE components (Unified CCE Call Server, which becomes the Unified CCE PG, and Unified CCE Data Server, which becomes the Unified AW-HDS-DDS). If you change these hostnames, you must update them in other places (such as Finesse, PG Setup, and private network DNS entries).
- Make sure that you are running the minimum supported version of ESXi. For information about supported ESXi versions, see the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html*Virtualization for Cisco HCS for Contact Center* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/hcs_cc_virt.html.

Preupgrade Tasks

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

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

Note

- The minimum disk space required to perform the upgrade is 1500 MB.
- During the upgrade process, the installer takes a backup of the existing configuration database. This backup is available in `drive\temp\<instance name_logger side><schema version>`.

  For example: `C:\Temp\Inst_sideA181`

Step	Task
1.	In the Unified CCE Administration **System Inventory** tool, check the status of the alerts for the hosts and for each virtual machine (VM). Resolve any issues. Make sure that inventory alerts are at 0 before you continue.
2.	Shut down Enterprise Chat and Email (ECE).

Step	Task
Reduce the impact of Side A services shutdown. Stopping Side A services to upgrade the components may force agents to sign out of their desktops and cause IP phones to rehome. If customers require agents to be active during the upgrade, you can reduce the impact of Side A shutdown by completing these preupgrade tasks.	
3.	Force phones to rehome to the Side B Unified Communications Manager Subscriber. Perform this step if the device pool for the agent phones contains only the Side A Unified Communications Manager Subscriber 1. In Unified Communications Manager Administration, add the Side B Unified Communications Manager Subscriber 2 as preferred and change the Subscriber 1 to secondary. Reset the phones after you change the device pool. You can skip this step if the device pool for the agent phones is configured with the Side A Unified Communications Manager Subscriber 1 as preferred and the Side B Unified Communications Manager Subscriber 2 as secondary. When you shut down Side A, Unified Communications Manager forces logout for agents using phones logged in to Subscriber 1 and rehomes their phones to Subscriber 2.
4.	Direct agents to sign in to the Side B Finesse Secondary node.
5.	Configure the Cisco IOS Enterprise Ingress Voice Gateway dial-peer priority so that calls are sent to the Side B Unified CVP Servers first, and then to the Side A Unified CVP Servers.
6.	To maintain reporting capabilities during the Side A upgrade, configure Unified Intelligence Center historical and real-time data sources to one of the following: • Side B Unified CCE Data Server • External HDS with Side B as the Central Controller preferred side See Configure Unified Intelligence Center Data Sources for External AW-HDS-DDSHDS, on page 105 for steps to configure Unified Intelligence Center data sources. For the **Datasource Host** and **Database Name** fields, enter values for the Side B Unified CCE Data Server with Side B as the Central Controller preferred side.
Complete Finesse preupgrade tasks	
7.	Save your current desktop layout configuration. Sign in to Finesse Administration on the primary Finesse node (`https://FQDN of primary Finesse server/cfadmin`). Copy the layout XML file from the Manage Desktop Layout gadget on the **Desktop Settings** tab. Save it as a text file on your local system. **Note** If you are currently running the default layout, the layout automatically upgrades to the new layout. To use the layout from the previous version, copy and paste the layout XML to the Manage Desktop Layout gadget after the upgrade is complete.
Complete Unified CVP preupgrade tasks	

Step	Task
8.	Complete the Unified CVP Server and Operations Console preupgrade tasks on Unified CVP Server 1A, Unified CVP Server 1B, and the Unified CVP OAMP Server. You do not need to complete these tasks on Unified CVP Servers 2A and 2B because they are removed during the migration process. See Unified CVP Preupgrade Tasks, on page 158.
9.	Change the Unified CVP scripts as required so they do not point to DNs and labels on Unified CVP Server 2A.
Complete Unified Communications Manager preupgrade tasks	
10.	Complete Unified Communications Manager preupgrade tasks. See Unified Communications Manager Preupgrade Tasks, on page 158.

Unified CVP Preupgrade Tasks

Unified CVP Server and Unified CVP OAMP Server Preupgrade Tasks

Procedure

Step 1 Close all programs.

Step 2 Stop any third-party services and applications that are running on the server.

Step 3 Back up the `C:\Cisco\CVP` folder for all Unified CVP Servers.

Step 4 Back up the Operations Console as follows:

a) Log in to Operations Console.

b) On the Operations Console page, click **System** > **Export System Configuration** > **Export**, and save the CVP-OpsConsole-Backup.zip file.

c) Manually copy the sip.properties file from the directory `<CVP_HOME>\conf`. (Unified CVP Operations Console cannot export the sip.properties file.)

d) Copy the exported configuration and custom files onto network storage media or a portable storage media.

Unified Communications Manager Preupgrade Tasks

Procedure

Step 1 Ensure that you have the necessary license files for the new release.

Step 2 Back up your system. For more information, see the *Administration Guide for Cisco Unified Communications Manager* at this address: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Step 3 Obtain the upgrade file from Cisco.com and save it to an FTP or SFTP server. Folder names and filenames that you enter to access the upgrade file are case-sensitive. For more information, see the *Release Notes for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html

Prepare Side A for Upgrade

Before you begin, complete all tasks listed in Preupgrade Tasks, on page 156.

The user account that performs the upgrade must have access to PG Explorer and Network Trunk Group Explorer in Configuration Manager. Use the User List tool in Configuration Manager to provide access. For more information, see the Configuration 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.

Perform the tasks in the following table during a maintenance window and in the order they are listed.

Important Make sure that you have backups of all components before you proceed.

Step	Task
1.	Sign in to Unified CCE Administration on the Side A Unified CCE Data Server. Select **System** > **Deployment**. To seamlessly upgrade to the new hardware layout Packaged CCE adopted from release 11.5 onwards, ensure that you switch out of the Packaged CCE: CCE-PAC-M1 deployment mode and into **UCCE 4000 Agents Rogger**. After the upgrade you can switch to the PCCE deployment model you require. **Note** When you sign in to Unified CCE Administration, a screen appears that contains warnings about virtual machine mismatches. You can ignore these warnings and close the screen.
2.	Disable configuration changes. Set the following registry key to **1** on the Side A Unified CCE Call Server: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance` The change is replicated to the other side automatically.
3.	On each of the following VMs, select **Unified CCE Service Control** on the desktop. Stop the Unified CCE services and change **Startup** to **Manual**: • Side A Unified CCE Call Server • Side A Unified CCE Data Server • External HDS associated with Side A (if used)

Step	Task
4.	If Outbound Option is used, on the Side B Unified CCE Call Server, select **Unified CCE Service Control** on the desktop. Stop the Dialer service and change **Startup** to **Manual**. **Note** Outbound Option does not work while Side A is down because there is no redundancy for the Campaign Manager process.

Upgrade Side A

Migrate and Upgrade Side A

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

- In Unified CVP Diagnostic Portal, check that no Side A ports are in use.
- In the Unified Communications Manager RTMT tool, check that phones have migrated to Side B.

Make sure that you have completed all tasks listed in Prepare Side A for Upgrade, on page 159.

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

For best results, place upgrade media ISOs on local data stores. Make sure to remove them when the upgrade is complete.

Step	Task
Upgrade the Side A Unified CVP VMs	
1.	Update the settings on the Unified CVP OAMP server VM. See Update VMware Settings for the Unified CVP OAMP Server, on page 168.
2.	Upgrade the Unified CVP OAMP Server. See Upgrade the Unified CVP Operations Console, on page 169.
3.	Update the settings on the Unified CVP Server 1A VM. See Update VMware Settings for the Unified CVP Server , on page 166.
4.	Upgrade Unified CVP Server 1A. See Upgrade the Unified CVP Server, on page 167.

Step	Task
5.	Remove the Unified CVP Server 2A VM. **Note** Delete the Call Server, Media Server, and VXML Server from the Unified CVP OAMP Server before removing the Unified CVP Server 2A VM.
6.	Update the Cisco IOS Enterprise Ingress Voice Gateway dial-peer configuration to remove Unified CVP Server 2A.
7.	Obtain and transfer the license now if you don't have an external Unified CVP Reporting Server. For an external Unified CVP Reporting Server, you can transfer the upgrade license to all Unified CVP components after you upgrade the external server. See Obtain and Transfer the Upgrade License for Unified CVP, on page 169.
8.	Transfer scripts and media files to the gateways not currently being used by Side B. If all gateways are being used, perform this step during the cutover to Side B. See Transfer Unified CVP Scripts and Media Files, on page 80. **Note** You must manually configure the Unified CVP properties files based on the upgrade path. For more information, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.
Upgrade Side A Cisco Voice Gateway IOS Version if needed	
9.	Upgrade the Side A Cisco Voice Gateway IOS version to the minimum required by the upgraded Packaged CCE release (or later). See Upgrade Cisco Voice Gateway IOS Version, on page 170. See the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for IOS support information.
Upgrade External Unified CVP Reporting Server (if used)	
10.	Complete the Unified CVP Reporting Server preupgrade tasks. See Unified CVP Reporting Server Preupgrade Tasks, on page 171.
11.	Unload the data from the Unified CVP Reporting Server. See Unload Data From Reporting Database, on page 171.
12.	Uninstall the Unified CVP Reporting Server. See Uninstall the Unified CVP Component from the Reporting Server VM, on page 172.
13.	Update the settings on the Unified CVP Reporting Server VM. See Update VMware Settings for the Unified CVP Reporting Server, on page 172.

Step	Task
14.	Install the External Unified CVP Reporting Server. See Install Cisco Unified CVP Reporting Server, on page 56.
15	Load data on the Unified CVP Reporting Server. See Load Data to Reporting Server Database, on page 173.
16.	Save and deploy the Unified CVP Reporting Server in the Operations Console. See Save and Deploy the Unified CVP Reporting Server, on page 174.
17.	Transfer the upgrade license. See Obtain and Transfer the Upgrade License for Unified CVP, on page 169.
Upgrade the Side A Finesse and Unified Intelligence Center VMs	
18.	Upgrade the VMware version on the Finesse Primary VM. See Upgrade the Virtual Machine Hardware Version, on page 174.
19.	Update the settings on the Finesse Primary VM. See Update VMware Settings for Cisco Finesse, on page 174.
20.	Upgrade the Finesse Primary node. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176.
21.	Upgrade the VMware version on the Unified Intelligence Center Publisher VM. See Upgrade the Virtual Machine Hardware Version, on page 174.
22.	Update the settings on the Unified Intelligence Center Publisher VM. See Update VMware Settings for Cisco Unified Intelligence Center, on page 175.
23.	Upgrade the Unified Intelligence Center Publisher node. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176. **Note** Your configuration information migrates automatically to the upgraded version in the active partition.
Prepare for Side A Migration to Packaged CCE 2000 Agent Rogger Deployment	
24.	Back up and export the Logger database and the Outbound Option (if used) pccebaA database. See Back Up Database, on page 177.

Step	Task
25.	Back up and export your network configuration. See Back Up Network Configuration, on page 177.
Install the Side A Unified CCE Rogger (if not previously staged off box)	
26.	Create a VM for the Side A Unified CCE Rogger. Using Packaged-CCE-UCCE.ova, Create a Virtual Machine from the OVA, on page 38. Select **Rogger** from the drop-down list.
27.	Install Microsoft Windows Server on the Side A Unified CCE Rogger VM. See Install Microsoft Windows Server, on page 45.
28.	Install VMware tools on the Side A Unified CCE Rogger VM. See Install VMware Tools, on page 47.
29.	Configure the network adapters for the Side A Unified CCE Rogger. See Configure Network Adapters for Unified CCE Rogger and Unified CCE PG, on page 47 .
30.	Install antivirus software on the Side A Unified CCE Rogger. See Install Antivirus Software, on page 43.
31.	Configure the database drive for the Side A Unified CCE Rogger. See Configure Database Drive, on page 41.
32.	Set persistent static routes. See Set Persistent Static Routes, on page 49.
33.	Run Windows updates. See Run Windows Updates, on page 50.
34.	Add the Unified CCE Rogger to the domain.
35.	Install Microsoft SQL Server. Install Microsoft SQL Server, on page 50.
36.	Install Cisco Unified Contact Center Enterprise Release 11.0(1). See Install Cisco Unified Contact Center Enterprise, on page 54.
Configure the Side A Unified CCE Rogger	
37.	Add a UCCE Instance in Web Setup. See Add a UCCE Instance, on page 177.
38.	Configure SQL Server for the Logger database on the Unified CCE Rogger. See Configure SQL Server for CCE Components, on page 69.

Step	Task
39.	Configure the Logger database and log. See Configure the Logger Database and Log, on page 178.
40.	Import the Logger and Outbound Option databases that you backed up and exported in step 24. See Import the Logger and Outbound Databases, on page 178.
41.	Add a Unified CCE Router component in Web Setup. See Add a Unified CCE Router Component, on page 179.
42.	Add a Unified CCE Logger component in Web Setup. See Add a Unified CCE Logger Component, on page 180.
Convert the Side A Unified CCE Data Server and Unified CCE Call Server	
43.	Upgrade the VMware version on the Side A Data Server VM. See Upgrade the Virtual Machine Hardware Version, on page 174.
44.	Update the settings on the Side A Data Server VM. See Update VMware Settings on the Unified CCE Data Server, on page 181.
46.	Convert the Side A Unified CCE Data Server to a Unified CCE AW-HDS-DDS. See Convert Unified CCE Data Server to Unified CCE AW-HDS-DDS, on page 182.
47.	Update the real-time and historical datasources for Unified Intelligence Center to point to the Unified CCE AW-HDS-DDS. You must update the historical data source database name from <*instancename*>_sideA to <*instancename*>_awdb.
48.	Upgrade the VMware version on the Side A Call Server VM. See Upgrade the Virtual Machine Hardware Version, on page 174.
49.	Update the settings on the Side A Call Server VM. See Update VMware Settings on the Unified CCE Call Server, on page 183.
50.	Remove the Router from the Side A Unified CCE Call Server. See Remove the Router from the Unified CCE Call Server, on page 184. The Call Server is now a PG.
51.	Run the Unified CCE Release 11.6(1) installer on the Side A Unified CCE Rogger. See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
52.	Disable configuration changes on the Unified CCE Rogger. Change the following registry key to 1: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance`

Step	Task
53.	Run the Unified CCE Release 11.6(1) installer on the Side A Unified CCE AW-HDS-DDS (former Data Server). See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
54.	Run the Unified CCE 11.6(1) installer on the Side A PG (former Call Server). See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
55.	Modify the Side A PG to point to the Unified CCE Rogger. See Modify the PG, on page 184.
56.	Modify the dialer to point to the Unified CCE Rogger (if using Outbound Option). See Modify the Dialer, on page 184.
Optional: Upgrade the External HDS associated with Side A (if used)	
57.	Upgrade the VMware version on the External HDS associated with Side A. See Upgrade the Virtual Machine Hardware Version, on page 174.
58.	Run the Unified CCE Release 11.6(1) installer the External HDS associated with Side A. See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
59.	Update the Central Controller connectivity to point to the Unified CCE Rogger. See Update the Central Controller Connectivity, on page 184.
Optional: Install language pack	
60.	Install the language pack on the Side A Unified CCE Rogger, AW-HDS-DDS (former Data Server), PG (former Call Server), and External HDS associated with Side A (if used). See Install the Language Pack, on page 185.
Upgrade the Side A Unified Communications Manager Publisher and Subscriber 1	
61.	Upgrade the Side A Unified Communications Manager Publisher. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176.
62.	Upgrade the Side A Unified Communications Manager Subscriber 1. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176. **Important** The Unified CM Publisher upgrade must be complete and the new release software must be the active version before you upgrade the Unified CM Subscriber.

Step	Task
63.	Upgrade the Unified Communications Manager License. See Upgrade Unified Communications Manager License, on page 185.
64.	Upgrade JTAPI on the Side A PG (former Call Server). See Upgrade JTAPI on the PG, on page 187. **Important** If you are installing CUCM 12.5, install Cisco JTAPI Client on CUCM. See Install Cisco JTAPI Client on PG, on page 186.
Optional: Change hostnames of the Unified CCE components	
65.	Optional: Change the hostnames of the Unified CCE components (AW-HDS-DDS and PG). **Note** You can perform this task when you reboot each component as part of the upgrade. If you do change the hostnames, also change them in the following places: • Cisco Finesse • PG Setup • Unified Intelligence Center - Historical and real-time • Private network DNS entries • Live Data—If you change the hostname of the AW-HDS-DDS (former Data Server), Live Data no longer connects to the AW-HDS-DDS after the Data Server hostname is removed from DNS. To fix this, do the following: 1. Run the following CLI command on the CUIC-LD-IdS Publisher: **unset live-data aw-access primary** 2. Restart Cisco Tomcat on the Side A AW-HDS-DDS.

Cisco Unified Customer Voice Portal Upgrade Procedures

Update VMware Settings for the Unified CVP Server

Update the virtual machine settings on the Unified CVP Servers 1A and 1B to match the OVA file.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Select the hard disk to modify. In the **Disk Provisioning** pane, increase the provisioned size to 250 GB.

b) Click **Memory** and update the **Memory Size** to 10 GB .

c) Click **Video Card** and update the **Total video memory** to 8 MB.

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** to 3000 MHz.

b) Click **Memory** and update the **Reservation** to 10240 MB.

Step 5 Click **OK** to save your changes.

Step 6 Power on the virtual machine.

Step 7 Open the **Disk Management Tool** (right-click **Start** and choose **Disk Management** from the context menu).

Step 8 Select the C drive.

Step 9 In the **Disk 0** row, right- click **(C:)** and select **Extend Volume**.

The Extend Volume Wizard opens.

Step 10 Click **Next**.

Step 11 Accept the default settings and click **Next**.

Step 12 Click **Finish**.

Step 13 Restart the server.

Upgrade the Unified CVP Server

When you upgrade the Unified CVP Server, you must upgrade Unified Call Studio to the same version.

You can upgrade all Unified CVP nodes on the same side in parallel.

Procedure

Step 1 To retain the default media file format for this Unified CVP release, which is U-Law, skip the next two steps and proceed to Step 4.

Step 2 If you are changing from the U-Law to A-Law format:

a) Navigate to the `C:\Cisco\CVP\conf` location.

b) Convert the custom media files, such as custom applications and Whisper Agent-Agent Greeting (WAAG), and applications that are in U-Law to A-Law.

c) In the `cvp_pkgs.properties` file, add the **cvp-pkgs.PromptEncodeFormatALaw = 1** property at line 7 to enable the A-Law flag.

Note Ensure that you leave a space before and after the "=" sign.

Step 3 If you are changing from U-Law or A-Law to G729 format:

a) Navigate to the `C:\Cisco\CVP\conf` location.

b) In the `cvp_pkgs.properties` file, add the **cvp-pkgs.PromptEncodeFormatG729 = 1** property at line 7 to enable the G729 flag.

Note Ensure that you leave a space before and after the "=" sign.

Step 4 Mount the Unified CVP ISO image.

Step 5 From the CVP\Installer_Windows folder of the new release of Unified CVP installation DVD, run **setup.exe**.

Follow the prompts as the installer guides you through the upgrade process.

Step 6 Restart the server.

What to do next

1. Transfer script and media files:
   a. Log in to the Operations Console and select **Bulk Administration** > **File Transfer** > **Scripts and Media**.
   b. In the **Select device type** field, select the Gateway.
   c. Move all Gateways to **Selected**.
   d. Select **Default Gateway files**.
   e. Select **Transfer**, and then select **OK** on the popup window.

Note If you have separate Ingress and VXML gateways, you must select the appropriate files and script for each component.

   f. After configuring the application services in the gateways, log in to the gateway and use the Cisco IOS CLI command **call application voice load <service_Name>** to load the gateway download transferred files into the Cisco IOS memory for each Unified CVP service.
2. Restore any backed-up third-party libraries.
3. Re-license Unified CVP Servers with a license for the new version.

Restore any backed-up third-party libraries.

Related Topics

Upgrade Unified Call Studio, on page 205
Mount and Unmount ISO Files, on page 37

Update VMware Settings for the Unified CVP OAMP Server

Update the virtual machine settings on the Unified CVP Reporting Server to match the OVA file.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.
   a) Click **Memory** and update the **Memory Size** to 4 GB.
   b) Click **Video Card** and update the **Total video memory** to 8 MB.

Step 4 Click the **Resources** tab.

a) Click **Memory** and update the **Reservation** field to 4096 MB.

Step 5 Click **OK** to save your changes.

Step 6 Power on the virtual machine.

Upgrade the Unified CVP Operations Console

The default media files are overwritten during the Unified CVP upgrade. Customized media files, such as whisper announcements and agent greetings, are not overwritten; they retain the format they had in previous releases.

Procedure

Step 1 To retain the default media file format for this Unified CVP release, which is U-Law, skip the next two steps and proceed to Step 4.

Step 2 If you are changing from the U-Law to A-Law format:

a) Navigate to the `C:\Cisco\CVP\conf` location.

b) Convert the custom media files, such as custom applications and Whisper Agent-Agent Greeting (WAAG), and applications that are in U-Law to A-Law.

c) In the `cvp_pkgs.properties` file, add the **cvp-pkgs.PromptEncodeFormatALaw = 1** property at line 7 to enable the A-Law flag.

Note Ensure that you leave a space before and after the "=" sign.

Step 3 If you are changing from U-Law or A-Law to G729 format:

a) Navigate to the `C:\Cisco\CVP\conf` location.

b) In the `cvp_pkgs.properties` file, add the **cvp-pkgs.PromptEncodeFormatG729 = 1** property at line 7 to enable the G729 flag.

Note Ensure that you leave a space before and after the "=" sign.

Step 4 Mount the Unified CVP ISO image.

Step 5 From the `CVP\Installer_Windows` folder of the Unified CVP installation DVD for this release, run `setup.exe`.

Step 6 Follow the instructions on the screen.

Step 7 Restart the server.

Related Topics

Mount and Unmount ISO Files, on page 37

Obtain and Transfer the Upgrade License for Unified CVP

The Unified CVP Server and the Unified CVP Reporting Server require an updated license. The Operations Console runs without requiring a license.

Before you begin

To upgrade software, enter your contract number into the Cisco Product Upgrade Tool (PUT): https://tools.cisco.com/gct/Upgrade/jsp/index.jsp. If there is an entitlement to upgrade, the tool returns a Product Authorization Key (PAK); if not, the tool displays the option to purchase a PAK.

Use the PAK to generate a license file, using the Product License Registration Portal on Cisco.com: https://tools.cisco.com/SWIFT/LicensingUI/Home.

See Generate a License, on page 80 for instructions.

Save the license file locally so that you can transfer it using the Operations Console.

Procedure

Step 1 In the Operation Console, go to **Bulk Administration** > **File Transfer** > **Licenses**.

Step 2 In the **Device Association** panel, select the device type from the drop-down list. For example select Unified CVP Reporting Server or Unified CVP Server.

Step 3 Move the objects you want to license from **Available** to **Selected**.

Step 4 In the Licenses Files panel, select **Select new file** and then browse to the location where you saved the upgrade license.

Step 5 Click **Transfer**.

Cisco Enterprise Voice Gateway Upgrade Procedures

Upgrade Cisco Voice Gateway IOS Version

Perform this procedure for each gateway on the side you are upgrading.

Upgrade the Cisco Voice Gateway IOS version to the minimum version required by this release. See the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for IOS support information.

For more information, see https://www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/upgrade.pdf.

Procedure

Step 1 Copy the new image from the remote TFTP server into flash memory, making sure that you specify your own TFTP server's IP address and Cisco IOS filename.

Step 2 Verify that the new image was downloaded.

Step 3 Boot using the new image. Update the gateway config to boot using the new version.

Step 4 Reload the gateway to use the new image.

Unified CVP Reporting Server Upgrade Procedures

Unified CVP Reporting Server Preupgrade Tasks

Procedure

Step 1 Back up the Informix database by running C:\Cisco\CVP\bin\cvpbackup.bat.

This backs up the database to E:\cvp-db-backup\cvp-backup-data.gz.

Step 2 Turn off the scheduled purge, as follows:

a) Open **Administrative Tools** > **Task Scheduler**.
b) In the **Active Tasks**, double-click one of the Unified CVP tasks.
c) Select all of the Unified CVP-related tasks, right-click, and choose **Disable**

Step 3 Ensure that Unified CVP Reporting Server is not part of any domain and is part of a workgroup. Add it to the domain after the upgrade, if necessary.

Unload Data From Reporting Database

Note While the Cisco CVP CallServer service is stopped, no reporting data is sent to the Unified CVP Reporting Server.

Procedure

Step 1 Log in to the Unified CVP Reporting Server as 'cvp_dbadmin' user.

Step 2 Stop the **Cisco CVP Call Server** service from the Windows Service Manager.

Note Ensure that enough disk space is available to unload data. To check the disk space (in MB), run the query:

```
select sum(tabsize(tabname)) from systables where tabid>99
```

Step 3 Access the Unified CVP installation file.

Step 4 From the command prompt, change the directory to the migration folder.

Note You can also copy the migration folder to local disk and run the unload script directly.

Step 5 Locate the `migrate_unload.bat` file.

By default, the data is exported to `c:\migration`. Ensure that this path exists. If you want to change the default path, then update the path in *unl.sql*:

```
create procedure unld(path char(128) default "c:\migration\") RETURNING char(128)
```

Step 6 Run the following command to unload the Reporting Server database:

```
migrate_unload.bat
```

Note You must run this command as an administrator.

After running the script, a set of .unl files is created under the path provided. The .unl files are exported to `c:\migration` folder. This folder must have full access permission for cvp_dbadmin user.

Step 7 Copy the exported migration folder to the Unified CVP Reporting Server database.

Note Reduce the retention period for data and execute a purge to reduce the data to migrate.

Step 8 Start **Cisco CVP Call Server** service from Windows Service Manager.

Uninstall the Unified CVP Component from the Reporting Server VM

Before you begin

- Shut down all applications and close all open files.
- Close the Unified CVP component and related files.

Procedure

Step 1 Click **Start** > **Control Panel** > **Programs and Features**.

Step 2 Click **Cisco Unified Customer Voice Portal / Cisco Unified Call Studio**, and then click **Uninstall**.

Step 3 Click **Next**.

After uninstallation, the **Uninstall Complete** screen appears. Reboot the server.

Note The Unified CVP uninstallation procedure does not clean up all the files and folders, such as log files, media files, and folders that are generated postinstallation. Media folders with same names are replaced during the CVP installation process. User-created media files and folders remain unchanged during CVP upgrade. Create all the media folders in `wwwroot` and use the relative paths to simplify the migration process for the future releases that support a-law and mu-law files.

Update VMware Settings for the Unified CVP Reporting Server

Update the virtual machine settings on the Unified CVP Reporting Server to match the OVA file.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Select the hard disk to modify (C drive). In the **Disk Provisioning** pane, increase the provisioned size to 80 GB.
b) Click **Memory** and update the **Memory Size** to 6 GB.
c) Click **Video Card** and update the **Total video memory** to 8 MB.

Step 4 Click the **Resources** tab.
a) Click **Memory** and update the **Reservation** field to 6144 MB.

Step 5 Click **OK** to save your changes.

Step 6 Power on the virtual machine.

Step 7 Open the **Disk Management Tool** (right-click **Start** and choose **Disk Management** from the context menu).

Step 8 Select the C drive.

Step 9 In the **Disk 0** row, right- click **(C:)** and select **Extend Volume**.

The Extend Volume Wizard opens.

Step 10 Click **Next**.

Step 11 Accept the default settings and click **Next**.

Step 12 Click **Finish**.

Step 13 Restart the server.

Load Data to Reporting Server Database

Procedure

Step 1 Open the Unified CVP installation file.

Step 2 Stop **Cisco CVP Call Server** service from Windows Service Manager.

Step 3 Go to **CVP** > **Migration**.

Step 4 Copy the migration folder to the local disk and run the load script directly. From the command prompt, change the directory to the migration folder.

Step 5 On the local disk, locate the .unl files that you want to load into the Unified CVP database and copy them into the migration folder.

Step 6 Run the following command as an administrator to load the Unified CVP database: `migrate_load.bat`

Note If the .unl files are located in `c:\migration`, you must run the script load as `migrate_load.bat`.

This script loads all the three Unified CVP Reporting databases with the previous call data to the Unified CVP Reporting database.

Note The load runs at a rate of about 1.5GB/hour.

Step 7 Start **Cisco CVP Call Server** service from Windows Service Manager.

Save and Deploy the Unified CVP Reporting Server

Procedure

Step 1 On the Unified CVP OAMP server, open the Operations Console and log in.
Step 2 Navigate to **Device Management** > **Unified CVP Reporting Server**.
Step 3 Click the hostname of the Unified CVP Reporting Server.
Step 4 Click **Save and Deploy**.

Common Software Upgrade Procedures

Upgrade the Virtual Machine Hardware Version

Perform the following procedure on the VSphere Web Client on the Finesse and Unified Intelligence Center VMs.

Procedure

Step 1 Shut down the virtual machine.
Step 2 Right-click the virtual machine and choose **Compatibility > Upgrade VM Compatibility**.
Step 3 Click **Yes** to confirm upgrade.
Step 4 From the **Compatible with (*)** drop-down list, choose **ESXi 5.1 and later**.
Step 5 Click **OK** to save the settings.
Step 6 Power on the virtual machine.

Update VMware Settings for Cisco Finesse

Update the virtual machine settings for the Finesse Primary and Finesse Secondary VMs to match the OVA file.

Procedure

Step 1 Use the following CLI command to shut down the virtual machine: **utils system shutdown**
Step 2 Right-click the virtual machine and choose **Edit Settings**.
Step 3 Click the **Hardware** tab.
a) Click **Memory** and update the **Memory Size** to 10 GB.
Step 4 Click the **Resources** tab.
a) Click **CPU** and update the **Reservation** field to 5000 MHz.
b) Click **Memory** and update the **Reservation** field to 10240 MB.

Step 5 Click **OK**.

Step 6 Power on the virtual machine.

Update VMware Settings for Cisco Unified Intelligence Center

Update the settings on the Unified Intelligence Center Publisher and Subscriber to match the OVA file.

Procedure

Step 1 Use the following CLI command to shut down the virtual machine: **utils system shutdown**

Step 2 Right-click the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Select the hard disk to modify. In the **Disk Provisioning** pane, change the **Provisioned Size** to 200 GB.
b) Click **Memory** and update the **Memory Size** to 16 GB.

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** field to 5500 MHz.
b) Click **Memory** and update the **Reservation** field to 16384 MB.

Step 5 Click **OK** to save your changes.

Step 6 Power on the virtual machine.

Upgrade VOS-Based Contact Center Applications from DVD/CD

Finesse and Unified Intelligence Center 11.0 support aligned partitions, but only with a fresh installation. When you upgrade from a previous release, the platform detects the unaligned partitions and displays the following error: `ERROR-UNSUPPORTED: Partitions unaligned`.

You can run Finesse and Unified Intelligence Center with the unaligned partitions without functional impact. To experience the benefits of aligned partitions, you must you perform a fresh installation after upgrade.

Procedure

Step 1 SSH to the Finesse, Unified Intelligence Center, or Unified Communications Manager system, or open it in the VM console in VSphere.

Step 2 Log in with the platform administration account.

Step 3 Mount the ISO image.

Step 4 From the CLI, run the command **utils system upgrade initiate**.

Step 5 Choose **Local DVD/CD**. Follow the instructions provided by the `utils system upgrade initiate` command.

Step 6 Enter SMTP server information when prompted. If you do not have an SMTP server, skip this step.

Step 7 At the Automatically switch versions if the upgrade is successful prompt, type **`yes`**.

Step 8 After the upgrade is complete, disconnect the CD/DVD drive by unmounting the ISO.

Step 9 Verify that the upgrade was successful, as follows:

- **Finesse:** Sign in to the Finesse Agent Desktop (`https://<FQDN of Finesse server>/desktop`).

  Note After Finesse restarts, wait approximately 20 minutes before signing in to the desktop.

- **Unified Intelligence Center:** Sign in to Unified Intelligence Center (`https://<hostname>:8444/cuic`).
- **Unified Communications Manager:** Verify on the sign-in screen in the console.

Related Topics

Mount and Unmount ISO Files, on page 37

Upgrade VOS-Based Contact Center Applications from a Remote File System

Finesse and Unified Intelligence Center 11.0 support aligned partitions, but only with a fresh installation. When you upgrade from a previous release, the platform detects the unaligned partitions and displays the following error: `ERROR-UNSUPPORTED: Partitions unaligned`.

You can run Finesse and Unified Intelligence Center with the unaligned partitions without functional impact. To experience the benefits of aligned partitions, you must you perform a fresh installation after upgrade.

Procedure

Step 1 SSH to your Finesse, Unified Intelligence Center, or Unified Communications Manager system, or open it in the VM console in VSphere.

Step 2 Log in with the platform administration account.

Step 3 From the CLI, run the command **utils system upgrade initiate**.

Step 4 Choose **SFTP** or **FTP**.

Step 5 Follow the instructions provided by the `utils system upgrade initiate` command.

Step 6 Provide the location and credentials for the remote site.

Step 7 Enter SMTP server information when prompted. If you do not have an SMTP server, skip this step.

Step 8 At the Automatically switch versions if the upgrade is successful prompt, type **`yes`**.

Step 9 Verify that the upgrade was successful, as follows:

- **Finesse:** Sign in to the Finesse Agent Desktop (`https://<FQDN of Finesse server>/desktop`).

  Note After Finesse restarts, wait approximately 20 minutes before signing in to the desktop.

- **Unified Intelligence Center:** Sign in to Unified Intelligence Center (`https://<hostname>:8444/cuic`).
- **Unified Communications Manager:** Verify on the sign-in screen in the console.

Migration Procedures

Back Up Database

You must perform both a SQL backup of the Logger database and an ICMDBA backup of the configuration from the Logger database on the Data Server. Later in the migration process, the configuration backup will be imported into the Unified CCE Rogger. The SQL backup, which contains the historical data, will be imported into the Unified CCE AW-HDS-DDS.

Back up the databases on to a network share.

Procedure

Step 1 Use Microsoft SQL Server Backup and Restore utilities to back up and export the Logger and Outbound Option (if used) databases.

You can then use the backup to restore the historical data to the Unified CCE AW-HDS-DDS.

Step 2 On Side A, use ICMDBA to export the Logger database.

Note When upgrading side B, ensure ICMDBA export is performed from the Side B Logger database.

Step 3 Note the HDS customizable values.

Step 4 Copy the backup files to a shared location.

Back Up Network Configuration

Back up your network configuration to use when setting persistent static routes on the Unified CCE Rogger.

Procedure

Make note of the local static route configuration on the Unified CCE Call Server.

When you install and configure the Unified CCE Rogger, configure the local static routes to match this configuration.

Note This procedure assumes that the private network will be the same.

Configure Unified CCE Rogger

Add a UCCE Instance

Procedure

Step 1 Launch **Web Setup** in the VM you want installed or upgraded.

Step 2 Sign in as a domain user with local administrator permission.

Step 3 Click **Instance Management** and then click **Add**.

Step 4 In the **Add Instance** dialog box, choose the customer facility and instance.

Step 5 In the **Instance Number** field, enter 0.

Step 6 Click **Save**.

Configure the Logger Database and Log

Procedure

Step 1 Launch **ICMdba**.

Step 2 Navigate to **Server** > **Instance**.

Step 3 Right-click the instance name and choose **Create**.

Step 4 In the **Select Component** dialog box, choose the logger you are working on (Logger A or Logger B). Click **OK**.

Step 5 At the prompt "SQL Server is not configured properly. Do you want to configure it now?", click **Yes**.

Step 6 On the **Configure** page, in the **SQL Server Configurations** pane, check the defaults for Memory (MB) and Recovery Interval. Click **OK**.

Step 7 On the **Stop Server** page, click **Yes** to stop the services.

Step 8 In the **Select Logger Type** dialog box, choose **Enterprise**. Click **OK** to open the **Create Database** dialog box.

Step 9 Create the Logger database and log as follows:

a) In the **DB Type** field, choose the side (A or B).
b) In the **Storage** pane, click **Add**.
c) Click **Data**.
d) Choose the E drive.
e) Enter 130000 MB in the **Size** field.
f) Click **OK** to return to the **Create Database** dialog box.
g) Click **Add** again.
h) Choose the E drive.
i) Enter 3072 MB in the **Size** field.
j) Click **OK** to return to the **Create Database** dialog box.

Step 10 In the **Create Database** dialog box, click **Create**. Then click **Start**.

When you see the successful creation message, click **OK** and then **Close**.

Import the Logger and Outbound Databases

Import the Logger and Outbound Option (if used) databases that you previously exported to a network share.

Note Do not import the SQL backup of the Logger database into the Unified CCE Rogger. The SQL backup contains the historical data from the Data Server. Depending on the amount of data, it may be larger than the allocated disk size on the Rogger VM.

Procedure

Step 1 Launch **ICMdba**.

Step 2 Select the Unified CCE Rogger VM under Servers and expand the tree to <*instance name*>_sideA.

Step 3 Choose **Data** > **Import**.

Step 4 Browse to the location where you stored the backup of the Logger database and click **Open**.

Step 5 Click **OK** and then click **Import**.

Step 6 Click **Start** and then click **OK** on all messages that appear.

Step 7 Repeat the above steps for Side B.

Step 8 If you use Outbound Option and want to keep your Outbound Option customer database, restore the database with the Microsoft SQL Server Backup and Restore utilities. Repeat to set up Outbound Option database for Side B.

For more information see the *Outbound Option Guide for Unified Contact Center Enterprise* guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

Note Size of the Outbound Option database should not exceed 10 GB.

During the Technology Refresh upgrade, run the EDMT tool for each of the Logger and HDS databases to migrate data to the new version.

For detailed information on running the EDMT tool to migrate the data, see *Synchronizing or Updating Data from Logger or HDS Production Server to Staged 12.0(1) Server During Cut-over* in the at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

For detailed information on running the EDMT tool to migrate the data, see *Synchronizing or Updating Data from Logger or HDS Production Server to Staged 12.5(1) Server During Cut-over* in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide, Release 12.5(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Add a Unified CCE Router Component

Procedure

Step 1 Launch **Web Setup**.

Step 2 Choose **Component Management** > **Routers**.

Step 3 Click **Add**.

Step 4 On the **Deployment** page:

a) Select the appropriate side (Side A or Side B).
b) Select **Duplexed**.
c) Click **Next**.

Step 5 On the **Router Connectivity** page:

a) Configure the Private Interfaces and Public (Visible) Interfaces. Use the same hostname for Side A Normal and High Priority and the same hostname for Side B Normal and High Priority.
b) Click **Next**.

Step 6 On the **Enable Peripheral Gateways** page:

a) In the **Enable Peripheral Gateways** field, enter 1-3.
b) Click **Next**.

Step 7 On the **Router Options** page:

a) Check the **Enable Quality of Service (QoS)** check box.
b) Check the **Enable Application Gateway** check box.
c) Click **Next**.

Note This step applies to Side A only.

Step 8 On the **Router Quality of Service** page, accept the default values and click **Next**.

Step 9 On the **Summary** page, confirm the Router Summary is correct and then click **Finish**.

Add a Unified CCE Logger Component

You can (optionally) configure the Logger to enable Outbound Option and Outbound Option High Availability. Outbound Option High Availability facilitates two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Use the ICMDBA tool to create an outbound database on Side A and Side B; then set up the replication by using Web Setup.

Note Before you configure the Logger for Outbound Option High Availability:

- Create a Microsoft SQL Server user and assign that user the sysadmin privilege. You must use the same username and password on Logger Side A and Logger Side B. (You use this username and password in the following procedure to configure Outbound Option and enable Outbound Option High Availability.)
- Assign the sysadmin privilege to the NT authority/System user.

Procedure

Step 1 Launch **Web Setup**.

Step 2 Choose **Component Management** > **Loggers**.

Step 3 Click **Add**. Choose the Instance.

Step 4 On the **Deployment** page:
a) Select the appropriate side (Side A or Side B).
b) Select **Duplexed**.
c) Click **Next**.

Step 5 On the **Central Controller Connectivity** page:
a) Enter the hostnames for Side A and Side B for the Router Private Interface and Logger Private Interface.
b) Click **Next**.

Step 6 On the **Additional Options** page, click the **Enable Outbound Option** check box.

Step 7 Click the **Enable High Availability** check box to enable Outbound Option High Availability on the Logger.Checking this check box enables Outbound Option High Availability two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Two-way replication requires that you check this check box on the Additional Options page for both Logger Side A and Side B. If you disable two-way replication on one side, you must also disable it on the other side. You must enable Outbound Option in order to enable Outbound Option High Availability. Similarly, if you want to disable Outbound Option and you have enabled Outbound Option High Availability, you must disable High Availability (uncheck the **Enable High Availability** check box) before you can disable Outbound Option (uncheck the **Enable Outbound Option** check box).

Step 8 If you enable High Availability, enter a valid public server hostname address for **Logger Side A** and **Logger Side B**. Entering a server IP address instead of a server name is not allowed.

Step 9 If you enable High Availability, enter the **SQL Server Admin Credentials (Username and Password)**, which are required to establish two-way replication. The username and password must be the same on Logger Side A and Logger Side B, and the user must have the SQL Server System Admin privilege. SQL replication requires that the correct SQL system admin username and password be in place when setting up Outbound Option High Availability. Changing the password for the SQL user used to set up SQL replication in Outbound Option High Availability causes replication to fail until you disable High Availability and re-enable it with the new username and password. Because of this requirement, be careful about how andwhen you change the password for this user.

Step 10 Click **Next**.

Step 11 Review the **Summary** page, and click **Finish**.

Update VMware Settings on the Unified CCE Data Server

Update the virtual machine settings on the Side A and Side B Unified CCE Data Servers to match the OVA for the Unified CCE AW-HDS-DDS.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.
a) Click **Memory** and update the **Memory Size** to 16 GB.
b) Click **Video Card** and update the **Total video memory** to 8 MB.

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** field to 5000 MHz.
b) Click **Memory** and update the **Reservation** to 16384 MB.

Step 5 Click **OK** to save your changes.

Step 6 Power on the virtual machine.

Convert Unified CCE Data Server to Unified CCE AW-HDS-DDS

Before you begin

Make sure that you can restore from the network share to which you backed up the databases.

Stop the SQL Server service. Then, delete the SQL server data and log files to ensure that you have enough space to perform this procedure.

Procedure

Step 1 Rename the database.

a) Ensure that the SQL backup of the Side A Logger is copied to the AW-HDS-DDS network shared folder.
b) Restart the SQL Server service.
c) Open MS SQL Management Studio and run the following queries under the master database:

- `RESTORE FILELISTONLY from Disk='Path of the backup\<instancename>_sideA.bak'`

  Identify the logical filenames.

- ```
  Restore database <instance name>_hds
  from disk='Path of the backup\<instance name>_sideA.bak'
  with
  Move '<instancename>_sideA_data0' to
  'E:\MSSQL\DATA\<instancename>_hds_data0.mdf',
  Move '<instancename>_sideA_log0' to
  'E:\MSSQL\DATA\<instancename>_hds_log0.ldf',Stats=5
  ```

  Note Use the drive letter that the database is installed on.

  <instance name>_hds is the new database instance and <instance name>_sideA_data0 and log0 filenames are the results from the previous query.

d) In the **SQL Management Studio** window, select the <instance name>_hds database. Click **Properties**, and then select the **Files** pane. Change the logical filenames according to the HDS database:

- `<instance name>_sideA-log0` to `<instance name>_hds_log0`
- `<instance name>_sideA_data0` to `<instancename>_hds_data0`

e) Open a new query tab for the `<instance name>_hds` database and run the following query:

- Truncate table Logger_Type
- Truncate table Recovery
- Truncate table Logger_Admin
  ```

Step 2 Edit the Distributor.

a) Open Web Setup.
b) Select **Component Management** > **Administration and Data server component**.
c) Edit the Administration and Data server component to convert it to AW-HDS-DDS, as follows:

- Change the **Server Role** from **AW** to **AW-HDS-DDS**.
- Change the **Central Controller Connectivity** for the Router and Logger to use the hostnames for the side A and B Unified CCE Rogger VMs.

Step 3 Remove the Logger.

a) Open Web Setup.
b) Select **Component Management** > **Logger component**.
c) Select **Logger** and then click **Delete**.

Step 4 Remove the network adapter previously used for the private network.

a) In vSphere Client, right-click the virtual machine and choose **Edit Settings**.
b) Click the **Hardware** tab.
c) Remove the network adapter associated with the private network.

Update VMware Settings on the Unified CCE Call Server

Update the virtual machine settings on the Side A and Side B Unified CCE Call Servers to match the OVA for the Unified CCE PG.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Click **CPUs**. Update the **Number of Virtual Sockets** to 2 and the **Cores per socket** to 1.
b) Click **Memory** and update the **Memory Size** to 6 GB.
c) Click **Video Card** and update the **Total video memory** to 8 MB.

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** field to 4000 MHz.
b) Click **Memory** and update the **Reservation** to 6144 MB.

Step 5 Click **OK** to save your changes.

Step 6 Power on the virtual machine.

Remove the Router from the Unified CCE Call Server

Procedure

Step 1 On the Unified CCE Call Server, open Web Setup.
Step 2 Select **Component Management** > **Router component**.
Step 3 Select **Router** and then click **Delete**.

Modify the PG

Procedure

Step 1 Open Peripheral Gateway Setup.
Step 2 Select **PG1**.
Step 3 Click **Edit**.
Step 4 Click **Next** until you reach the **Peripheral Gateway Network Interfaces** dialog box.
Step 5 Update the Side A and Side B Router visible interfaces to point to the Unified CCE Rogger VMs.
Step 6 Click **Finish**.
Step 7 Repeat Step 2 through Step 6 for PG2.

Modify the Dialer

Perform this procedure if you use Outbound Option.

Update the Central Controller Connectivity

Procedure

Step 1 Launch **Web Setup**.
Step 2 Choose **Component Management** > **Administration & Data Servers**.
Step 3 Check the **Administration & Data Server** check box and then click **Edit**.
Step 4 Click **Next** until you reach the Central Controller Connectivity page.
Step 5 On the Central Controller Connectivity page:
a) In the **Router Side A** and **Logger Side A** fields, enter the hostname of the Side A Rogger.
b) In the **Router Side B** and **Logger Side B** fields, enter the hostname of the Side B Rogger.
c) Click **Next**.
Step 6 Click **Finish**.

Install the Language Pack

If a customer requires a language other than the default (English), download the Packaged CCE Language Pack executable from the Unified Contact Center Download Software page.

Install Language Pack

Install the Language Pack on the Unified CCE Data Servers and on any External HDS servers after upgrading them.

After you install the Language Pack, the Unified CCE Administration Sign In page has a language drop-down menu that lists all available languages. Select a language to display the user interface and the online help in that language.

Uninstall Language Pack

You can uninstall the Language Pack from Windows **Control Panel > Programs and Features > Uninstall or change a program**.

Unified Communications Manager Upgrade Procedures

Upgrade Unified Communications Manager License

Before you begin

Generate the license using this procedure: Generate and Register License, on page 64

Procedure

Step 1 Unzip the license file from the email message.

Step 2 Launch Unified Communications Manager in a browser (`https://<IP Address of CUCM Publisher>`).

Step 3 Click **Cisco Prime License Manager** and navigate to **Licenses** > **Fulfillment**.

Step 4 Under Other Fulfillment Options, select **Fulfill Licenses from File**.

Step 5 Click **Browse** and locate your license file.

Step 6 Click **Install** and close the popup window.

Step 7 Navigate to **Product Instances**. Delete any old instances. Then click **Add**.

Step 8 Fill in the name, hostname/IP address, username, and password for your Cisco Unified Communications Manager Publisher.

Step 9 Select Product type of Unified CM.

Step 10 Click **OK**.

Step 11 Click **Synchronize Now**.

Install Cisco JTAPI Client on PG

After setting up the Cisco Unified Communications Manager (CUCM) PG, you must install the Cisco JTAPI client. PG uses Cisco JTAPI to communicate with CUCM. Install the Cisco JTAPI client from CUCM Administration.

Note Continue with the steps provided in this section if you are installing the JTAPI client for CUCM version earlier than Release 12.5.

To install the JTAPI client for CUCM, Release 12.5 and above, see Install Cisco JTAPI Client on PG, on page 186.

Before you begin

Before you install the JTAPI client, ensure that the previous version is uninstalled.

Procedure

Step 1 Open a browser window on the PG machine.

Step 2 Enter the URL for the Unified Communications Manager Administration utility: http://<*Unified Communications Manager machine name*>/ccmadmin.

Step 3 Enter the username and password that you created while installing and configuring the Unified Communications Manager.

Step 4 Choose **Application** > **Plugins**. Click **Find**.

Step 5 Click the link next to **Download Cisco JTAPI for Windows**.We recommend you to download the 64 bit version. However, if you have already downloaded the 32 bit version, you can proceed to step 7.

Download the JTAPI plugin file.

Step 6 Choose **Save** and save the plugin file to a location of your choice.

Step 7 Open the installer.

Step 8 In the Security Warning box, click **Yes** to install.

Step 9 Choose **Next** or **Continue** through the remaining Setup screens. Accept the default installation path.

Step 10 When prompted for the TFTP Server IP address, enter the CUCM IP address.

Step 11 Click **Finish**.

Step 12 Reboot the machine.

Install Cisco JTAPI Client on PG

Complete the following procedure only if you are installing JTAPI client to connect to Cisco Unified Communications Manager, Release 12.5 and above.

Before you begin

Before you install the JTAPI client, ensure that the previous version is uninstalled.

Procedure

Step 1 Open a browser window on the PG machine.

Step 2 Enter the URL for the Unified Communications Manager Administration utility: http://<*Unified Communications Manager machine name*>/ccmadmin.

Step 3 Enter the username and password that you created while installing and configuring the Unified Communications Manager.

Step 4 Choose **Application** > **Plugins**. Click **Find**.

Step 5 Click the link next to **Download Cisco JTAPI Client for Windows** 64 bit or **Download Cisco JTAPI Client for Windows** 32 bit.

Step 6 Choose **Save** and save the plugin file to a location of your choice.

Step 7 Unzip the JTAPI plugin zip file to the default location or a location of your choice.

There are two folders in the unzipped folder `CiscoJTAPIx64` and `CiscoJTAPIx32`.

Step 8 Run the `install64.bat` file in the `CiscoJTAPIx64` folder or run the `install32.bat` file in the `CiscoJTAPIx32` folder.

The default install path for JTAPI client is `C:\Program Files\JTAPITools`.

Step 9 To accept the default installation path, click Enter and proceed.

Follow the instructions. Click Enter whenever necessary as per the instructions.

Provide IP address of the TFTP server, when prompted for. For 4000 and 12000 deployments, IP address should be same as CUCM IP address provided in CUCM PIM.

The JTAPI client installation completes at the default location. The following message is displayed:

```
Installation Complete.
```

Step 10 Reboot the machine.

What to do next

Note The default location, where the JTAPI client is installed, also contains the `uninstall64.bat` and `uninstall32.bat` file. Use this file to uninstall this version of the client, if necessary.

Upgrade JTAPI on the PG

If you upgrade Unified Communications Manager, you must also upgrade the JTAPI client that resides on the Side A and Side B PGs.

You must install the new JTAPI client using the Unified Communications Manager Administration application. For more information, see the *Install Cisco JTAPI Client on Unified Communications Manager PG* section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* available here

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Procedure

Step 1 Uninstall the old JTAPI client from each Call Server:
a) Go to **Control Panel** > **Programs and Features**.
b) Uninstall the Cisco Unified Communications Manager JTAPI Client , following all prompts.

Step 2 To launch the Unified Communications Manager Administration application, enter the following URL in a Web browser on each Unified CCE Call Server: `https://<IP address of Unified Communications Manager Publisher>/ccmadmin`.

Step 3 Enter the username and password that you created when you installed and configured Unified Communications Manager.

Step 4 Select **Application** > **Plug-ins**.

Step 5 Click **Find** to see the list of applications.

Step 6 Click the download link next to **Cisco JTAPI 32-bit Client for Windows**.

Step 7 Choose **Run this program from its current location**. Click **OK**.

Step 8 If a Security Warning box appears, click **Yes** to install.

Step 9 When asked for the Cisco TFTP Server IP Address, enter the IP address of the Unified Communications Manager Publisher. Click **Next**.

Step 10 Choose **Next** or **Continue** through the remaining setup windows. Accept the default installation path.

Step 11 Click **Finish**.

Update VMware Settings for Cisco Unified Communications Manager

Update the virtual machine settings when you upgrade Unified CM from 11.5(1) to 12.0.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Change the Guest operation system version from “Red Hat Enterprise Linux 6 (64-bit)” to “CentOS 4/5/6/7 (64-bit)”.

Step 4 Click **OK** to save your changes.

Step 5 Power on the virtual machine.

Cut Over from Side B to Side A

Perform the following tasks during a maintenance window, in the order that they are listed.

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

Step	Task
Configure the Cisco Voice Gateway dial-peer priority	
1.	Reverse the Cisco IOS Enterprise Ingress Voice Gateway dial-peer priority configuration so that calls are sent to the Side A Unified CVP server first and then to Side B.
2.	Change the Unified CVP scripts as required so they do not point to DNs and labels on Unified CVP Server 2B.
Bring down Side B	
3.	On each of the following VMs, select **Unified CCE Service Control** on the desktop. Stop the Unified CCE services and change **Startup** to **Manual**: • Side B Unified CCE Call Server • Side B Unified CCE Data Server • External HDS with Side B as the Central Controller preferred side (if used)
4.	Power off the Finesse Secondary node VM in the vSphere client.
5.	Power off the Unified Intelligence Center Subscriber VM in the vSphere client.
6.	Transfer the Unified CVP scripts and media files to the gateways that are not currently in use on Side A. See Transfer Unified CVP Scripts and Media Files, on page 80.
7.	Shut down the following Unified CVP VMs from their Windows OS in the following order: **1.** Unified CVP Server 1B **2.** Unified CVP Server 2B **3.** Unified CVP Reporting Server **Important** At this point, Courtesy Callback no longer works. Unified CVP Reporting does not work unless you have an external Unified CVP Reporting Server.
8.	Power off the Unified Communications Manager Subscriber 2 VM in the vSphere client.
Bring up Side A	

Step	Task
9.	On each of the following VMs, select **Unified CCE Service Control** on the desktop. Start the Unified CCE services and change **Startup** to **Automatic**: • Side A Unified CCE Rogger • Side A Unified CCE AW-HDS-DDS (former Data Server) • Side A PG (former Call Server) • External HDS with Side A as the Central Controller (if used) Verify that services are started.
10.	If you changed the Unified Communications Manager device pool settings as part of the preupgrade, restore the original settings.
11.	Direct agents to sign in to the Side A Finesse Primary node.
12.	Change Unified Intelligence Center historical and real-time data sources to point to the Side A Unified CCE AW-HDS-DDS. See Configure Unified Intelligence Center Data Sources for External AW-HDS-DDSHDS, on page 105 for steps on how to configure Unified Intelligence Center data sources. Use the IP address of the Unified CCE AW-HDS-DDS.

Upgrade Side B

Migrate and Upgrade Side B

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

For best results, place the upgrade media ISOs on local data stores. Make sure to remove them when the upgrade is complete.

Step	Task
Start the Side B Unified CVP components	
1.	Start Unified CVP Server 1B and then start the Unified CVP Reporting Server. **Note** You do not need to start Unified CVP Server 2B as it is removed during the migration.
Upgrade the Side B Unified CVP Servers	

Step	Task
2.	Update the settings on the Unified CVP Server 1B VM. See Update VMware Settings for the Unified CVP Server , on page 166.
3.	Upgrade Unified CVP Server 1B. See Upgrade the Unified CVP Server, on page 167.
4.	Remove the Unified CVP Server 2B VM. **Note** Delete the Call Server, Media Server, and VXML Server from the Unified CVP OAMP Server before removing the Unified CVP Server 2B VM.
5.	Update the Cisco IOS Enterprise Ingress Voice Gateway dial-peer configuration to remove Unified CVP Server 2B.
6.	Obtain and transfer the license now if you don't have an on-box Unified CVP Reporting Server. If you have an on-box Unified CVP Reporting Server, you can transfer the upgrade license to all Unified CVP components after you upgrade the Unified CVP Reporting Server. See Obtain and Transfer the Upgrade License for Unified CVP, on page 169. **Note** You must manually configure the Unified CVP properties files based on the upgrade path. For more information, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.
Upgrade the on-box Unified CVP Reporting Server (if used)	
7.	Complete the Unified CVP Reporting Server preupgrade tasks. See Unified CVP Reporting Server Preupgrade Tasks, on page 171.
8.	Unload the data from the Unified CVP Reporting Server. See Unload Data From Reporting Database, on page 171.
9.	Uninstall the Unified CVP Reporting Server. See Uninstall the Unified CVP Component from the Reporting Server VM, on page 172.
10.	Update the settings on the Unified CVP Reporting Server VM. See Update VMware Settings for the Unified CVP Reporting Server, on page 172.
11.	Install the Unified CVP Reporting Server. See Install Cisco Unified CVP Reporting Server, on page 56.
12	Load data on the Unified CVP Reporting Server. See Load Data to Reporting Server Database, on page 173.

Step	Task
13.	Save and deploy the Unified CVP Reporting Server in the Operations Console. See Save and Deploy the Unified CVP Reporting Server, on page 174.
14.	Transfer the upgrade license. See Obtain and Transfer the Upgrade License for Unified CVP, on page 169.
Upgrade Side B Cisco Voice Gateway IOS Version if needed	
15.	Upgrade the Side B Cisco Voice Gateway IOS version to the minimum required by the upgraded Packaged CCE release (or later). See Upgrade Cisco Voice Gateway IOS Version, on page 170. See the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for IOS support information.
Upgrade the Side B Finesse and Unified Intelligence Center VMs	
16.	Power on the Finesse Secondary node VM in the vSphere client.
17.	Upgrade the VMware version on the Finesse Secondary VM. See Upgrade the Virtual Machine Hardware Version, on page 174.
18.	Update the settings on the Finesse Secondary VM. See Update VMware Settings for Cisco Finesse, on page 174.
19.	Upgrade the Finesse Secondary node. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176.
20.	Power on the Unified Intelligence Center Subscriber VM in the vSphere client.
21.	Upgrade the VMware version on the Unified Intelligence Center Subscriber VM. See Upgrade the Virtual Machine Hardware Version, on page 174.
22.	Update the settings on the Unified Intelligence Center Subscriber VM. See Update VMware Settings for Cisco Unified Intelligence Center, on page 175.

Step	Task
23.	Upgrade the Unified Intelligence Center Subscriber. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176. **Note** Your configuration information migrates automatically to the upgraded version in the active partition.
Prepare for Side B Migration to Packaged CCE 2000 Agent Rogger Deployment	
24.	Back up and export the Side B SQL database. See Back Up Database, on page 177.
Install the Side B Unified CCE Rogger	
25.	Create a VM for the Side B Unified CCE Rogger. Using Packaged-CCE-UCCE.ova, Create a Virtual Machine from the OVA, on page 38. Select **CCE Rogger** from the drop-down list.
26.	Install Microsoft Windows Server on the Side B Unified CCE Rogger VM. See Install Microsoft Windows Server, on page 45.
27.	Install VMware tools on the Side B Unified CCE Rogger VM. See Install VMware Tools, on page 47.
28.	Configure the network adaptors for the Side B Unified CCE Rogger. See Configure Network Adapters for Unified CCE Rogger and Unified CCE PG, on page 47 .
29.	Install antivirus software on the Side B Unified CCE Rogger. See Install Antivirus Software, on page 43.
30.	Configure the database drive for the Side B Unified CCE Rogger. See Configure Database Drive, on page 41.
31.	Set persistent static routes. See Set Persistent Static Routes, on page 49.
32.	Run Windows updates. See Run Windows Updates, on page 50.
33.	Add the Unified CCE Rogger to the domain.
34.	Install Microsoft SQL Server. Install Microsoft SQL Server, on page 50.

Step	Task
35.	Install Cisco Unified Contact Center Enterprise. See Install Cisco Unified Contact Center Enterprise, on page 54.
Configure the Side B Unified CCE Rogger	
36.	Add a UCCE Instance in Web Setup. See Add a UCCE Instance, on page 177.
37.	Configure SQL Server for the Logger database. See Configure SQL Server for CCE Components, on page 69.
38.	Configure the Logger database and log. See Configure the Logger Database and Log, on page 178.
39.	Import the Side B SQL database that you previously backed up in step 24. **Note** Do not import the Outbound database to Side B.
40.	Add a Unified CCE Router component in Web Setup. See Add a Unified CCE Router Component, on page 179.
41.	Add a Unified CCE Logger component in Web Setup. See Add a Unified CCE Logger Component, on page 180.
Convert the Side B Unified CCE Data Server and Unified CCE Call Server	
42.	Upgrade the VMware version on the Side B Data Server VM. See Upgrade the Virtual Machine Hardware Version, on page 174.
43.	Update the settings on the Side B Data Server VM. See Update VMware Settings on the Unified CCE Data Server, on page 181.
44.	Convert the Side B Unified CCE Data Server to a Unified CCE AW-HDS-DDS. See Convert Unified CCE Data Server to Unified CCE AW-HDS-DDS, on page 182.
45.	Update the real-time and historical datasources for Unified Intelligence Center to point to the Unified CCE AW-HDS-DDS. You must update the historical data source database name to <*instancename*>_awdb.
46.	Upgrade the VMware version on the Side B Call Server VM. See Upgrade the Virtual Machine Hardware Version, on page 174.
47.	Update the settings on the Side B Call Server VM. See Update VMware Settings on the Unified CCE Call Server, on page 183.

Step	Task
48.	Remove the Router from the Side B Unified CCE Call Server. See Remove the Router from the Unified CCE Call Server, on page 184. **Note** If CTI OS Server is present, remove it as well. CTI OS is no longer supported. The Call Server is now a PG.
49.	Run the Unified CCE 11.6(1) installer on the Side B Unified CCE Rogger to upgrade to Release 11.6(1). See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
50.	Disable configuration changes on the Side B Unified CCE Rogger. Change the following registry key to 1: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterB\Router\CurrentVersion\Configuration\Global\DBMaintenance`
51.	Run the Unified CCE 11.6(1) installer on the Side B Unified CCE AW-HDS-DDS (former Data Server) to upgrade to Release 11.6(1). See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
52.	Run the Unified CCE 11.6(1) installer on the Side B PG (former Call Server) to upgrade to Release 11.6(1). See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
53.	Modify the Side B PG to point to the Unified CCE Rogger. See Modify the PG, on page 184.
54.	Modify the dialer to point to the Unified CCE Rogger (if using Outbound Option). See Modify the Dialer, on page 184.
Optional: Upgrade the External HDS associated with Side B (if used)	
55.	Upgrade the VMware version on the External HDS associated with Side B. See Upgrade the Virtual Machine Hardware Version, on page 174.
56.	Run the Unified CCE 11.6(1) installer on the External HDS associated with Side B to upgrade to Release 11.6(1). See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
57.	Update the Central Controller connectivity to point to the Unified CCE Rogger. See Update the Central Controller Connectivity, on page 184.
Optional: Install language pack	
58.	Install the language pack on the Side B Unified CCE Rogger, AW-HDS-DDS, PG (formerly Call Server), and External HDS (if used). See Install the Language Pack, on page 185.

Step	Task
Upgrade Side B Unified Communications Manager Subscriber 2	
59.	Power on the Unified Communications Manager Subscriber 2 VM in the vSphere client.
60.	Upgrade the Side B Unified Communications Manager Subscriber 2. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176.
61.	Upgrade JTAPI on the Side B PG (formerly Call Server). See Upgrade JTAPI on the PG, on page 187. **Important** If you are installing CUCM 12.5, install Cisco JTAPI Client on CUCM. See Install Cisco JTAPI Client on PG, on page 186.
Optional: Change hostnames of the Unified CCE components	
62.	Optional: Change the hostnames of the Unified CCE components (AW-HDS-DDS and PG). **Note** You can perform this task when you reboot each component as part of the upgrade. If you do change the hostnames, you must also change them in the following places: • Finesse • PG Setup • Unified Intelligence Center - Historical and real-time • Private network DNS entries • Live Data—If you change the hostname of the AW-HDS-DDS (former Data Server), Live Data no longer connects to the AW-HDS-DDS after the Data Server hostname is removed from DNS. To fix this, do the following: 1. Run the following CLI command on the CUIC-LD-IdS Publisher: **unset live-data aw-access secondary** 2. Restart Cisco Tomcat on the Side B AW-HDS-DDS.

Sync Side A to Side B

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

Step	Task
1	Set the following registry key to 0 on either the Side B Unified CCE Rogger: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router B\Router\CurrentVersion\Configuration\Global\DBMaintenance`
2	On each of the following VMs, select **Unified CCE Service Control** on the desktop. Start the Unified CCE services and change Startup to Automatic, in this order: **1.** Side B Unified CCE Rogger **2.** Side B Unified CCE AW-HDS-DDS **3.** Side B PG **4.** External HDS with Side B as the Central Controller preferred side (if used) Verify that the services are started.

Migrate Call Server to Unified CCE PG

Perform these tasks in a maintenance window. Perform these tasks on the Side A PG (former Call Server) and then on the Side B PG and in the order they are listed.

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

Note You can continue the maintenance window that you used to sync Side A and Side B or you perform them in a later maintenance window.

Step	Task
For the Side A PG (formerly Call Server):	
1.	Add a new CUCM PG. See Add a New CUCM PG, on page 198.
2.	Remove the Dialed Number configuration. See Remove Dialed Number Configuration, on page 199.
3.	Remove the Agent Targeting Rule configuration. See Remove Agent Targeting Rule Configuration, on page 199.

Step	Task
4.	Remove the Network Trunk configuration. See Remove Network Trunk Configuration, on page 200.
5.	Remove the Label configuration. See Remove Label Configuration, on page 200.
6.	Remove the Unified CVP PIMs from PG Explorer. See Remove Unified CVP PIMs, on page 200.
7.	Install CUCM PG3. See Install the CUCM PG, on page 201.
8.	Install CG3. See Install CG3, on page 202.
9.	Modify PG1 to VRU PG. See Modify PG1 to VRU PG , on page 203.
10.	Uninstall CG1. See Uninstall CG1, on page 203.
11.	In Finesse Administration, configure the CTI port information in CTI Server Settings for Side A. Restart the Cisco Tomcat service and the Cisco Finesse Tomcat service.
For the Side B PG (formerly Call Server):	
12.	Repeat Step 7 through Step 10 for the Side B PG.
13.	In Finesse Administration, configure the CTI port information in CTI Server Settings for Side B. Restart the Cisco Tomcat service and the Cisco Finesse Tomcat Service.
Redo Dialed Number, Agent Targeting Rule, and Network Trunk Group configuration as required	

Add a New CUCM PG

Procedure

Step 1 In the **Configuration Manager** window, expand **Tools** > **Explorer Tools**.

Step 2 Open **PG Explorer**.

Step 3 Click **Add PG** and then enter the following values in the **Logical Controller** pane:

- In the **Name** field, enter **`CUCM_PG`**.
- For **Client type**, choose **CUCM**.
- Enter **Primary CTI Address** and **Secondary CTI Address** as mentioned in the generic PG.

Step 4 Delete the peripheral that was automatically created in the previous step.

Step 5 Click **Save**.

Step 6 Drag the CUCM peripheral from the Generic PG to the CUCM PG.

A message appears asking if you are sure you want to move the peripheral to a different PG. Click **Yes** to confirm.

Step 7 Rename the Generic PG to VRU PG and change the Client type to **VRU**.

Step 8 Click **Save**.

Note Make sure to record the Logical Controller ID of the new CUCM PG. You need to enter it when you install the PG.

Remove Dialed Number Configuration

Before you begin

Dialed numbers that are mentioned in any scripts must be removed from the scripts before you perform this procedure. Make sure that they are removed from all versions (not just the active scripts).

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 In Configuration Manager, expand **Tools** > **List Tools**.

Step 3 Open **Dialed Number / Script Selector List**.

Step 4 Select **Routing Client** as the existing VRU for Unified CVP 2A / Unified CVP 2B and then click **Retrieve**.

Step 5 Select each dialed number associated to the routing client and then click **Delete**.

Step 6 Click **Save**.

Remove Agent Targeting Rule Configuration

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 Expand **List Tools**.

Step 3 Select **Agent Targeting Rule**.

Step 4 Remove the Routing Client for Unified CVP 2A and Unified CVP 2B.

Step 5 Click **Save**.

Remove Network Trunk Configuration

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.
Step 2 Expand **Explorer Tools**.
Step 3 Select **Network Trunk Group Explorer**.
Step 4 From the **PG** list, select **VRU_PG** and then click **Retrieve**.
Step 5 Expand **GENERIC** and click any trunk group that appears beneath it.
Step 6 Click **Multiple**.
Step 7 In the **Delete Multiple** dialog box, select all of the CVP 2A and CVP 2B trunk groups and then click **Delete**.
Step 8 Click **OK**.
Step 9 Click **Save**.

Remove Label Configuration

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.
Step 2 Expand **List Tools**.
Step 3 Select **Label List**.
Step 4 Remove the labels associated with Unified CVP 2A and Unified CVP 2B.

Remove Unified CVP PIMs

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.
Step 2 Expand **Tools** > **Explorer Tools**.
Step 3 Open **PG Explorer**.
Step 4 Select **VRU PG**.

Step 5 Delete the PIMs for Unified CVP 2A and Unified CVP 2B.

Step 6 Click **Save**.

Install the CUCM PG

Procedure

Step 1

Step 2 On the PG (former Call Server), choose **Start** > **All Programs** > **Unified CCE Tools** > **Peripheral Gateway Setup**.

Step 3 In the **Instance Component** section, click **Add**.

Step 4 Click **Peripheral Gateway**.

Step 5 In the **Peripheral Gateways Properties** dialog, do the following:

a) Check the **Production Mode** check box.
b) Check the **Auto start at system start up** check box.
c) Check the **Duplexed Peripheral Gateway** check box.
d) From the **PG Node Properties ID** drop-down list, select **PG3**.
e) Select the appropriate side (Side A or Side B).
f) In the **Client Type Selection** section, add **CUCM** to the Selected Types.
g) Click **Next**.

Step 6 In the **Peripheral Gateway Managers** section of the **Peripheral Gateway Component Properties** dialog box, click **Add**.

Step 7 Select **CUCM** and **PIM1** and click **OK**.

Step 8 Check the **Enabled** check box.

Step 9 In the **Peripheral Name** field, enter CM.

Step 10 In the **Peripheral ID** field, enter the Peripheral ID that the system generated in Step 8 after the CUCM PG was added.

Step 11 In the **Agent Extension Length** field, enter the extension length for this deployment.

Step 12 In the **CUCM Parameters** section, do the following:

a) In the **Service** field, enter the hostname of the Unified Communications Manager Subscriber.
b) In the **User ID** field, enter pguser.
c) In the **User Password** field, enter the password of the user that will be created on Unified Communications Manager.
d) In the **Mobile Agent Codec** field, choose either **G711 ULAW/ALAW** or **G.729**.

Step 13 Click **OK**.

Step 14 In the **Logical controller ID** field, enter the Logical controller ID of the CUCM PG that you created previously in PG Explorer.

Step 15 In the **CTI Call Wrapup Data delay** field, enter 0. Click **Next**.

Step 16 In the **Device Management Protocols Properties** dialog box, do the following:

a) For Side A PG:

- Select **Side A preferred**.
- For Side A properties, select **CallRouter is local**.
- For Side B properties, select **CallRouter is remote (WAN)**.

b) For Side B PG:

- Select **Side B preferred**.
- For Side A properties, select **CallRouter is remote (WAN)**.
- For Side B properties, select **CallRouter is local**.

c) For both sides:

- Accept the default in the Usable Bandwidth (kbps) field.
- Accept the default in the Heartbeat Interval (100ms) field.

d) Click **Next**.

Step 17 In the **Peripheral Gateway Network Interfaces** dialog box, complete the interface fields:

a) Enter the Private and Visible network interface hostnames. For the PG, use the same hostnames for private and private high. For the Router, enter the hostname of the Unified CCE Rogger Side A for the Router visible A and Router visible A high interfaces. Enter the hostname of the Unified CCE Rogger Side B for the Router visible B and Router visible B high interfaces.
b) For the Side A PG, in the **Private Interfaces** section, click **QoS**. Check **Enable QoS** and click **OK**.
c) For both the Side A and Side B PGs, in the **Visible Interfaces** section, click **QoS**. Check **Enable QoS** and click **OK**.
d) Click **Next**.

Step 18 In the **Check Setup Information** dialog box, click **Next**.

Step 19 In the **Setup Complete** dialog box, click **Finish**.

Install CG3

Procedure

Step 1 Launch **Peripheral Gateway Setup**.

Step 2 In the **Instance Components** section, click **Add**.

Step 3 In the Component Selection dialog box, click **CTI Server**.

a) Check **Production mode**.
b) Check **Auto start at system startup**.
c) Check **Duplexed CTI Server**.
d) From the CG node properties pane ID list, choose **CG3**.
e) Enter 3 in the CG node properties ICM system ID field.
f) Click the appropriate side.

g) Click **Next**.

Step 4 In the CTI Server Component Properties dialog box, do the following:

a) For Side A, enter 42027 in the Client Connection Port Number field.

b) For Side B, enter 43027 in the Client Connection Port Number field.

Step 5 Click **Next**.

Step 6 In the CTI Server Network Interface Properties dialog box, fill in all interface fields and then click **Next**.

Step 7 Check your setup information and then click **Next**.

Step 8 Click **Finish**.

Modify PG1 to VRU PG

Procedure

Step 1 Open Peripheral Gateway Setup.

Step 2 Select **PG1**.

Step 3 Click **Edit**.

Step 4 In the **Client Type Selection** section, remove **CUCM**.

Step 5 Click **Next**.

Step 6 In the **Peripheral Gateway Component Properties** dialog box, remove the CUCM PIMs that were used for connecting to CUCM and click **Next**.

Step 7 In the **Device Management Protocol Properties** dialog box, click **Next**.

Step 8 In the **Peripheral Gateway Network Interfaces** dialog box, enter the hostname or IP address of the Unified CCE Rogger Side A for the Router visible A and Router visible A high interfaces. Enter the hostname or IP address of the Unified CCE Rogger Side B for the Router visible B and Router visible B high interfaces.

Step 9 Click **Next**.

Step 10 In the **Check Setup Information** dialog box, click **Next**.

Step 11 Check the **Yes, start the Unified ICM/CC Node Manager** check box and click **Finish**.

Uninstall CG1

Procedure

Step 1 Open Peripheral Gateway Setup.

Step 2 Select **CG1**.

Step 3 Click **Delete**.

Step 4 Click **OK**.

Switch into Packaged CCE Deployment

Switch into Packaged CCE Deployment

Step	Task
1.	In **Unified CCE Administration** > **Deployment**, switch into the Packaged CCE: 2000 Agents deployment type.
2.	Validate the Packaged CCE deployment in Unified CCE Administration. See Validate Packaged CCE Deployment and Build System Inventory, on page 204.
3.	Direct agents to sign in to the correct Finesse node.

Validate Packaged CCE Deployment and Build System Inventory

Validate the PCCE deployment using the Unified CCE Administration Deployment tool.

As you complete the procedure, you are prompted only for missing information; you may not need to perform each step.

Postupgrade Tasks

You can perform these postupgrade tasks in any order.

Component	Task
Finesse	Complete postupgrade tasks for the Finesse desktop layout. See Finesse Desktop Layout Postupgrade Tasks, on page 204. Finesse server need a restart after the upgrade of peripheral gateways (PG).
Unified CVP	Upgrade Call Studio. Upgrade Unified Call Studio, on page 205
	Optional: Synchronize the metadata files for the Unified CVP REST API using the sync-up tool. See Initiate Metadata Synchronization for Unified CVP Rest API, on page 206.
All	Optional: Upgrade ESXi. See Upgrade VMware vSphere ESXi, on page 207.

Finesse Desktop Layout Postupgrade Tasks

If you do not use a custom desktop layout, do the following after upgrading Cisco Finesse:

1. Click **Restore Default Layout** on the Manage Desktop Layout gadget to add all updates from the new default desktop layout.
2. Disable the Agent Queue Statistics gadget from the default desktop layout for the Agent role. This gadget is not supported for the Agent role in Packaged CCE deployments.
3. **Optional:** Enable Live Data Report gadgets for the Agent role.

If you use a custom desktop layout, do the following after upgrading Finesse:

1. Add optional Live Data Report gadgets for the Agent role after upgrading Cisco Finesse.
2. If you want to restore a previous layout for the desktop, sign in to the Administration Console on the primary Finesse node. Copy and paste your saved layout XML into the Manage Desktop Layout gadget.

Related Topics

Disable Agent Queue Statistics Gadget in Default Desktop Layout
Add Live Data Reports to Default Desktop Layout, on page 113
Add Live Data Reports to Custom Desktop Layout, on page 114

Upgrade Unified Call Studio

Before you begin

Obtain a new license for Unified Call Studio because licenses for earlier versions are invalid with the latest version.

Note Upgrade of Call Studio is supported through the migration process.

Procedure

Step 1 Open Call Studio, right-click any existing project in the Navigator view, choose **Export**.

The **Export** wizard opens.

Step 2 Navigate to **General** > **File System**, and click **Next**.

Note From the list displayed by the Export wizard, select multiple projects to export them simultaneously.

Step 3 Browse to the directory where the projects will be exported and click **OK** and then click **Finish**.

Step 4 Uninstall the Call Studio software.

For more information, see the Uninstall the Unified CVP Component.

Step 5 Install the Call Studio software.

For more information, see the Install Unified Call Studio section.

Related Topics

Unified Customer Voice Portal Licenses, on page 80

Install Unified Call Studio

Procedure

Step 1 Mount the Unified CVP software (including CVP Studio) installer ISO image, and run setup.exe.

Step 2 On the **Welcome** screen, click **Next**.

Note If you click **Cancel** here or on the dialog screens that follow before the **Ready to Install the Program** screen, the installation is canceled. The **Exit Setup** dialog box appears.

Step 3 Review **Copyrights to Products** used by Call Studio and click **Next**.

Step 4 Review and accept the license agreement, and click **Next**.

Step 5 On the Choose Destination Location screen, select the folder where setup will install files. By default, it is `C:\Cisco\CallStudio`.

Step 6 On the **InstallShield Wizard Complete** screen, click **Install**.

Step 7 Click **Finish** to exit the wizard.

The Call Studio software is installed on your computer.

Related Topics

Mount and Unmount ISO Files, on page 37

Initiate Metadata Synchronization for Unified CVP Rest API

In the CVP REST API architecture, information of media files on Media Server and VXML applications on a VXML server is saved on a WSM Server as metadata in Derby database. This metadata information is created, updated, and deleted by the REST API calls. There may be situations where the metadata may go out of sync with files on VXML Servers and Media Servers. Examples are addition and deletion of CVP Servers, deployment of apps and media files by a tool other than the REST API, and CVP Media Server or the VXML server upgraded from a version where the REST API was not supported.

A command line tool “metasynch.cmd” is available at `C:\Cisco\CVP\wsm\CLI` to enable synchronization of metadata with the files on VXML Servers and Media Servers. The tool internally uses the Synch up API to perform the synchronization. It takes three arguments- WSM user name, WSM user password, and server type (MEDIA, VXML or VXML_ STANDALONE). Based on the server type information, all servers of the respective server type are synchronized. If the server type argument is not provided, metadata is synchronized with all media servers and VXML servers configured in OAMP.

In case of an upgrade, the media files and VXML applications are present in the Media Servers and VXML Servers but corresponding metadata information is not present in the WSM Server. The absence of metadata information limits a user from using the REST API to access, update, and delete existing media files and VXML applications on the Media Server and the VXML Server.

Synchronize Metadata Files Using Sync-Up Tool

To invoke **metasynch.cmd**, complete the following steps.

Procedure

Step 1 On the Unified CVP OAMP Server, navigate to the `C:\Cisco\CVP\wsm\CLI` location.

Step 2 Run the **metasynch.cmd** file with following arguments:

- **wsm username**
- **wsm password**

Example:

```
metasynch.cmd wsmusername wsmpassword MEDIA
```

Usage : metasynch [options] username password [servertype]

servertype : MEDIA/VXML

options : -help -? print this help message

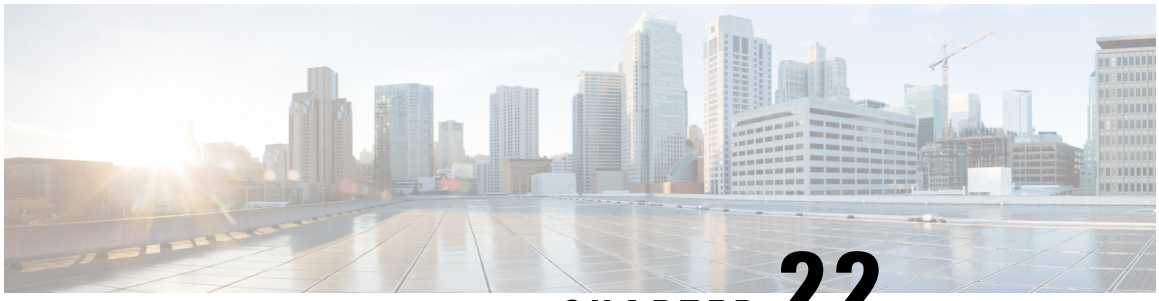
Note The server type argument should be MEDIA, VXML type. If the server type argument is not provided, the metadata is synched with all the VXML applications on VXML servers and all media files on Media servers. Logs for synch command tool can be found at the following location:

`C:\Cisco\CVP\wsm\CLI\log\SyncTool.log`

Upgrade VMware vSphere ESXi

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

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



CHAPTER 22

Packaged CCE 11.5 to 11.6 Upgrade

Packaged CCE 11.5 to 11.6 Upgrade

Migrate and Upgrade Side A

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

- In Unified CVP Diagnostic Portal, check that no Side A ports are in use.
- In the Unified Communications Manager RTMT tool, check that phones have migrated to Side B.

For best results, place upgrade media ISOs on local data stores. Make sure to remove them when the upgrade is complete.

Step	Task
Upgrade the Side A Unified CVP VMs	
1.	Upgrade the Unified CVP OAMP Server. See Upgrade the Unified CVP Operations Console, on page 169.
2.	Upgrade Unified CVP Server 1A. See Upgrade the Unified CVP Server, on page 167.
3.	Obtain and transfer the license now if you don't have an external Unified CVP Reporting Server. For an external Unified CVP Reporting Server, you can transfer the upgrade license to all Unified CVP components after you upgrade the external server. See Obtain and Transfer the Upgrade License for Unified CVP, on page 169.
4.	Transfer scripts and media files to the gateways not currently being used by Side B. If all gateways are being used, perform this step during the cutover to Side B. See Transfer Unified CVP Scripts and Media Files, on page 80.
Upgrade Side A Cisco Voice Gateway IOS Version if needed	

Step	Task
5.	Upgrade the Side A Cisco Voice Gateway IOS version to the minimum required by the upgraded Packaged CCE release (or later). See Upgrade Cisco Voice Gateway IOS Version, on page 170. See the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for IOS support information.
Upgrade External Unified CVP Reporting Server (if used)	
6.	Complete the Unified CVP Reporting Server preupgrade tasks. See Unified CVP Reporting Server Preupgrade Tasks, on page 171.
7.	Unload the data from the Unified CVP Reporting Server. See Unload Data From Reporting Database, on page 171.
8.	Uninstall the Unified CVP Reporting Server. See Uninstall the Unified CVP Component from the Reporting Server VM, on page 172.
9.	Install the External Unified CVP Reporting Server. See Install Cisco Unified CVP Reporting Server, on page 56.
10.	Load data on the Unified CVP Reporting Server. See Load Data to Reporting Server Database, on page 173.
11.	Save and deploy the Unified CVP Reporting Server in the Operations Console. See Save and Deploy the Unified CVP Reporting Server, on page 174.
12.	Transfer the upgrade license. See Obtain and Transfer the Upgrade License for Unified CVP, on page 169.
Upgrade the Side A Finesse and Unified Intelligence Center VMs	
13.	Upgrade the Finesse Primary node. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176.

Step	Task
14.	Upgrade the Unified Intelligence Center Publisher node. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176. **Note** Your configuration information migrates automatically to the upgraded version in the active partition.
Prepare for Side A Migration to Packaged CCE 2000 Agent Rogger Deployment	
15.	Back up and export the Logger database and the Outbound Option (if used) pccebaA database. See Back Up Database, on page 177.
16.	Back up and export your network configuration. See Back Up Network Configuration, on page 177.
17.	Run Windows updates. See Run Windows Updates, on page 50.
Convert the Side A Unified CCE Data Server and Unified CCE Call Server	
18.	Run the Unified CCE Release 11.6(1) installer on the Side A Unified CCE Rogger. See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
19.	Disable configuration changes on the Unified CCE Rogger. Change the following registry key to 1: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance`
20.	Run the Unified CCE Release 11.6(1) installer on the Side A Unified CCE AW-HDS-DDS. See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
21.	Run the Unified CCE 11.6(1) installer on the Side A PG. See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
Optional: Upgrade the External HDS associated with Side A (if used)	
22.	Run the Unified CCE Release 11.6(1) installer the External HDS associated with Side A. See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
Optional: Install language pack	
23.	Install the language pack on the Side A Unified CCE Rogger, AW-HDS-DDS (former Data Server), PG (former Call Server), and External HDS associated with Side A (if used). See Install the Language Pack, on page 185.

Step	Task
Upgrade the Side A Unified Communications Manager Publisher and Subscriber 1	
24.	Upgrade the Side A Unified Communications Manager Publisher. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176.
25.	Upgrade the Side A Unified Communications Manager Subscriber 1. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176. **Important** The Unified CM Publisher upgrade must be complete and the new release software must be the active version before you upgrade the Unified CM Subscriber.
26.	Upgrade the Unified Communications Manager License. See Upgrade Unified Communications Manager License, on page 185.
27.	Upgrade JTAPI on the Side A PG. See Upgrade JTAPI on the PG, on page 187. **Important** If you are installing CUCM 12.5, install Cisco JTAPI Client on CUCM. See Install Cisco JTAPI Client on PG, on page 186.

Migrate and Upgrade Side B

For best results, place the upgrade media ISOs on local data stores. Make sure to remove them when the upgrade is complete.

Step	Task
Start the Side B Unified CVP components	
1.	Start Unified CVP Server 1B and then start the Unified CVP Reporting Server. **Note** You do not need to start Unified CVP Server 2B as it is removed during the migration.
Upgrade the Side B Unified CVP Servers	
2.	Upgrade Unified CVP Server 1B. See Upgrade the Unified CVP Server, on page 167.

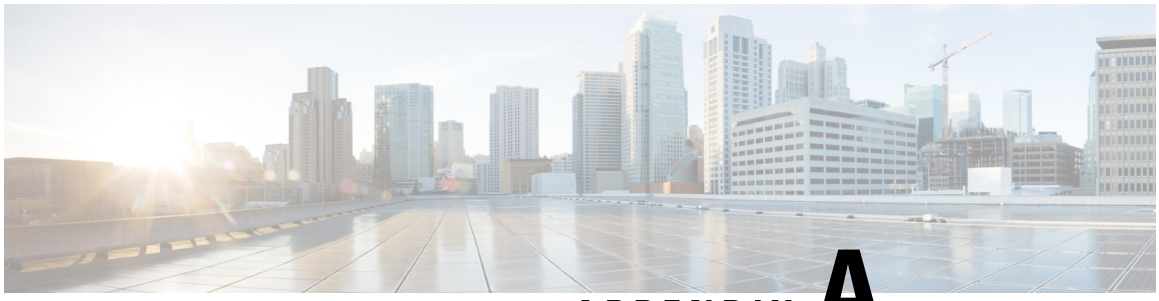
Step	Task
3.	Obtain and transfer the license now if you don't have an on-box Unified CVP Reporting Server. If you have an on-box Unified CVP Reporting Server, you can transfer the upgrade license to all Unified CVP components after you upgrade the Unified CVP Reporting Server. See Obtain and Transfer the Upgrade License for Unified CVP, on page 169.
Upgrade the on-box Unified CVP Reporting Server (if used)	
4.	Complete the Unified CVP Reporting Server preupgrade tasks. See Unified CVP Reporting Server Preupgrade Tasks, on page 171.
5.	Unload the data from the Unified CVP Reporting Server. See Unload Data From Reporting Database, on page 171.
6.	Uninstall the Unified CVP Reporting Server. See Uninstall the Unified CVP Component from the Reporting Server VM, on page 172.
7.	Install the Unified CVP Reporting Server. See Install Cisco Unified CVP Reporting Server, on page 56.
8.	Load data on the Unified CVP Reporting Server. See Load Data to Reporting Server Database, on page 173.
9.	Save and deploy the Unified CVP Reporting Server in the Operations Console. See Save and Deploy the Unified CVP Reporting Server, on page 174.
10.	Transfer the upgrade license. See Obtain and Transfer the Upgrade License for Unified CVP, on page 169.
Upgrade Side B Cisco Voice Gateway IOS Version if needed	
11.	Upgrade the Side B Cisco Voice Gateway IOS version to the minimum required by the upgraded Packaged CCE release (or later). See Upgrade Cisco Voice Gateway IOS Version, on page 170. See the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for IOS support information.
Upgrade the Side B Finesse and Unified Intelligence Center VMs	
12.	Power on the Finesse Secondary node VM in the vSphere client.
13.	Upgrade the Finesse Secondary node. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176.

Step	Task
14.	Power on the Unified Intelligence Center Subscriber VM in the vSphere client.
15.	Upgrade the Unified Intelligence Center Subscriber. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176. **Note** Your configuration information migrates automatically to the upgraded version in the active partition.
Prepare for Side B Migration to Packaged CCE 2000 Agent Rogger Deployment	
16.	Back up and export the Side B SQL database. See Back Up Database, on page 177.
Convert the Side B Unified CCE Data Server and Unified CCE Call Server	
17.	Run the Unified CCE 11.6(1) installer on the Side B Unified CCE Rogger to upgrade to Release 11.6(1). See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
18.	Disable configuration changes on the Side B Unified CCE Rogger. Change the following registry key to 1: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterB\Router\CurrentVersion\Configuration\Global\DBMaintenance`
19.	Run the Unified CCE 11.6(1) installer on the Side B Unified CCE AW-HDS-DDS to upgrade to Release 11.6(1). See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
20.	Run the Unified CCE 11.6(1) installer on the Side B PG to upgrade to Release 11.6(1). See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
Optional: Upgrade the External HDS associated with Side B (if used)	
21.	Run the Unified CCE 11.6(1) installer on the External HDS associated with Side B to upgrade to Release 11.6(1). See Install Cisco Unified Contact Center Enterprise Release 11.6(1), on page 55.
Optional: Install language pack	
22.	Install the language pack on the Side B Unified CCE Rogger, AW-HDS-DDS, PG (formerly Call Server), and External HDS (if used). See Install the Language Pack, on page 185.
Upgrade Side B Unified Communications Manager Subscriber 2	

Step	Task
23.	Power on the Unified Communications Manager Subscriber 2 VM in the vSphere client.
24.	Upgrade the Side B Unified Communications Manager Subscriber 2. See either: • Upgrade VOS-Based Contact Center Applications from DVD/CD, on page 175. • Upgrade VOS-Based Contact Center Applications from a Remote File System, on page 176.
25.	Upgrade JTAPI on the Side B PG. See Upgrade JTAPI on the PG, on page 187. **Important** If you are installing CUCM 12.5, install Cisco JTAPI Client on CUCM. See Install Cisco JTAPI Client on PG, on page 186.

Sync Side A to Side B 11.6

After the migration and upgrade, you must sync side A to side B. See Sync Side A to Side B, on page 196 for more information.



APPENDIX A

Security Considerations

Update the Java Runtime Environment (Optional)

The Unified CCE Installer installs the Java Runtime Environment (JRE) to a default location (for example, C:\Program Files (x86)\Java\jre<version>) and creates a JAVA_HOME environment variable set to that location. In most circumstances, you do not need to modify or configure the JRE.

For more information on the JRE version installed, see the *Cisco Packaged CCE Software Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html.

If required, you can update the JRE to a later version.

To update the JRE to a later version: Cisco Packaged CCE Software Compatibility Matrix

1. Review the *Cisco Packaged CCE Software Compatibility Matrix* to confirm that Packaged CCE supports the JRE version you want to install.
2. Follow the JRE installer procedure to install the JRE to the VM on which your Unified CCE components are installed.
3. Set the JAVA_HOME environment variable to the location of the new JRE.
4. Restart the virtual machine.

When you have completed the update to the new JRE version, uninstall the old JRE.

Note

Upgrade Tomcat Utility

Use the optional Cisco Upgrade Tomcat Utility to:

- Upgrade Tomcat to version 7.0 build releases. (That is, only version 7.0 build releases work with this tool.) You may choose to upgrade to newer builds of Tomcat release 7.0 to keep up with the latest security fixes.

  Tomcat uses the following release numbering scheme: Major.minor.build. For example, you can upgrade from 7.0.62 to 7.0.65 . You cannot use this tool for major or minor version upgrades.

  Revert a Tomcat upgrade.

  We do not guarantee compatibility with the latest build release of Tomcat.

Note If you use the utility to upgrade Tomcat multiple times, you can revert to only one version back of Tomcat. For example, if you upgrade Tomcat from 7.0.62 to 7.0.63, and then to 7.0.75, the utility reverts Tomcat to 7.0.63.

Before using the tool:

- Download the Tomcat installer (apache-tomcat-version.exe) from the Tomcat website: http://archive.apache.org/dist/tomcat/tomcat-7/ . Copy the installer onto the Unified CCE component VMs. For Example C:\UpgradeTomcatTool.
- Download the utility zip file, extract it, and run the file to upgrade Tomcat.

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

  c:\icm\tomcat\logs
  c:\icm\debug.txt

Upgrade Tomcat

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

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

Procedure

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

Step 2 Enter this command to run the tool: **java -jar UpgradeTomcatTool-<version>.jar -upgrade**

For example:

```
java -jar UpgradeTomcatTool-<version>.jar -upgrade
```

Step 3 When prompted, enter the full pathname of the new Tomcat installer.

For example:

```
c:\tomcatInstaller\apache-tomcat-<version>.exe
```

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

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

Revert Tomcat

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

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

Procedure

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

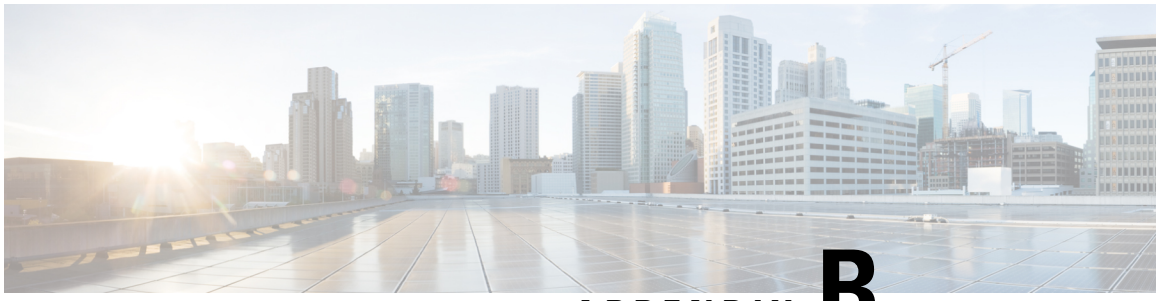
Step 2 Enter this command to run the tool: **java -jar UpgradeTomcatTool-<version>.jar -revert**

For example:

```
java -jar UpgradeTomcatTool-11.6.1.jar -revert
```

Step 3 When prompted, enter **yes** to continue with the reversion.

Step 4 Repeat these steps for all unified CCE component VMs.



APPENDIX B

Reference

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) facilitates the exchange of management information among network devices so that administrators can manage network performance and solve network problems. SNMP community strings, users, and network destinations are configured in Cisco Unified Serviceability.

Unified Serviceability is one of the tools that open from the Navigation drop-down in Cisco Unified Communications Solutions tools. You can also access Unified Serviceability by entering http://x.x.x.x/ccmservice/, where x.x.x.x is the IP address of the publisher.

See the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html for information about configuring SNMP for Unified CCE.

Community Strings

The SNMP agent uses community strings to provide security. You must configure community strings to access any management information base (MIB). Add new community strings in the Cisco Serviceability Administration interface.

A community string is configured with:

- a server
- a name of up to 32 characters
- a setting to accept SNMP packets from any host or from specified hosts
- access privileges (readonly, readwrite, readwritenotify, notifyonly, readnotifyonly, and none)
- a setting to apply the community string to all nodes in the cluster

Notification Destinations

Add notification destinations for delivery of SNMP notification events when events occur. Add and maintain notification destinations in the Cisco Serviceability Administration interface.

A notification destination is configured with:

- a server
- the host IP addresses of the trap destination
- a port number
- the SNMP version (V1 or V2c)
- the community string name to be used in the notification messages that the host generates
- the notification type
- a setting to apply to the notification destination configuration to all nodes in the cluster

Certificates for Live Data

You must set up security certificates for Finesse and Cisco Unified Intelligence Center with HTTPS.

You can:

- Use the self-signed certificates provided with Finesse and Cisco Unified Intelligence Center.
- Obtain and install a Certification Authority (CA) certificate from a third-party vendor.
- Produce a certificate internally.

Note As is the case when using other self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when the sign in before they can use the Live Data gadget.

Add Self-Signed Certificates for Live Data

Both Finesse and Unified Intelligence Center are installed with self-signed certificates. If you choose to work with these self-signed certificates (rather than producing your own CA certificate or obtaining a CA certificate from a third-party certificate vendor), you must first export the certificates from the Unified Intelligence Center Publisher and Subscriber. You must then import the certificates into Finesse, importing the Publisher certificate to the Finesse Primary node and the Subscriber certificate to the Finesse Secondary node.

As is the case when using other self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration on Cisco Unified Intelligence Center (`https://<hostname of Cisco Unified Intelligence Center server>/cmplatform`).

Step 2 From the **Security** menu, select **Certificate Management**.

Step 3 Click **Find**.

Step 4 Do one of the following:

- If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)
- If the tomcat certificate for your server is not on the list, do the following:
  a. Click **Generate New**.
  b. When the certificate generation is complete, restart the Cisco Tomcat service, Unified Intelligence Center Reporting service, and Cisco Live Data NGNIX service.
  c. Restart this procedure.

Step 5 Click **Download .pem file** and save the file to your desktop.

You must download the certificates that contain the hostnames Cisco Unified Intelligence Center publisher and Cisco Unified Intelligence Center subscriber.

Step 6 Sign in to Cisco Unified Operating System Administration on the primary Finesse server (https://*FQDN of Finesse server*:8443/cmplatform).

Step 7 From the **Security** menu, select **Certificate Management**.

Step 8 Click **Upload Certificate**.

Step 9 From the **Certificate Name** drop-down list, select **tomcat-trust**.

Step 10 Click **Browse** and browse to the location of the .pem files (Cisco Unified Intelligence Center publisher and subscriber certificates).

Step 11 Click **Upload File**.

Step 12 Restart Cisco Finesse Tomcat on the Finesse server.

Obtain and Upload CA Certificate for Live Data from a Third Party Vendor

You can use a Certification Authority (CA) certificate provided by a third-party vendor to establish an HTTPS connection between the Finesse and Cisco Unified Intelligence Center servers.

Follow the instructions in the TechNote *Procedure to Obtain and Upload CA Certificate from a Third-party Vendor*, available at https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-enterprise-1101/200286-Unified-CCE-Solution-Procedure-to-Obtai.html.

Produce Certificate Internally

Set up Microsoft Certificate Server for Windows 2008 R2

This procedure assumes that your deployment includes a Windows Server 2008 R2 (Standard) Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows 2008 R2 (Standard) domain controller.

Procedure

Step 1 Click **Start**, right-click **Computer**, and select **Manage**.

Step 2 In the left pane, click **Roles**.

Step 3 In the right pane, click **Add Roles**.

The Add Roles Wizard opens.

Step 4 On the Select Server Roles screen, check the **Active Directory Certificate Services** check box, and then click **Next**.

Step 5 On the Introduction to Active Directory Certificate Services screen, click **Next**.

Step 6 On the Select Role Services screen, check the **Certification Authority** check box, and then click **Next**.

Step 7 On the Specify Setup Type screen, select **Enterprise**, and then click **Next**.

Step 8 On the Specify CA Type screen, select **Root CA**, and then click **Next**.

Step 9 Click **Next** on the Set Up Private Key, Configure Cryptography for CA, Configure CA Name, Set Validity Period, and Configure Certificate Database screens to accept the default values.

Step 10 On the Confirm Installations Selections screen, verify the information, and then click **Install**.

Set up Microsoft Certificate Server for Windows Server

This procedure assumes that your deployment includes a Windows Server Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows Server domain controller.

Before you begin

Before you begin, Microsoft .Net Framework must be installed. See Windows Server documentation for instructions.

Procedure

Step 1 In Windows, open the **Server Manager**.

Step 2 In the **Quick Start** window, click **Add Roles and Features** .

Step 3 In the **Set Installation Type** tab, select **Role-based or feature-based installation** , and then click **Next**.

Step 4 In the **Server Selection** tab, select the destination server then click **Next**.

Step 5 In the **Server Roles** tab, check the **Active Directory Certificate Services** box, and then click the **Add Features** button in the pop-up window.

Step 6 In the **Features** and **AD CS** tabs, click **Next** to accept default values.

Step 7 In the **Role Services** tab, verify that **Certification Authority** box is checked, and then click **Next**.

Step 8 In the **Confirmation** tab, click **Install**.

Step 9 After the installation is complete, click the **Configure Active Directory Certificate Service on the destination server** link.

Step 10 Verify that the credentials are correct (for the domain Administrator user), and then click **Next**.

Step 11 In the **Role Services** tab, check the **Certification Authority** box, and then click **Next**.

Step 12 In the **Setup Type** tab, select **Enterprise CA**, and then click **Next**.

Step 13 In the **CA Type** tab, select **Root CA**, and then click **Next**.

Step 14 In the **Private Key**, **Cryptography**, **CA Name**, **Validity Period**, and **Certificate Database** tabs, click **Next** to accept default values.

Step 15 Review the information in the **Confirmation** tab, and then click **Configure**.

Download CA certificate

This procedure assumes that you are using the Windows Certificate Services. Perform the following steps to retrieve the root CA certificate from the certificate authority. After you retrieve the root certificate, each user must install it in the browser used to access Finesse.

Procedure

Step 1 On the Windows domain controller, run the CLI command certutil -ca.cert *ca_name*.cer, in which *ca_name* is the name of your certificate.

Step 2 Save the file. Note where you saved the file so you can retrieve it later.

Deploy Root Certificate for Internet Explorer

In environments where group policies are enforced via the Active Directory domain, the root certificate can be added automatically to each user's Internet Explorer. Adding the certificate automatically simplifies user requirements for configuration.

Note To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

Procedure

Step 1 On the Windows domain controller, navigate to **Administrative Tools** > **Group Policy Management**.

Note Users who have strict Group Policy defined on the Finesse Agent Desktop are required to disable **Cross Document Messaging** from **Group Policy Management** to ensure proper functioning of Finesse on Internet Explorer 11.

Step 2 Right-click Default Domain Policy and select **Edit**.

Step 3 In the Group Policy Management Console, go to **Computer Configuration** > **Policies** > **Window Settings** > **Security Settings** > **Public Key Policies**.

Step 4 Right-click Trusted Root Certification Authorities and select **Import**.

Step 5 Import the *ca_name*.cer file.

Step 6 Go to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Certificate Services Client - Auto-Enrollment**.

Step 7 From the Configuration Model list, select **Enabled**.

Step 8 Sign in as a user on a computer that is part of the domain and open Internet Explorer.

Step 9 If the user does not have the certificate, run the command **gpupdate.exe /target:computer /force** on the user's computer.

Set Up CA Certificate for Internet Explorer Browser

After obtaining and uploading the CA certificates, either the certificate must be automatically installed via group policy or all users must accept the certificate.

In environments where users do not log directly in to a domain or group policies are not utilized, every Internet Explorer user in the system must perform the following steps once to accept the certificate.

Procedure

Step 1 In Windows Explorer, double-click the *ca_name*.cer file (in which *ca_name* is the name of your certificate) and then click **Open**.

Step 2 Click **Install Certificate** > **Next** > **Place all certificates in the following store**.

Step 3 Click **Browse** and select **Trusted Root Certification Authorities**.

Step 4 Click **OK**.

Step 5 Click **Next**.

Step 6 Click **Finish**.

A message appears that states you are about to install a certificate from a certification authority (CA).

Step 7 Click **Yes**.

A message appears that states the import was successful.

Step 8 To verify the certificate was installed, open Internet Explorer. From the browser menu, select **Tools** > **Internet Options**.

Step 9 Click the **Content** tab.

Step 10 Click **Certificates**.

Step 11 Click the **Trusted Root Certification Authorities** tab.

Step 12 Ensure that the new certificate appears in the list.

Step 13 Restart the browser for certificate installation to take effect.

Note If using Internet Explorer 11, you may receive a prompt to accept the certificate even if signed by private CA.

Set Up CA Certificate for Firefox Browser

Every Firefox user in the system must perform the following steps once to accept the certificate.

Note To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

Procedure

Step 1 From the Firefox browser menu, select **Options**.

Step 2 Click **Advanced**.

Step 3 Click the **Certificates** tab.

Step 4 Click **View Certificates**.

Step 5 Click **Authorities**.

Step 6 Click **Import** and browse to the *ca_name*.cer file (in which *ca_name* is the name of your certificate).

Step 7 Check the **Validate Identical Certificates** check box.

Step 8 Restart the browser for certificate installation to take effect.