Cisco Hosted Collaboration Solution for Contact Center Configuration Guide 12.5(1)

First Published: 2020-02-05

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

Change	See	Date
OpenJDK updates	Import CA Certificate into AW Machines, on page 134	Mar, 2021
	Import CCE Component Certificates, on page 137	
	Import Diagnostic Framework Portico Certificate into AW Machines, on page 138	
	Import VOS Components Certificate, on page 139	
	Java Upgrades, on page 490	
	Upgrade Tomcat Utility, on page 492	
Support for 36000 Agents on a 24000 Agent Reference Design	Support for 36000 Agents in HCS for CC 24000 Agent Deployment	February 2021
	Change Limits for Calls per Second	

Change	See	Date
Support for Edge Chromium (Microsoft Edge)	Set Up CA Certificate for Chrome and Edge Chromium (Microsoft Edge) Browsers	December 2020
	Accept Security Certificates	
	Install Microsoft Windows Server	
Initial Release of Document for Release 12.5(1)		February 2020
Added a new topic for certificates	Certificates for CCE Web Administration	
Updated topics with certificate details	Configure Customer Instance for the 2000 Agent Deployment Model Create a Customer Instance for the 4000 Agent Deployment Model Create Customer Instance for 12000 Agent Deployment Model Create Customer Instance for 24000 Agent Deployment Model Create Customer Instance for Small Contact Center Agent Deployment Model	
Added support for the Cloud Connect component	Cloud Connect	
Added support for Smart Licensing	Smart Licensing	

About this Guide

This document provides the reader with the necessary information to deploy, configure, and integrate a new Hosted Collaboration Solution for Contact Center(HCS for CC) for Contact Center instance with the required and in-place Hosted Collaboration Solution for Contact Center infrastructure. It provides a list of procedures you must perform to configure and integrate this solution.

This document requires the Hosted Collaboration Solution for Contact Center applications and infrastructure to be in place and ready for HCS for CC for CC deployment and integration. This document assumesHCS for CC for CC Golden Templates have been created for deployment and integration.

Audience

This document is intended for Cisco Authorized Technology Partners (ATP) personnel certified on or equivalently experienced with Cisco Unified Contact Center Enterprise(Unified CCE) products, design, requirements, installation and administration methods and procedures.

HCS for CC for Contact Center, as a subset of the Hosted Collaboration Solution for Contact Center, requires the reader to have a corresponding familiarity and experience with those required and optional applications, platforms and infrastructure.

Related Documents

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

For the installation procedure of Cisco HCS for Contact Center, see http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

For information on design, installation, and configuration of the Hosted Collaboration Solution applications and Infrastructure, see https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/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 Notice

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

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

- Cisco Security Advisories
- Field Notices

- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

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

Documentation Feedback

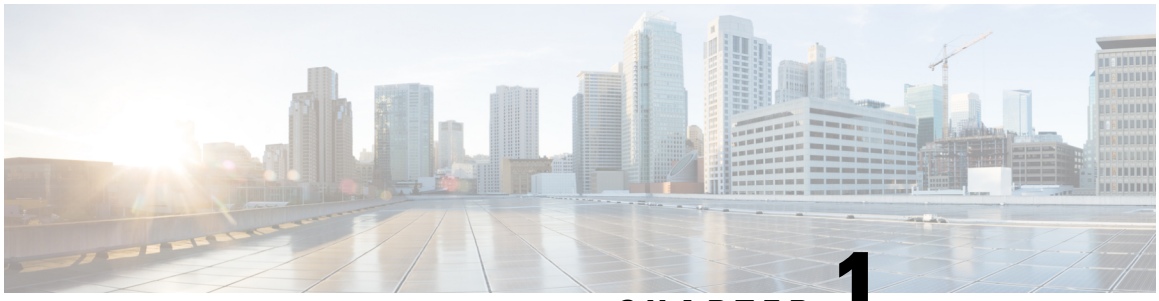
To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Conventions

This document uses the following conventions:

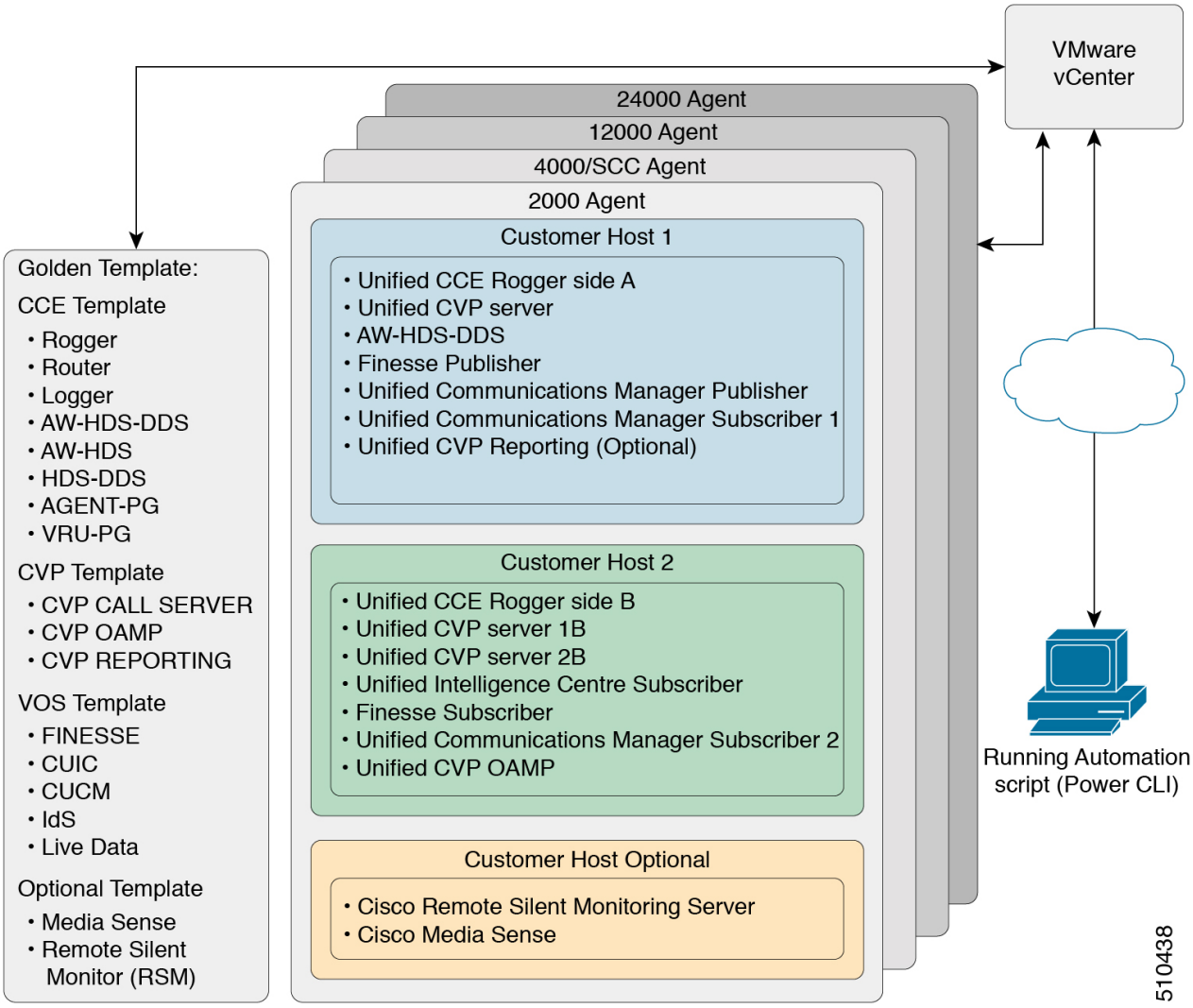
Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems, Inc. </title></html>`
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.



CHAPTER 1

Clone and OS Customization

Clone and OS Customization Process



Automated Cloning and OS Customization

For the following automation software and download information see, *Automation Software* section in *Cisco HCS for Contact Center Installing and Upgrading Guide* http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html

- GoldenTemplateTool
- PowerCLI
- OVF Tool

- WinImage

Automated Cloning and OS Customization Using Golden Templates

Sequence	Task	Done
1	Download Golden Template Automation Tool, on page 3	
2	Complete Automation Spreadsheet, on page 4	
3	Run Automation Script, on page 5	
4	OS Customization Process, on page 6	

Download Golden Template Automation Tool

Golden Template Tool is required for automated cloning of Golden Templates and deploying the customized Virtual machines in a customer instance. To download and extract the Golden Template Tool, see Automated Cloning and OS Customization, on page 2 to the root of the **C: drive** on your system. You can browse the automation scripts using VMware vSphere PowerCLI.

The extracted content includes the following:

- The *automation spreadsheet*s, which is the interface to the scripts.
- The *scripts* folder that contains five scripts. The deployVM.PS1 file is the primary automation script, which calls the other four scripts.
- The *Archive, Log, OVF, PlatformConfigRepository,* and *Report* folders are empty until you run the automation script for export.

After you run the script for the first time:

- *Archive* holds the prior versions of the automation spreadsheet, saved with a date and a time stamp.
- *Log* holds all the log files saved with a date and a time stamp.
- *OVF*, when the tool runs the Export operation, a sub folder is created for each virtual machine. The folders take their names from the GOLDEN_TEMPLATE_NAME cells in the spreadsheet. These folders are used to import the virtual machines to the customer ESXi host.
- *PlatformConfigRepository* is populated with three subfolders that holds XML files generated as part of the golden template process.
- *Report* holds all automation reports, saved with a date and a time stamp.

Related Topics

Automated Cloning and OS Customization, on page 2

Complete Automation Spreadsheet

Fill the information provided in the table to complete the automation spreadsheet for cloning process. Deploy VM automation script requires this information to clone the virtual machines to the customer instance.

The table describes the values of each virtual server and associated properties:

Column	Domain-based VM	Workgroup-based VM	VOS-based VM
CREATEVM	*YES*	*YES*	*YES*
CUSTOMIZATION	*YES*	*YES*	*YES*
OPERATION			
SOURCE_HOST_IP	*10.10.0.10*	*10.10.0.10*	*10.10.0.10*
SOURCE_DATASTORE_NAME	*Datastore-A0*	*Datastore-A0*	*Datastore-A0*
SOURCE_VMNAME			
OVF_NETWORK1			
OVF_NETWORK2			
GOLDEN_TEMPLATE_NAME	*GT-Rogger*	*GT-CVP-Server*	*GT-CUCM*
NEW_VM_NAME	*CCE-RGR-SIDE-A*	*CVP-SVR-SIDE-A*	*UCM-SUB-SIDE-A*
DEST_HOST_IP	*10.10.1.10*	*10.10.1.11*	*10.10.1.12*
DEST_DATASTORE_NAME	*Datastore-A1*	*Datastore-A3*	*Datastore-A6*
PRODUCT_VERSION			*10.0.1*
COMPUTER_NAME	*CCE-RGR-SIDE-A*	*CVP-SVR-SIDE-A*	*UCM-SUB-SIDE-A*
WORK_GROUP	*NO*	*YES*	
WORK_GROUP_NAME		*WORKGROUP*	
DOMAIN_NAME	*HCSCC.COM*		*HCSCC.COM* (Optional)
TIME_ZONE_LINUX_AREA			*America*
TIMEZONE_LINUX_LOCATION			*Los Angeles*
TIME_ZONE_WINDOWS	*(GMT-08:00)*	*(GMT-08:00)*	
DOMAIN_USER	*HCSCC\administrator*		
DOMAIN_PASSWORD	••••••••		
PRODUCT_KEY	*XXXX-XXXX-XXXX-XXXX*	*XXXX-XXXX-XXXX-XXXX*	
OWNER_NAME	*HCS*	*HCS*	
ORGANIZATION_NAME	*CISCO*	*CISCO*	*CISCO*
ORGANIZATION_UNIT			*HCS*
ORGANIZATION_LOCATION			*San Jose*

Column	Domain-based VM	Workgroup-based VM	VOS-based VM
ORGANIZATION_STATE			*CA*
ORGANIZATION_COUNTRY			*USA*
NTP_SERVER			*10.81.254.131*
NIC_NUM	*2*	*1*	*1*
IP_ADDRESS_NIC1	*10.10.10.10*	*10.10.10.20*	*10.10.10.30*
SUB_NET_MASK_NIC1	*255.255.255.0*	*255.255.255.0*	*255.255.255.0*
DEFAULT_GATEWAY_NIC1	*10.10.10.1*	*10.10.10.1*	*10.10.10.1*
DNS_IP_NIC1	*10.10.10.3*	*10.10.10.3*	*10.10.10.3*
DNS_ALTERNATE_NIC1			
IP_ADDRESS_NIC2	*192.168.10.10*		
SUB_NET_MASK_NIC2	*255.255.255.0*		
DEFAULT_GATEWAY_NIC2	*192.168.10.1*		
DNS_IP_NIC2	*192.168.10.3*		
DNS_ALTERNATE_NIC2			
VM_NETWORK1			
VM_NETWORK2			

Run Automation Script

Before you begin

Download and install VMware vSphere PowerCLI on the client computer.

Note Ensure WinImage (32-bit) is installed in the following location: C:\Program Files (x86)\WinImage

Note If you import any of the VOS VMs and have an unlicensed copy of WinImage, displays the popup for each VOS platform. Click **OK** to continue the import process.

Procedure

Step 1 Sign-in as an administrator and open **VMware vSphere PowerCLI (32-bit)** application.

Step 2 Enter the **get-executionPolicy** command to determine the restricted execution policy.

Step 3 If the policy is restricted, enter **set-executionPolicy** command. At the `Supply Values` prompt, enter **`Unrestricted`**, then enter **`Y`**.

Change the execution policy to run unsigned scripts on your local computer and signed scripts from other users.

Step 4 Enter the **CD < GoldenTemplate directory>** command.

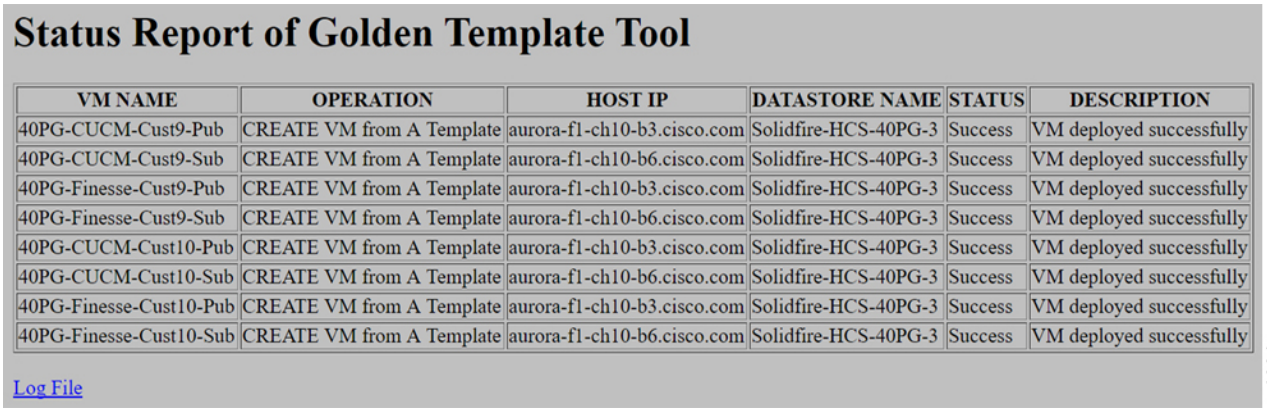
Step 5 Run the automation script using the following syntax:

Syntax:	*Example:*
<Path to the script> <Path of the spreadsheet> <vCenter IP / Hostname> <vCenter User> <Password to connect to vCenter>	`.\scripts\DeployVM.PS1 C:\GoldenTemplate\GoldenTemplate_VMDataSheet.xls` **testvCenter testuser testpassword**

This starts the script that parses and validates the data, creates entries in the `GoldenTemplate` directory. Displays the completion percentage on the screen and generates the `Status Report` in the `Report` folder.

Click the Log File link in the Status report to debug error conditions and to consult Cisco Support.

Figure 1: Status Report of Golden Template Tool



Status Report of Golden Template Tool

VM NAME	OPERATION	HOST IP	DATASTORE NAME	STATUS	DESCRIPTION
40PG-CUCM-Cust9-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-CUCM-Cust9-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust9-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust9-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-CUCM-Cust10-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-CUCM-Cust10-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust10-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust10-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully

Log File

510047

Related Topics

Automated Cloning and OS Customization, on page 2
OS Customization Process, on page 6

OS Customization Process

Sequence	Task	Done
Windows Customization Process		
1	Validate Network Adapter Settings and Power On, on page 7	
2	Edit Registry Settings and Restart VM, on page 7	
VOS Customization Process		
1	Configure DNS Server, on page 125	

Sequence	Task	Done
2	Configure Host in DNS Server , on page 126	
3	Validate Network Adapter Settings and Power On, on page 7	

Validate Network Adapter Settings and Power On

Perform this procedure for all Windows VMs.

Procedure

Step 1 Select the Virtual Machine in the vSphere client. Right-click the VM and choose **Edit settings**.

Step 2 On the **Hardware** tab, select each Network adapter. Make sure that **Connect at power on** in the Device Status group is checked:

Step 3 Power on the virtual machine.

Important Do not press Ctrl-Alt-Delete. If you press Ctrl-Alt-Delete after powering on, the customization does not take effect. You must complete it manually.

Step 4 Wait for the VM to restart and to apply customization. This can take five to ten minutes.

Recover from Pressing Ctrl-Alt-Del During Power-On

Validate Network Adapter Settings and Power On initializes the customization process. Although you are prompted to press **Ctrl-Alt-Delete** after powering on, doing do prevents the customization from taking effect. DO NOT press **Ctrl-Alt-Del**. If you inadvertently press **Ctrl-Alt-Del**, you have the following option to restore the customization.

Procedure

Step 1 Get the GoldenTemplate_VMDataSheet.xls from the `C:/GoldenTemplateTool/Archive`.

Step 2 Copy and paste the GoldenTemplate_VMDataSheet.xls to `C:/GoldenTemplateTool`.

Step 3 In the GoldenTemplate_VMDataSheet.xls select **`No`** in all the rows for the column CREATEVM except for those which needs to re-deploy.

Step 4 Else, you can enter that data manually for the VM.

Edit Registry Settings and Restart VM

Perform this procedure for all Windows VMs.

Procedure

Step 1 Select **Start** > **All Programs** > **Administrative Tools** > **Computer Management**.

Step 2 On the left panel, expand **Computer Management (Local)** > **System Tools** > **Local Users and Groups** > **Users**.

Step 3 On the right panel, right-click the administrator and select **Set Password**.

Step 4 Click **Proceed** at the warning message, then enter the new password.

Step 5 Click **OK**.

Step 6 Access the Registry Editor (**Start** > **Run** > **regedit**).

Step 7 Select **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **Windows NT** > **Current Version** > **Winlogon**.

a) Set **AutoAdminLogon** to **0**.

b) Remove these keys if they exist: **DefaultDomainName** and **DefaultUserName**.

Step 8 Restart the machine. If the machine is in the domain, log in to the domain.

Step 9 Enter **NET TIME /DOMAIN:<domain>** command to synchronize time with the domain controller.

Automated Cloning and OS Customization Using OVF

Sequence	Task	Done
1	Download Golden Template Automation Tool, on page 3	
2	Complete Automation Spreadsheet for Export, on page 8	
3	Run Automation Script for Export, on page 9	
4	Transport to Desired Location, on page 10	
5	Ensure Readiness of the Location, on page 11	
6	OS Customization Process, on page 6	

Complete Automation Spreadsheet for Export

Prerequisite:

Before the Export process, ensure that the VM has only one Network Adapter to export.

When you complete the automation spreadsheet to export, fill only the columns so that the export automation script creates export *OVFs* in the *OVF* subfolder of the GoldenTemplate directory.

Table 1: Required Columns for Automation Spreadsheet for Export

Column	Description	Example
CREATEVM	Select **NO** to skip VM creation.	NO
OPERATION	Select **ExportServer** to specify the operation you are performing with the script.	ExportServer
SOURCE_HOST_IP	The IP address of the physical server hosting the VM to be exported.	xx.xx.xxx.xxx
SOURCE_DATASTORE_NAME	The name of the Datastore defined in VMware.	datastore1(3)
SOURCE_VMNAME	The name of the VM that will be exported cannot contain spaces or special characters. Maximum of 32 characters.	TemplateRoggerA
GOLDEN_TEMPLATE_NAME	New Name for the Exported VM cannot contain spaces or special characters. Maximum of 32 characters.	CustomerRoggerA

Leave all the other columns blank.

Run Automation Script for Export

The export script processes the data in the export spreadsheet and validates that the required fields are present in the correct format.

The script creates a folder from which you can import the OVF at the desired location.

Note Run the script from the `GoldenTemplate` directory.

Before you begin

Download and install VMware vSphere PowerCLI on the client computer.

Procedure

Step 1 Launch **VMware vSphere PowerCLI (32-Bit)** as administrator.

Step 2 Enter **`get-executionPolicy`** command to determine whether the Restricted Execution policy is in effect or is unrestricted.

Step 3 If the policy is restricted, enter **`set-executionPolicy`** command. At the Supply Values prompt, enter **`Unrestricted`** and then enter **`Y`**. This changes the execution policy, so that you can run unsigned scripts that you write on your local computer and signed scripts from other users

Step 4 Enter **`cd < GoldenTemplate directory>`** command.

Step 5 Enter the command to run the automation script using the following syntax:

Syntax:	Example:
<**Path to the script**> <**Path of the spreadsheet**> <**vCenter IP / Hostname**> <**vCenter User**> <**Password to connect to vCenter**>	`.\scripts\DeployVM.PS1 C:\GoldenTemplate\GoldenTemplate_VMDataSheet.xls` **testvCenter testuser testpassword**

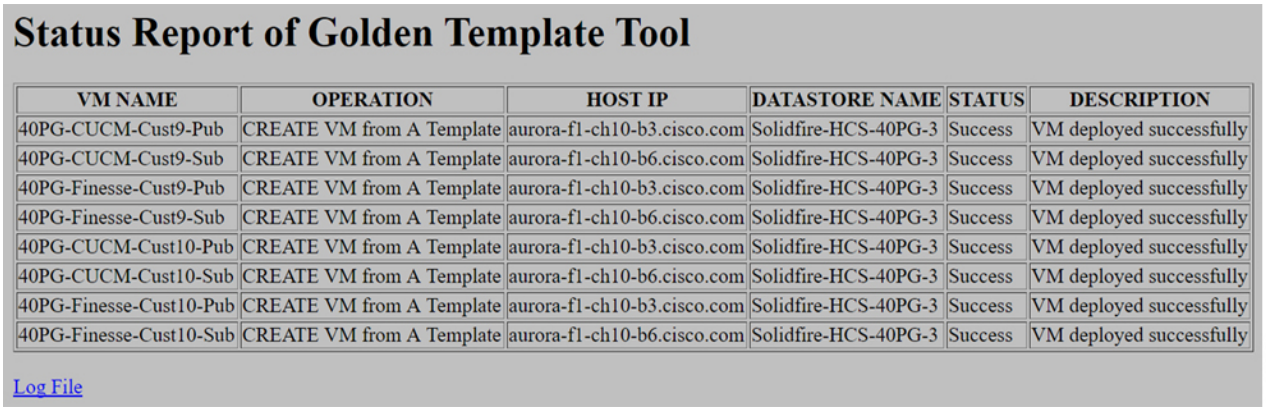
This starts a script that parses the data, validates the data, and creates entries in the `OVF` folder in the `GoldenTemplate` directory.

Script is run despite errors. Errors get displayed on the screen and stored in the log file.

Script takes several hours to complete.

After completion, script generates a status report in the `Report` folder. The status report has a link to the Log file. Use this file to debug error conditions and to consult with Cisco Support.

Figure 2: Status Report of Golden Template Tool



Status Report of Golden Template Tool

VM NAME	OPERATION	HOST IP	DATASTORE NAME	STATUS	DESCRIPTION
40PG-CUCM-Cust9-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-CUCM-Cust9-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust9-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust9-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-CUCM-Cust10-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-CUCM-Cust10-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust10-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust10-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully

Log File

510047

Related Topics

Automated Cloning and OS Customization, on page 2

Transport to Desired Location

After the successful completion of export process, the *OVF* files can be transferred to any desired location.

You can also transfer the GoldenTemplate directory to a USB device.

Note In that case, you would complete the import spreadsheet and run the import script from the USB drive.

Ensure Readiness of the Location

Before completing the import spreadsheet and running the import script, the environment must be set up with the following:

- the ESXihost or vCenter
- the datastores

Manual Cloning and OS Customization

Create Customization File for Windows Based Components

Complete the following procedure to create the customization file for windows based components .

Procedure

Step 1 In VMware vSphere Client, choose View > Management > Customization Specification Manager.

Step 2 Click **New**.

Step 3 On the New Customization Specification page, complete the new customization specification:

a) From the Target Virtual Machine OS menu, choose Windows.

b) Under the Customization Specification Information, enter a name for the specification and an optional description and click **Next**.

Step 4 On the Registration Information page, specify the registration information for this copy of the guest operating system. Enter the virtual machine owner's name and organization and click **Next**.

Step 5 On the Computer Name page, click the most appropriate computer name option that identifies this virtual machine on the network.

Step 6 On the Windows License page, specify the Windows licensing information for this copy of the guest operating system:

a) Enter your product volume license key.

b) Check **Include Server License information** (required to customize a server guest operating system).

c) Click **Per server** to specify the server license mode. Enter 5 as the maximum number of connections you want the server to accept. Click **Next**.

Step 7 On the Administrator Password page, enter a password for the administrator account and confirm the password by reentering it. Click **Next**.

Step 8 On the Time Zone page, choose the time zone for the virtual machine and click **Next**.

Step 9 On the Run Once page, click **Next**.

Step 10 On the Network page, choose the type of network settings to apply to the guest operating system and click **Next**:

a) Typical settings allow the vCenter server to configure all network interfaces from a DHCP server.
b) Custom settings require you to manually configure the network settings.

Step 11 On the Workgroup or Domain page, click Windows Server Domain and enter the destination domain, the username, and the password for a user account that has permission to add a computer to the specified domain.

Step 12 On the Operating System Options page, check Generate New Security ID (SID) to generate a new security identity and click **Next**.

Step 13 On the Ready to complete page, review your Customization File Summary, and then click **Finish**.

Deploy Virtual Machine from the Golden Template

Complete the following procedure to deploy the virtual machine from the golden template. Use the deployment checklists to record the hosts, IP addresses, and SAN locations for your deployment.

Procedure

Step 1 Right-click the template and choose Deploy Virtual Machine from this template.

Step 2 Enter a virtual machine name, choose a location, and click **Next**.

Step 3 On the Host/Cluster page, specify the host on which you want to store the template. Make sure that the host/cluster is valid. Click **Next**.

Step 4 Click **Advanced**. Specify a valid datastore for the virtual machine that complies with the Cisco HCS for CC for Contact Center component you deploy.

Step 5 Click **Next**.

Step 6 Make sure that the data store RAID levels for the component that you install comply with conditions specified in the table of SAN Configuration for your deployment model.

Step 7 Click **Thick provisioned Lazy Zeroed** to allocate a fixed amount of storage space to the virtual disk. Click **Next**.

Step 8 Click **Customize** using an existing customization specification and click **Next**.

Step 9 Select the customization file created in the Customization File for the Template.

Step 10 Review the settings for the new virtual machine. Click **Finish**.

Generate Answer File for VOS Product Virtual Machines

Complete the following procedure to generate an answer file for VOS product Virtual machines.

Procedure

Step 1 Open the link http://www.cisco.com/web/cuc_afg/index.html.

Step 2 Configure the following cluster-wide parameters:

a) Under Hardware, select **Virtual Machine** for **Primary Node Installed On**.
b) Under Product, select the product name and the product version.

c) Under Administrator credentials, enter the administrator username and password, and confirm the password.
d) Under Security Password, enter a password and confirm password.
e) Under the Application user credentials, enter the application username, password, and confirm the password.

Use the same System Application or Administrator credentials for all nodes.

f) Under Certificate information, enter the organization name, unit, location, state, and country for the Unified CM and Unified Intelligence Center.
g) Under SMTP, check the box **Configure SMTP host** and enter the SMTP location.

Step 3 Configure the following primary node parameters:

a) Under NIC Interface Settings, check the check box **Use Auto Negotiation**.

Note Do not change the MTU settings.

b) Under Network Information, enter the IP address, hostname ,IP mask, and gateway information.

Do not select the option **Use DHCP for IP Address Resolution**.

c) Under DNS, select the option **Configure Client DNS**, and enter Primary DNS IP and DNS name.
d) Under Timezone, select the option **Use Primary Time Zone Settings**.
e) Under Network Time Protocol, check **Use Network Time Protocol** and enter the IP address, NTP server name, or NTP Server Pool name for at least one external NTP server.

Step 4 Configure the following secondary node parameters:

a) Under NIC Interface Settings, check the check box **Use Auto Negotiation**.

Note Do not change the MTU settings.

b) Under Network Information, enter the IP address, hostname, IP mask, and gateway information.

Do not select the option **Use DHCP for IP Address Resolution**.

c) Under DNS, select the option **Configure Client DNS**, and enter primary DNS IP and DNS name.
d) Under Timezone, check **Use Primary Time Zone Settings** check box.
e) Under List of Secondary Nodes, click **Add Secondary Node**.

Step 5 Click **Generate Answer files & License MAC** to download the answer file for publisher and first subscriber.

Note For Unified CM, where an answer file for a second subscriber is required, close and open the answer file generator web page and enter the details for the publisher and second subscriber. Download the answer file for the second subscriber only, because you already downloaded the publisher file along with the first subscriber.

Step 6 Perform steps given in section for mounting the answer files to VM.

Related Topics

Copy Answer Files to Virtual Machines, on page 13

Copy Answer Files to Virtual Machines

Golden Template automation tool generates answer files for unattended installations. Individual answer files get copied to the *C:\GoldenTemplateTool_lO\PlatformConfigRepository* directory. These answer files are then converted to a floppy diskette file format and are used in addition to your VOS product DVD during the installation process.

Before you begin

Download and then install WinImage 8.5 on the client computer from which the automation scripts will be run. http://winimage.com/download.htm

Procedure

Step 1 Copy the generated Answer file to the folder and rename it to platformConfig.xml

Example:

Copy CUCM_PUB_SideA_platformConfig.xml to other location and rename it to platformConfig.xml

Step 2 Launch WinImage and select **File** > **New** > **1.44 MB** and click **OK**

Step 3 Drag and drop *platformConfig.xml* into WinImage

Step 4 When prompted to inject the file, click **Yes**.

Step 5 Select **File** > **Save As**

Step 6 From the **Save as type** list, choose **Virtual floppy image**. Provide the file name as *platformConfig.flp* and click **Save**

Step 7 Open vSphere infrastructure client and connect to the vCenter. Go to the customer ESXi host where the VMs are deployed

Step 8 Navigate to the **Configuration** tab. In the storage section, right click on the Datastore and choose **Browse Datastore**, create a folder named <Product_Node>

Example:

CUCM_PUB .

Step 9 **Upload** the *platformConfig.flp* file to the folder <Product_Node>.

Example:

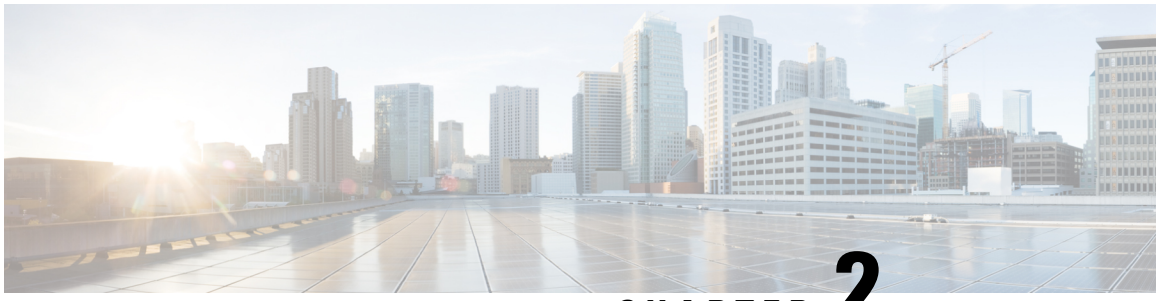
CUCM_PUB .

Step 10 Navigate to the <Product_Node> Virtual Machine*(Ex; CUCM_PUB_SideA)*. Right-click and choose **Edit Settings**

Step 11 On the Hardware tab, click **Floppy drive 1**, choose the radio button **Use The Existing Floppy Image in Datastore**.

Step 12 Mount the **platformConfig.flp** from the <Product_Node> folder *(Ex: CUCM_PUB)* on the data store and click **OK**

Step 13 Ensure that the Device status shows **Connect at Power On** checked for the Network adapter and for the Floppy drive and click **OK**.



CHAPTER 2

Configure Customer Instance

Configure Customer Instance for the 2000 Agent Deployment Model

Follow this sequence of tasks to create the customer instance to deploy 2000 agent for Cisco HCS for CC for Contact Center.

Table 2: Create customer instance for 2000 agent deployment of Cisco HCS for CC for Contact Center

Sequence	Task	Done?
1	Upgrade VMware Tools, on page 16	
2	Set Up Virtual Machine Startup and Shutdown, on page 16	
3	Create a Domain Controller Server, on page 17	
4	Configure Cisco Unified CCE Rogger, on page 20	
5	Configure Unified CCE AW-HDS-DDS, on page 31	
6	Configure Unified CCE PG, on page 36	
7	Configure Unified CVP, on page 48	
8	Configure Cisco IOS Enterprise Voice Gateway, on page 66	
9	Configure Unified Communications Manager, on page 72	
10	Configure Unified Intelligence Center Coresident Deployment, on page 79	

Sequence	Task	Done?
11	Configure Cisco Finesse, on page 93	

What to do next:

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

- CA certificates, see CA Certificates, on page 131

Upgrade VMware Tools

Procedure

Step 1 Right-click on the VM. Select **Guest** > **Install / Upgrade VMware tools**.

Step 2 Wait for the popup window (this may take time) and accept the default Automatic Tools Upgrade.

Step 3 Click **OK**.

Step 4 Restart, only if you are prompted.

Note VMWare Tools must be installed and up to date in all VMs.

Set Up Virtual Machine Startup and Shutdown

Procedure

Step 1 In the **VMware vSphere Client** window, select **ESXi server**.

Step 2 Click the **Configuration** tab.

Step 3 Click the **Virtual Machine Startup/Shutdown** link.

Step 4 Click **Properties**.

Step 5 In the **Virtual Machine Startup and Shutdown** dialog box, check the **Allow virtual machines to start and stop automatically with the system** check box.

Step 6 Use the **Move Up** and **Move Down** buttons to rearrange the virtual machines under **Automatic Startup** in the following order:

- Cisco Unified CCE Central Controller Servers
- Cisco Unified CCE Administration and Data Servers
- Cisco Unified CCE PG Servers
- Cisco Unified CVP Servers
- Cisco Finesse Servers
- Cisco Unified Intelligence Center

- Cisco Unified Communication Manager
- Cisco Unified CVP Reporting Server
- Cisco Unified CVP OAMP Server

Step 7 Click **OK**.

Create a Domain Controller Server

- Create a Virtual Machine for the Domain Controller, on page 17
- Install Microsoft Windows Server, on page 385
- Install Antivirus Software, on page 17
- .
- Configure a DNS Server, on page 20
- Create Two-Way Forest Trust, on page 20

Create a Virtual Machine for the Domain Controller

Procedure

Step 1 Create a new virtual machine from vCenter.

Step 2 On the **Name and Location** page, provide a name for the **Domain Controller**.

Step 3 In the **Disk format** field, choose the **Thick Provisioned** format.

Step 4 Enter the virtual machine specifications, see *Domain and Active Directory Considerations for HCSCC* section of *Solution Design Guide for Cisco Hosted Collaboration Solution for Contact Center* http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

Install Antivirus Software

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

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

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

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

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

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

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

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

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

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

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

Disable Port Blocking

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

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

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

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

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

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

The General Antivirus Guidelines section of the Security Guide for Cisco Unified ICM/Contact Center Enterprise at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

Enable DNS Server

Procedure

Step 1 Go to **Start > Server Manager**.

Step 2 In the **Server Manager** window, select **Manage > Add Roles and Features**.

Step 3 In the **Before You Begin** tab, click **Next**.

Step 4 In the **Installation Type** tab, choose **Role based or feature based installation** option and click **Next**.

Step 5 The **Server Selection** tab, displays the list of servers that are running on Windows Server. Select a server from this list and click **Next**.

Step 6 On the **Server Roles** tab, do the following:

a) Select the **Active Directory Domain Services** if you intend to promote a domain controller.

b) In the **Add Features that are required for Active Directory Domain Services?** dialog box, ensure the following tools are listed and then click **Add Features**.

- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AS LS Tools
      - [Tools] AS DS Snap-Ins and Command-Line Tools
      - [Tools] Active Directory Administrative Center

Step 7 Select **DNS Server**.

Step 8 In the **Add Features that are required for DNS Server?** dialog box, ensure the following tools are listed and then click **Add Features**.

- Remote Server Administration Tools
  - Role Administration Tools

- [Tools] DNS Server Tools

Step 9 In the **Features** tab, ensure **Remote Server Administration Tools and Role Administration Tools** are selected and click **Next**.

Step 10 In the **AD DS** tab, click Next.

Step 11 In the **DNS Sever** tab, click Next.

Step 12 n the **Confirmation** tab, click Install.
The **Result** tab displays the progress of the DNS server installation.

Step 13 After the installation completes, click on the **Promote this server to a domain controller** link to make the server a domain controller.

Step 14 In the **Deployment Configuration** tab, select **Add a New Forest,** enter a valid fully qualified domain DNS name, and click **Next**.

Note Enter a valid domain name that adheres to the naming conventions listed at https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and

Step 15 In the **Domain Controller Options** tab, enter the following and click **Next**:

a) From the **Forest functional level** drop-down list, select Windows Server version based on your AD version.

b) From the **Domain functional level** drop-down list, select Windows Server version based on your AD version.

Note You can also choose to set the forest functional level to an older Windows Server version.

c) Ensure that the **Domain Name System (DNS) Server** and the **Global Catalog (GC)** check box is checked.

d) Set the **Directory Services Restore Mode** password.

Step 16 In the **Additional Options** tab, enter the **NetBios** name and click **Next**.

Step 17 In the **Paths** tab, enter the paths where you would like to store the database, log files, and SYSVOL.

Step 18 In the **Review Options** tab, click **Next**.

Step 19 In the **Prerequisites Check** tab, you can read through the warning if any and click **Install**.
The **Results** page displays whether the installation was a success. The server will automatically reboot in 10 minutes.

Configure a DNS Server

To configuring a DNS server, see Configure DNS Server, on page 125.

Create Two-Way Forest Trust

To create two-way forest trust between Unified CCE and CCDM,

Configure Cisco Unified CCE Rogger

This table lists the configuration procedures you must perform to configure Cisco Unified CCE Rogger.

Sequence	Task	Done?
1	Configure Network Cards, on page 21	
2	Verify the Machine in Domain, on page 23	
3	Configure the Domain Manager, on page 24	
4	Configure Unified CCE Encryption Utility, on page 25	
5	Configure SQL Server for CCE Components, on page 25	
6	Allocate a Second Virtual Hard Drive, on page 26	
7	Configure the Unified CCE Logger, on page 27	
8	Configure the Unified CCE Router, on page 29	
9	Load Base Configuration, on page 30	
10	Verify Cisco Diagnostic Framework Portico, on page 45	
11	Cisco SNMP Setup, on page 45	

Configure Network Cards

Note Do this for all the Unified CCE virtual machines that have two network adapters.

Procedure

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

Step 2 Click **Change adapter settings** to open the Network Connections page.

Step 3 Rename the network adapter with Visible IP address configurations as **Visible**.

Step 4 Rename the network adapter with Private IP address configurations as **Private**.

Step 5 On the **Network Connections** page, press **Alt N** to display the Advanced menu.

Step 6 From the **Advanced** menu, select **Advanced Settings**.

Step 7 Under **Adapters and Bindings**, sort the connections so that `visible` is on top.

Step 8 Click **OK**.

Configure Private Ethernet Card

Procedure

Step 1 Right-click **private** and select **Properties**.

Step 2 Uncheck **Client for Microsoft Networks**.

Step 3 Uncheck **File and Printer Sharing for Microsoft Networks**.

Step 4 Uncheck **Internet Protocol Version 6 (TCP/IPV6)**.

Step 5 Check **Internet Protocol Version 4 (TCP/IPV4)** and click **Properties**.

a) Remove the IP Address for the Default Gateway.
b) Remove the IP Address for the Preferred DNS server.
c) Remove the IP Address for the Alternate DNS server.

Step 6 Click the **Advanced** button. Open the DNS tab. Uncheck **Register this connection's addresses in DNS**.

Step 7 Add an entry for the private IP address.

Note This IP address should have an entry in the DNS server. This would be required while adding the Router or a Peripheral Gateway through Websetup and PeripheralGatewaySetup respectively.

A host (A) resource record must be created in the **DNS' Forward Lookup Zones**, and can be of the form hostname followed by a suffix "p" to easily identify it as the private interface.

For example: If the host name is **RoggerA**, make an entry in the DNS as "RoggerAp" for the private IP address.

Step 8 Optional: Add another entry for the private high IP address.

Note This IP address should have an entry in the DNS server. This would be required while adding the Router or a Peripheral Gateway through Websetup and PeripheralGatewaySetup respectively.

A host (A) resource record must be created in the **DNS' Forward Lookup Zones**, and can be of the form hostname followed by a suffix "ph" to easily identify it as the private interface.

For example: If the host name is **RoggerA**, make an entry in the DNS as "RoggerAph" for the private high IP address.

Step 9 Click **OK** twice. Then, click **Close**.

Configure Public Ethernet Card

Procedure

Step 1 Right-click **Visible** and select **Properties**.

Step 2 Check **Client for Microsoft Networks**.

Step 3 Check **File and Printer Sharing for Microsoft Networks**.

Step 4 Uncheck **Internet Protocol Version 6 (TCP/IPV6)**.

Step 5 Check **Internet Protocol Version 4 (TCP/IPV4)** and click **Properties**.

Step 6 Confirm the **Public IP address**, **Subnet mask**, **Default gateway** and **Preferred DNs server**, and click **Advanced**.

Step 7 On the **Advanced** tab, enter the public IP addresses.

Step 8 On the DNS tab, in the DNS suffix for this connection field, enter the name of the local DNS zone for the server and check **Register this connection's addresses in DNS**.

Step 9 Optional: Add another entry for the public IP address.

Note This IP address should have an entry in the DNS server. This would be required while adding the Router or a Peripheral Gateway through Websetup and PeripheralGatewaySetup respectively.

A host (A) resource record must be created in the **DNS' Forward Lookup Zones**, and can be of the form hostname followed by a suffix "PuH" to easily identify it as the public interface.

For example: If the host name is **RoggerA**, make an entry in the DNS as "RoggerAPuH" for the public IP address.

Step 10 If the server requires access to resources in a different trusting or trusted domain or DNS zone, select **Append these DNS suffixes (in order)** and enter the local DNS zone for the server first, and then add the other secondary zones that represent the trusting or trusted domain.

Step 11 Click **OK** twice. Then, click **Close**.

Set Local Administrator Password

Procedure

Step 1 Open **Computer Management**.

Step 2 In left pane, expand **Local and Users Groups** and select **Users**.

Step 3 In right pane, right-click **administrator** and choose **Set password**.
Displays **Set Password for Administrator** dialog box.

Step 4 Click **Proceed**.

Step 5 Enter **New Password** and **Confirm Password**.

Verify the Machine in Domain

For Unified CCE golden template, the Automation Tool script clones and deploys the virtual machines automatically to the destination domain. Complete the following procedure to verify if the Virtual Machine is placed in destination domain.

For small contact center deployment model Agent PG can be in customer domain instead of service provider domain.

Procedure

Step 1 Log in to the Unified CCE machine.

Step 2 Navigate to **Start** > **All Programs** > **Administrative Tools** > **Server Manager** to verify if the Virtual Machine is mapped to correct domain. If the machine is not in Domain, follow the below steps.

Step 3 Click **Change System Properties** on Right side panel to open System Properties.

Step 4 In Computer name tab, Click **Change**.

Step 5 Choose **Domain** radio button to change the member from Workgroup to Domain.

Step 6 Enter fully qualified Domain name and Click **OK**.

Step 7 In Windows security pop-up, Validate the domain credentials and click **OK**.

Step 8 On successful authentication, Click **OK**.

Step 9 Reboot the server and login with domain credentials.

Configure the Domain Manager

This procedure creates a organizational unit (Cisco_Unified CCE, facility,instance) from any of the Unified CCE PGs.

Note The domain manager is a one-time configuration. You do not need to configure the domain manager for side B.

Note For Small Contact Center agent deployment model, follow the below procedure to create OU structure for the Agent PG in sub customer domain similar to the Unified CCE domain or skip the below procedure if you want to install Agent PG in the Unified CCE domain.

Procedure

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

Step 2 Select the **Domain Manager** icon from the list of applications.

Step 3 Log in as a user who has permissions to create organizational units (OUs) in the domain.

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

Step 5 Add the Cisco root as Cisco_Unified CCE :

a) Under the Cisco root, click **Add**.

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

When you return to the **Domain Manager** dialog box, the Cisco root OU appears either at the domain root or under the OU that you selected. You can now add the facility.

Step 6 Add the facility organizational unit (OU):

a) Select the Cisco root OU under which you want to create the Facility OU.

b) In the right section, under **Facility**, click **Add**.

c) Enter the name for the **Facility**and click **OK**.

Step 7 Add the Instance OU:

a) Navigate to and select the Facility OU under which you want to create the Instance OU.
b) In the right section, under , click **Add**.
c) Enter the instance name and click **OK**.

Step 8 Click **Close**.

Configure Unified CCE Encryption Utility

Procedure

Step 1 Start **All Programs** > **Cisco Unified CCE Tools**.
Step 2 Select **SSL Encryption Utility**.
Step 3 Click the **Certificate Administration** tab.
Step 4 Click **Uninstall**. Select **Yes**.
Step 5 When the uninstallation completes, choose **Install**.

You see a stream of messages, ending with *SSL Certificate successfully installed*.

Step 6 Click **Close**.

What to do next

Create and Bind System CLI Certificate, on page 25

Create and Bind System CLI Certificate

Complete the following procedure to create and bind the system CLI certificate:

Procedure

Step 1 Open the command prompt.
Step 2 Enter the command **cd C:\icm\serviceability\diagnostics\bin** and press **Enter**.
Step 3 Enter the command **DiagFwCertMgr /task:CreateAndBindCert** and press **Enter**.

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.

Allocate a Second Virtual Hard Drive

After deploying the OVA files, the second hard drive is no longer automatically created. To create a second hard drive:

Procedure

Step 1 Right-click the virtual machine and click **Edit Settings**.

Step 2 In the **Virtual Hardware** tab, click on **Add New Device**.

Step 3 You can select the type of device you wish to add. Select **Hard Disk**. The new hard disk appears. Assign the desired disk space to the hard disk.

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

Virtual Machine Template	Default Second Disk Size
Logger	500 GB
Rogger	150 GB
AW-HDS-DDS	500 GB
AW-HDS	500 GB
HDS-DDS	500 GB

You can custom size the SQL database disk space to meet data retention requirements, as calculated by the Database Estimator tool.

Step 4 On the **Disk Provisioning** section, choose **Thick provision Lazy Zeroed**.

Step 5 In the **VM Options** > **Advanced Options** section, retain the default options.

Step 6 Click **OK** to confirm the changes.

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

Configure the Unified CCE Logger

Configure the Unified CCE logger for Side A and Side B.

Note Ensure that your browser is enabled.

Procedure

Step 1 Launch the **Unified CCE Web Setup**.

Step 2 Sign in using as domain user having local Administrator permissions.

Step 3 Click **Instance Management**, and then click **Add**.

Step 4 In the **Add Instance** window, select **Facility and Instance** from the drop-down list.

Step 5 In the **Instance Number** field, enter `0` and click **Save**.

Step 6 Configure the logger database as follows:

a) Open **ICMDBA** application.
b) Select **Server** > **Instance** (logger being installed).
c) Right-click the instance name and choose **Create** to create the logger database.
d) In **Select Component** dialog box, choose the logger you are working on (Logger A or Logger B). Click **OK**.
e) In **Select Logger Type** window, select **Enterprise** from the drop-down list. Click **OK**.

Step 7 In **Create Database** window, configure the following to create the Log:

a) From **DB Type** drop-down list, choose either **side A** or **side B**.
b) Choose **Region**.
c) In **Storage** pane, click **Add**.

Step 8 In **Add Device** dialog box, configure as follows:

a) Select **Log**.
b) Choose **C** drive.
c) Accept the default in the size field.
d) Click **OK**.

Step 9 In **Create Database** window, in **Storage** section, click **Add**.

Step 10 In **Add Device** dialog box, configure as follows:

a) Select **Data**.
b) Choose the secondary drive (typically E).
c) Accept the default in the size field.
d) Click **OK**.

Step 11 In **Create Database** window, click **Create** and click **Start**.

When you see the successful creation message, click **OK** and click **Close**.

Step 12 Configure the logger component as follows:

a) Return to **Unified CCE Web Setup**. You might need to log in again.
b) Choose **Component Management** > **Loggers**.

c) Click **Add** and choose the **Instance**.
d) From **Fault Tolerance Mode** drop-down list, choose **Duplexed** option and click **Next**.
e) In **Central Controller Connectivity** window, enter the host names for Sides A and B for the Router Private Interface and Logger Private Interface and click **Next**.

Step 13 In **Additional Options** window, configure as follows:

a) Check the **Enable Historical/Detail Data Replication** check box.
b) Check the **Display Database Purge Configuration Steps** check box and click **Next**.

Step 14 In **Data Retention** window, in the data retention table, retain the default values and click **Next**.

Step 15 In **Data Purge** window, configure purge for a time when there is low demand on the system. Click **Next**.

Step 16 In the **Summary** window

a) Enter the domain user.

Verify that the user is created in the specified domain,

For more information on creating the domain user, see Create Users in Active Directory, on page 161.

b) Enter the valid password.
c) Review the Summary and click **Finish**.

Note Do not start service until all Unified CCE components are installed.

Caution Use the same domain user account for all the distributor and logger services. If you want to use different domain accounts for the logger and the distributor, ensure that the distributor service user account is added to the local logger `UcceService` groups on Side A and Side B.

What to do next

Set database and log file size, see Database and Log File Size, on page 28.

Database and Log File Size

Complete the following procedure to increase the database and log sizes.

Before you begin

To calculate database and log file size, download and use the Database Size Estimator from https://software.cisco.com/download/type.html?mdfid=268439622&catid=null.

Alternative option is to size the database and log using the values from the following table.

Procedure

Step 1 Open **SQL Server Management Studio**.

Step 2 Click **Connect**. In the left pane, expand **Databases**.

Step 3 Right-click Logger database [<Instance>_<Side>] and select Properties..

Step 4 In the left pane, select **Files**. Ensure that **Auto Growth** is disabled for data and enabled for log files. Log files automatically grow in 10 percent increments.

Step 5 Set the initial size of the data and log files according to the Database Size Estimator or from the following table:

Table 3: Data and Log File Size

Database	Data size(MB)	Log Size(MB)	Deployment Type
Side A, Side B	409600	1024	12000 and 24000 agent
Side A, Side B	122900	1024	Other HCS for CC for CC Deployments

Configure the Unified CCE Router

Procedure

Step 1 Launch the Unified CCE Web Setup.

Step 2 Sign in as the domain user with local Administrator permission.

Step 3 Click **Instance Management**, and then click **Add**.

Step 4 In the **Add Instance** window, select **Facility and Instance** from the drop-down list.

Step 5 In the **Instance Number** field, enter `0`. Click **Save** .

Step 6 Select **Component Management** > **Routers**.

Step 7 Click **Add** to set up the Call Router.

Step 8 In the **Deployment window**, select the appropriate **Side**.

Step 9 Select **Duplexed** as Fault Tolerance Mode. Click **Next**.

Step 10 In the **Router Connectivity** window, configure the Private Interface and Public (Visible) Interfaces. Click **Next**.

Step 11 In the **Enable Peripheral Gateways** dialog box, enter the following in the Enable Peripheral Gateways field. Click **Next**.

- For 2000 agents deployments, typically `2-4`.
- For 4000 agents deployment, typically `2-4`.
- For 12000 agents deployment, typically `2-16`.
- For 24000 agents deployment, typically `2-32`.

Step 12 In the **Router Options** window, configure as follows:

a) Check **Enable Database Routing**.
b) Check **Enable Quality of Service (QoS)**. (Applicable to Side A only.)
c) Click **Next**.

Step 13 In **Router Quality of Service** window, click **Next**. (Applicable to Side A only.)

Step 14 In the **Summary** window, make sure that the router summary is correct, then click **Finish**.

Note
- Do not start the service until all Unified CCE components are installed.

What to do next

To enable the **DNWildcard**, select the Registry > HKEY_LOCAL_MACHINE > SOFTWARE > Cisco Systems > ICM > <instance> >RouterA > Router > CurrentVersion > Configurations > Global, and select the DNWildcardEnabled and set to `1`.

Load Base Configuration

Complete this procedure to import base configuration parameters.

Procedure

Step 1 Based on your timezone, download the HCS-CC_12.5.1-Day1_2000_NA.zip or HCS-CC_12.5.1-Day1_2000_UK.zip file. Save it locally and unzip it.

Step 2 Download the Domain_Update_Tool.zip file. Save it locally and unzip it.

Step 3 Copy the configuration folder to the local drive of Unified CCE Rogger on Side A.

Step 4 Open the ICMDBA Tool on the Unified CCE Rogger on Side A.

Step 5 Select the Unified CCE Rogger and expand the tree to <instance name>_sideA.

Step 6 Select Data on the menu bar and click **Import**.

Step 7 Browse to locate the configuration folder and click **Open**.

Step 8 Click **OK** and then click **Import**.

Step 9 Click **Start** and then click **OK** on all messages.

Step 10 Navigate to the folder Domain_Update_Tool and right-click UpdateDomain.PS1. and Run with PowerShell. Respond as follows:

a) For Server name, enter the computer name of the Unified CCE Rogger Side A.
b) For Database name, enter <instance_sideA (Logger database)>.
c) For Domain Name, enter the customer's domain name.

Step 11 Return to the ICMDBA tool. Select Logger <instance name> database for the side that you want to synchronize.

Step 12 Click **Data** in menu bar and select **Synchronize** and perform the following:

a) In **Synchronize** window, click **Add** in **Source** pane.
b) Enter hostname for Unified CCE Rogger of source in **Server Name** field and click **OK**.
c) Click **Add** in **Destination** pane.
d) Enter hostname for Unified CCE Rogger of destination in **Server Name** field and click **OK**.
e) Click **Synchronize**.

Step 13 Click **Start** and then click **OK** on all messages.

Configure Unified CCE AW-HDS-DDS

This section explains the configuration procedures you must perform for the Unified CCE AW-HDS-DDS for Sides A and B.

Table 4: Configuring Unified CCE AW-HDS-DDS for Side A and Side B

Sequence	Task	Done?
1	Configure Network Cards, on page 21	
2	Validate Network Card, on page 49	
3	Configure Unified CCE Encryption Utility, on page 25	
4	Configure SQL Server for CCE Components, on page 25	
5	Allocate a Second Virtual Hard Drive, on page 26	
6	AW-HDS-DDS, on page 31	
7		
8	Verify Cisco Diagnostic Framework Portico, on page 45	
9	Cisco SNMP Setup, on page 45	
10	Set the HCS for CC Deployment Type, on page 34	

AW-HDS-DDS

- Create Instance, on page 31
- Create HDS Database, on page 32
- Configure AW-HDS-DDS, on page 32
- Database and Log File Size, on page 34
- Set the HCS for CC Deployment Type, on page 34

Create Instance

Procedure

Step 1 Launch Unified CCE Web Setup from the desktop and log in using the Domain Administrator credentials to complete the installation.

Step 2 Click **Instance Management**, and then click **Add**.

Step 3 In the Add Instance window, select **Facility** and **Instance** from the drop-down list.

Step 4 In the Instance Number field, enter **0**. Click **Save**.

Create HDS Database

Procedure

Step 1 Configure the HDS database as follows:
a) Choose **Start > Programs > Cisco Unified CCE Tools > ICMdba**.
b) Navigate to **Server > Instance**.
c) Right-click the instance and choose **Create**.

Step 2 In the Select Component dialog box, choose **Administration & Data Server** from the drop-down list. Click **OK**.

Step 3 At the prompt, *SQL Server is not configured properly. Do you want to configure it now?"* Click **Yes**.

Step 4 On the Configure page, in the **SQL Server Configurations** pane check **Memory (MB)** and **Recovery Interval**. Click **OK**.

Step 5 On the Stop Server page, click **Yes** to stop the services.

Step 6 In the **Select AW Type** dialog box, choose **Enterprise** from drop-down list. Click **OK**.

Step 7 In the **Create Database** dialog box, configure as follows:
a) In the DB Type field, choose **HDS** from drop-down.
b) In the Storage pane, click **Add**.

Step 8 In the Add Device dialog box, configure as follows:
a) Select **Data**.
b) Select the secondary drive (typically **E**).
c) Accept the default in the size field.
d) Click **OK**.

Step 9 In the Create Database dialog box, under Storage, click **Add**.

Step 10 In the Add Device dialog box, configure as follows:
a) Select **Log**.
b) Select the **C** drive.
c) Accept the default in the size field.
d) Click **OK**.

Step 11 In the Create Database dialog box, configure as follows:
a) Click **Create**.
b) Click **Start**.
c) Click **OK**.
d) Click **Close**.

Configure AW-HDS-DDS

Complete the following procedure to install the Cisco Unified CCE Administration Server & Real-time Data Server, Historical Data Server, and Detailed Data Server (AW-HDS-DDS).

Before you begin

Create a domain user if a domain user does not exist already for that service account. For more information on creating the domain user, see *Create Users in Active Directory*.

Procedure

Step 1 Choose **Component Management** > **Administration & Data Servers**.

Step 2 Click **Add**.

Step 3 On the Deployment window, choose the current instance.

Step 4 On the Add Administration & Data Servers window, 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 window, configure as follows:

a) Choose the option **Administrator Server Real-time Data Server**, **Historical Data Server**, and **Detailed Data Server (AW-HDS-DDS)**.
b) Click **Next**.

Step 6 On the Administration & Data Servers Connectivity window, configure as follows:

a) Select **Primary Administration & Data Server**.
b) Enter the hostname of the Secondary AW-HDS-DDS in the *Secondary Administration & Data Server field.
c) Enter the site name in the Primary/Secondary Pair (Site) Name field.

Note Ensure that the site name match with the site name defined under **PG Explorer** > **Agent Peripheral** > **Agent Distribution**.

d) Click **Next**.

Step 7 On the Database and Options window, configure as follows:

a) In the Create Database(s) on Drive field, select **E**.
b) Check **Configure Management Service (CMS) Node**.
c) Check **Internet Script Editor (ISE) Server**.
d) Check **Next**.

Step 8 On the Central Controller Connectivity window, configure as follows:

a) For Router Side A enter the host name/IP address machine where Router A resides.
b) For Router Side B enter the host name/IP address machine where Router B resides.
c) For Logger Side A enter the host name/IP address machine where Logger A resides.
d) For Logger Side B enter the host name/IP address machine where Logger B resides.
e) Enter the **Central Controller Domain Name**.
f) Click **Central Controller Side A Preferred**.
g) Click **Next**.

Step 9 In the **Summary** window

a) Enter the domain user of the service account.

Create a domain user if a domain user does not exist already for that service account. For more information on creating the domain user, see Create Users in Active Directory, on page 161.

b) Enter the valid password.
c) Review the Summary and click **Finish**.

Note Do not start service until all Unified CCE components are installed.

Caution Use the same domain user account for all the distributor and logger services. If you want to use different domain accounts for the logger and the distributor, ensure that the distributor service user account is added to the local logger `UcceService` groups on Side A and Side B.

Database and Log File Size

Complete the following procedure to increase the database and log sizes.

Before you begin

Use Database Size Estimator to calculate database and log file size.

Alternative option is to size the database and log using the values from Table 5: Data and Log File Size, on page 34.

Procedure

Step 1 Open **Microsoft SQL Server Management Studio**.

Step 2 Expand the Database in Object Explorer.

Step 3 Select **HDS database**. Right-click on the database and select **Properties**.

Step 4 Click **Files** to increase the database and log sizes.

Step 5 Ensure that **Auto Growth** is disabled for data and enabled for log files. Log files automatically grow in 10 percent increments.

Step 6 Set the initial size of the data and log files according to Database Size Estimator or from the following table:

Table 5: Data and Log File Size

Database	Data size (MB)	Log Size
<instance>_hds	409600	1024

Set the HCS for CC Deployment Type

Before you begin

- Ensure that a domain user logging into **CCE Web Administration** is part of the `UcceConfig local` group of all Unified CCE AW DB (real-time distributor) machines.
- Import self-signed certificate from CCE AW component into the AW Machine where the deployment type would be set. For more information, see .

Procedure

Step 1 Launch **CCE Web Administration**.

Step 2 Login with user credentials.

Step 3 Set the HCS for CC for CC Deployment Type

a) Click **Deployment** under the **System** tab

b) Select the Deployment Type from the drop-down list.

Note For small contact center agent deployment, select Deployment type as **HCS for CC 4000 Agents**

c) Click **Save** and click **Yes** on the warning message.

Step 4 View the Deployment Type.

a) Click **Home** tab to view the deployment type

Step 5 View the System Validation Rules

a) Click **Information** under the **System** Tab

b) Click **System Validation**

Step 6 View the System Configuration Limits

a) Click **Information** under the **System** Tab

b) Click **Capacity Info**

What to do next

Set the principal AW and configure it with the Diagnostic Framework Service domain, username, and password if you have not already.

Configure Permissions in the Local Machine

In this release,Unified CCE defaults to providing user privileges by memberships to local user groups on local machines. This technique moves authorization out of Active Directory. However, it requires a one-time task on each local machine to grant the required permissions.

Note You can use the ADSecurityGroupUpdate registry key to choose between the new default behavior and the previous behavior. For more information, see the chapter on solution security in the Solution Design Guide.

Before using the Configuration Manager tool, configure the required registry and folder permissions for the `UcceConfig` group.

Configure Registry Permissions

This procedure only applies to all the AW machines. Grant the required registry permissions for the `UcceConfig` group on the local machine.

Procedure

Step 1 Run the `regedit.exe` utility.

Step 2 Select `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM`.

Step 3 Right-click and select **Permissions**.

Step 4 If necessary, add `UcceConfig` in **Group or user names**.

Step 5 Select `UcceConfig` and check **Allow** for the **Full Control** option.

Step 6 Click **OK** to save the change.

Step 7 Repeat the previous steps to grant **Full Control** to the `UcceConfig` group for `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco Systems, Inc.\ICM`.

Step 8 Repeat the previous steps to grant **Full Control** to the `UcceConfig` group for `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2`.

Note If you have configured the Unified CCE Administration Client, open Local security policy and go to **User Rights Assignment**. Right click **Create Global Object**. Go to **properties** and add the local Group `UcceConfig`.

Configure Folder Permissions

Grant the required folder permissions to the `UcceConfig` group on the local machine.

Procedure

Step 1 In Windows Explorer, select `<ICM install directory>\icm`.

Step 2 Right-click and select **Properties**.

Step 3 On the **Security** tab, select `UcceConfig` and check **Allow** for the **Full Control** option.

Step 4 Click **OK** to save the change.

Step 5 Repeat the previous steps to grant **Full Control** to the `UcceConfig` group for `<SystemDrive>:\temp`.

What to do next

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

Configure Unified CCE PG

The following table explains the tasks that you must perform to configure Unified CCE PG on both side A and B.

Table 6: Configure Unified CCE Unified PG on Side A and B

Sequence	Tasks	Done?
1	Configure Network Cards, on page 21	

Sequence	Tasks	Done?
2	Validate Network Card, on page 49	
3	Configure Unified CCE Encryption Utility, on page 25	
4	Configure CUCM Peripheral Gateway, on page 37	
5	Configure VRU Peripheral Gateway, on page 40	
6	Configure MR Peripheral Gateway, on page 41	
7	Configure CTI Server, on page 43	
8	Upgrade Cisco JTAPI Client on PG, on page 44	
9	Verify Cisco Diagnostic Framework Portico, on page 45	
10	Cisco SNMP Setup, on page 45	
11	Start Unified CCE Services, on page 48	

Configure CUCM Peripheral Gateway

Complete the following tasks to configure CUCM peripheral gateways for the PG Server on Side A and then repeat the same procedure for Side B.

- Configure CUCM PG, on page 37
- Prepare to Add PG, on page 38
- Add CUCM PG, on page 38
- Add CUCM PIM, on page 38
- After Creating PIMs, on page 39

Configure CUCM PG

Before you begin

You can lauch the **Configuration Manager** after logging into a windows machine only if you are a domain administrator or part of any one of the following groups:

- `UcceConfig Local` group
- `Local administrator` group

Procedure

Step 1 Open **Configuration Manager > PG Explorer**.

Step 2 Select the option **Enable Agent Reporting for CUCMPG1 Routing Client**.

Step 3 Enter the Primary and Secondary CTI address and port information in the **Unified Communications Manager PG** for the Cisco Unified WIM and EIM feature.

Step 4 In the **Agent Distribution** tab, enter a site name in **Administration and Data Server** field.

Prepare to Add PG

Procedure

Step 1 Open **Peripheral Gateway Setup**.

Step 2 In the **ICM Instances** pane, click **Add**.

Step 3 In the **Add Instance** window, select the appropriate **Facility** and **Instance Name** from the drop-down list.

Step 4 In the **Instance Number** field, enter `0`.

Step 5 Click **Save**.

Add CUCM PG

Procedure

Step 1 Open **Peripheral Gateway Setup**.

Step 2 In the **Instance Components** pane, click **Add**.

Step 3 From the **ICM/CCE/CCH Component Selection** dialog box, select **Peripheral Gateway**.

Step 4 In the **Peripheral Gateway Properties** dialog box:

a) Check the **Production mode** check box.
b) Check the **Auto start at system startup** check box.
c) Check the **Duplexed Peripheral Gateway** check box.
d) In the **PG Node Properties ID** pane, from the **ID** drop-down list, select the appropriate PG.
e) Select the appropriate side (**Side A** or **Side B**).
f) In the **Client Type Selection** pane, add **CUCM** to the **Selected types**.
g) Click **Next**.

Add CUCM PIM

Procedure

Step 1 In the **Peripheral Gateway Component Properties** window, click **Add**.

Step 2 From the **Client Type** drop-down list, select **CUCM**.

Step 3 From the **Available PIMS** list, select **PIM**, then click **OK**.

Step 4 In the **CUCM Configuration** dialog box, check the **Enabled** check box.

Step 5 In the **Peripheral name** field, enter the peripheral name.

Step 6 In the **Peripheral ID** field, enter the logical controller ID.

Step 7 In the **Agent Extension Length** field, enter the extension length for this deployment.

Note For the SCC deployment model, agent extension length is 8.

Step 8 In the **CUCM Parameters** pane, configure as follows:

a) In the **Service** field, enter the hostname of appropriate Unified Communications Manager subscriber.
b) In the **User ID** field, enter the user ID.
c) In the **User Password** field, enter the Unified Communication Manager password.
d) In the **Mobile Agent Codec** field, select **G.711U or G.711A or G.729**.
e) Click **OK**.

Step 9 Repeat these steps to configure the remaining PIMs.

Unified Communication Domain Manager sets the default password as "pguser", during Unified Communication Manager Integration.

After Creating PIMs

Procedure

Step 1 In the **Logical Controller ID** field, enter the logical controller ID of the PIM.

Step 2 In the **CTI Wrapup Data Delay** field, enter 0, then click **Next**.

Step 3 In the **Device Management Protocol Properties** window:

a) Select the appropriate side (**Side A** or **Side B**).
b) In the **Side A Properties** panel, select **Call Router**.
c) In the **Side B Properties** panel, select **Call Router**.
d) In the **Usable Bandwidth (kbps)** field, retain the default values.
e) In the **Heartbeat Interval (100ms)** field, enter **4**, then click **Next**.

Step 4 In the **Peripheral Gateway Network interfaces** window, enter **PG Private Interfaces** and **PG Visible (Public) Interfaces**.

Step 5 For Side A only:

a) In the **Private Interfaces** pane, click **QoS**.
b) In the **PG Private Link QoS Settings** pane, check the **Enable QoS** check box, then click **OK**.
c) In the **Visible(Public) Interfaces**, click **QoS**.
d) In the **PG Private Link QoS Settings** pane, check the **Enable QoS** check box, then click **OK**.

Note For 12000, 24000, and SCC deployments, if there are six or more Agents PGs, then QoS must be disabled.

Step 6 In the **Peripheral Gateway Network Interfaces** window, click **Next**.

Step 7 In the **Check setup Information** window, click **Next**.

Step 8 In the **Setup Complete** window, click **Finish**.

Note Do not start Unified CCE /CCNodeManager until all Unified CCE components are installed.

Configure VRU Peripheral Gateway

- Add VRU PG, on page 40
- Add VRU PIM, on page 40
- After Creating PIMs, on page 39

Add VRU PG

Procedure

Step 1 Open **Peripheral Gateway Setup**.

Step 2 In the **Instance Components** pane, click **Add**.

Step 3 From the **Component Selection** dialog box, select **Peripheral Gateway**.

Step 4 In the **Peripheral Gateway Properties** dialog box:

a) Check the **Production mode** check box.
b) Check the **Auto start at system startup** check box.
c) Check the **Duplexed Peripheral Gateway** check box.
d) In the **PG Node Properties ID** pane, from the **ID** drop-down list, select **PG3**.
e) Select the appropriate side (**Side A** or **Side B**).
f) In the **Client Type Selection** pane, add **VRU** to the **Selected types**.
g) Click **Next**.

Add VRU PIM

Caution Before you enable secured connection between the components, ensure to complete the security certificate management process.

For more information, see 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.

Procedure

Step 1 In the **Peripheral Gateway Component Properties** window, click **Add**.

Step 2 From the **Client Type** drop-down list, select **VRU**.

Step 3 Select the appropriate PIM from the **Available PIMS** list, then click **OK**.

Step 4 In the **Configuration** dialog box, check the **Enabled** check box.

Step 5 In the **Peripheral name** field, enter the CVP server name.

Step 6 In the **Peripheral ID** field, enter the logical controller ID of CVP server.

Step 7 In the **VRU Hostname** field, enter the hostname of the CVP server.

Step 8 In the **VRU Connect port** field, enter `5000`.

Step 9 In the **Reconnect interval (sec)** field, enter `10`.

Step 10 In the **Heartbeat interval (sec)** field, enter `5`.

Step 11 From the **DSCP** drop-down list, select **CS3(24)**.

Step 12 Check the **Enable Secured Connection** option to enable secured connection.

This establishes a secured connection between VRU PIM and CVP.

Step 13 Click **OK**.

Step 14 Repeat these steps to configure the remaining PIMs.

Configure MR Peripheral Gateway

- Add Media Routing PG, on page 41
- Add Multichannel PIM to 2000 Agent Deployment, on page 42
- Add Outbound PIM, on page 43
- After Creating PIMs, on page 39

Add Media Routing PG

Configure Media Routing PG, though Multichannel and Outbound are not used. In this case, Media Routing PG remains idle or disabled.

Procedure

Step 1 Open **Peripheral Gateway Setup**.

Step 2 In the **Instance Components** pane, click **Add**.

Step 3 From the **Component Selection** dialog box, select **Peripheral Gateway**.

Step 4 In the **Peripheral Gateway Properties** dialog box:

a) Check the **Production mode** check box.
b) Check the **Auto start at system startup** check box.
c) Check the **Duplexed Peripheral Gateway** check box.
d) In the **PG Node Properties ID** pane, from the **ID** drop-down list, select the appropriate PG.
e) Select the appropriate side (**Side A** or **Side B**).
f) In the **Client Type Selection** pane, add **MediaRouting** to the **Selected types**.
g) Click **Next**.

Add Multichannel PIM to 2000 Agent Deployment

Caution Before performing the step to enable the secured connection between the components, ensure that the security certificate management process is completed.

Procedure

Step 1 In the **Peripheral Gateway Component Properties** window, click **Add**.

Step 2 From the **Client Type** drop-down list, select **Media Routing**.

Step 3 From the **Available PIMS** list, select **MR PIM1**, then click **OK**.

Step 4 In the **Configuration** dialog box, check the **Enabled** check box.

Step 5 In the **Peripheral name** field, enter the peripheral name.

Step 6 In the **Peripheral ID** field, enter the logical controller ID of the Unified CCE component you are adding. The following are the names by which the Unified CCE components are represented in the database. Refer *Peripheral Gateway* page in CCE Admin to get the peripheral ID of the corresponding PIM.

- Name of Outbound is *Outbound*
- Name of ECE is *Multichannel*
- Name of CCP is *Multichannel2*
- Name of THIRD_PARTY_MULTICHANNEL is *MutliChannel3*
- Name of Digital Routing is *DigitalRouting*

Example:

If you are adding ECE, find the component of the name *Multichannel* in the database. Enter the logical controller ID of that component in the **Peripheral ID** field.

Step 7 In the **Application Hostname (1)** field, enter the hostname or the IP address of the ECE services server.

Step 8 In the **Application connection port (1)** field, enter the port number.

Note Use the port number that is on the ECE services server that PIM uses to communicate with the application. The default port is 38001.

Step 9 In the **Application Hostname (2)** field, leave the field blank.

Step 10 In the **Application connection port (2)** field, leave the field blank.

Step 11 In the **Heartbeat interval (sec)** field, enter `5`.

Step 12 In the **Reconnect interval (sec)** field, enter `10`.

Step 13 Check the **Enable Secured Connection** option.

This establishes a secured connection between the MR PIM and the application server.

Ensure that you provide the correct information in the application hostname(1) and Application Connection Port(1) fields.

Step 14 Click **OK**.

Add Outbound PIM

Caution Before you enable secured connection between the components, ensure to complete the security certificate management process.

For more information, see 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.

Procedure

Step 1 In the **Peripheral Gateway Component Properties** window, click **Add**.

Step 2 From the **Client Type** drop-down list, select **Media Routing**.

Step 3 From the **Available PIMS** list, select **MR PIM2**, then click **OK**.

Step 4 In the **Configuration** dialog box, check the **Enabled** check box.

Step 5 In the **Peripheral name** field, enter the peripheral name.

Step 6 In the **Peripheral ID** field, enter the logical controller ID.

Step 7 In the **Application Hostname (1)** field, enter the hostname or the IP address of Agent PG machine of Side A.

Step 8 In the **Application connection port (1)** field, retain the default value.

Step 9 In the **Application Hostname (2)** field, enter the hostname or the IP address of Agent PG machine of Side B.

Step 10 In the **Application connection port (2)** field, retain the default value.

Step 11 In the **Heartbeat interval (sec)** field, enter `5`.

Step 12 In the **Reconnect interval (sec)** field, enter `10`.

Step 13 Check the **Enable Secured Connection** option.

This establishes a secured connection between MR PIM and Application Server.

Ensure that you provide the correct information in the Application Hostname(1) and Application Connection Port(1) fields.

Step 14 Click **OK**.

Configure CTI Server

Complete the following procedure to configure the CTI server for Side A and Side B.

Caution Before enabling secured connection between the components, ensure that the security certificate management process is completed. For more information on security certificate management, see *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.

Procedure

Step 1 Select **Start > All Programs > Cisco Unified CCE Tools > Peripheral Gateway Setup**.

Step 2 In the Instance Components pane of the Components Setup dialog box 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) Choose **CG1** for Agent PG1 and choose **CG2** for Agent PG2.
e) Enter the system ID number corresponding to the Agent PG.
For example: Enter 1 for Agent PG1 and 2 for Agent PG2.
f) Click the appropriate side (Side A or Side B).
g) Click **Next**.

Step 4 In the Server Component Properties dialog box, configure as follows:

a) To enable secured connection, check the **Enable Secure-Only Mode** checkbox.
b) Enter the appropriate port number in the Client Connection Port Number field. The default port is 42027 for non-secured connection and 42030 for secured connection. Ensure that the CTI server port matches with the CTI Gateway (CG) configuration.

Step 5 Click **Next**.

Step 6 In the Network Interface Properties dialog box, enter the private interfaces.

Step 7 Enter the public (visible) interfaces and the CG visible interfaces, and click **Next**.

Step 8 Under the Check Setup Information page, verify all the settings, and click **Next**.

Step 9 In the Setup Completed dialog box, click **Finish**.

Step 10 Click **Exit Setup**.

Note Do not start Unified CCE /CC Node Manager until all Unified CCE components are installed.

Upgrade Cisco JTAPI Client on PG

If you upgrade Unified Communications Manager (Unified CM) in the contact center, also upgrade the JTAPI client that resides on the PG. To upgrade the JTAPI client, uninstall the old version of the client, restart the server, and reinstall a new version. You install the JTAPI client using the Unified Communications Manager Administration application.

To install the JTAPI client for the Unified CM release that you have upgraded to, see the Install Cisco JTAPI Client on PG, on page 77 topic.

Before you begin

Before you perform this procedure, you must:

- Uninstall the old JTAPI client from the Unified Communications Manager PG
- Restart the PG server.

Verify Cisco Diagnostic Framework Portico

Do this for the Unified CCE machines.

Procedure

Step 1 Open the command prompt and enter **cd C:**.

Step 2 Enter **cd icm\serviceability\diagnostics\bin** and press **Enter**.

Step 3 Enter **DiagFwCertMgr /task:CreateAndBindCert /port:7890** and press **Enter**.

Step 4 Go to **Start -> Run** and enter **services.msc** to open the Services tool. Make sure the Cisco Diagnostic Framework service is running. If it is not running start it.

Step 5 Open Diagnostic Framework Portico: **Start** > **Programs** > **Cisco Unified CCE Tools** > **Diagnostic Framework Portico**. Then make sure you can log in to the Diagnostic Framework Portico using domain user credentials.

Cisco SNMP Setup

Complete the following procedures to configure Cisco SNMP:

- Add Cisco SNMP Agent Management Snap-In, on page 45
- Save Cisco SNMP Agent Management Snap-In View, on page 46
- Set Up Community Names for SNMP V1 and V2c , on page 46
- Set Up SNMP User Names for SNMP V3 , on page 46
- Set Up SNMP Trap Destinations , on page 47
- Set Up SNMP Syslog Destinations , on page 47

Add Cisco SNMP Agent Management Snap-In

You can configure Cisco SNMP Agent Management settings using a Windows Management Console snap-in.

Complete the following procedure to add the snap-in and change Cisco SNMP Management settings.

Procedure

Step 1 From the Start menu, enter **mmc.exe /32**.

Step 2 From the Console, choose **File** > **Add or Remove Snap-ins**.

Step 3 In the Add or Remove Snap-ins dialog box, choose **Cisco SNMP Agent Management** from the list of available snap-ins. Click **Add**.

Step 4 In the Selected snap-ins pane, double-click **Cisco SNMP Agent Management**.

Step 5 In the Extentions for Cisco SNMP Agent Management dialog box, select **Always enable all available extentions**. Click **OK**.

Step 6 In the Add/Remove Snap-in window, click **OK**. The Cisco SNMP Agent Management Snap-in is now loaded into the console.

Save Cisco SNMP Agent Management Snap-In View

After you load the Cisco SNMP Agent Management MMC snap-in, you can save the console view to a file with a .MSC file extension. You can launch the file directly from Administrative Tools.

Complete the following procedure to save the Cisco SNMP Agent Management snap-in view.

Procedure

Step 1 Choose **File** > **Save**.

Step 2 In the Filename field, enter **Cisco SNMP Agent Management**.

Step 3 In the Save As type field, choose a file name to map to the administrative tools such as **Microsoft Management Console Files(*.msc)**.

Step 4 Click **Save**.

Set Up Community Names for SNMP V1 and V2c

If you use SNMP v1 or v2c you must configure a community name so that Network Management Systems (NMSs) can access the data your server provides. Use SNMP community names to authenticate data exchange of SNMP information. An NMS can exchange SNMP information only with servers that use the same community name.

Complete the following procedure to configure the community name for SNMP v1 and v2c.

Before you begin

Ensure Cisco SNMP is added and saved using the procedures Add Cisco SNMP Agent Management Snap-In, on page 45 and Save Cisco SNMP Agent Management Snap-In View, on page 46.

Procedure

Step 1 Choose **Start** > **All Programs** > **Administrative tools** > **Cisco SNMP Agent Management**.

Step 2 Right-click **Cisco SNMP Agent Management** and choose **Run as administrator**.

Step 3 The Cisco SNMP Agent Management screen lists some of the configurations that require SNMP for traps and system logs.

Step 4 Right-click **Community Names (SNMP v1/v2c)** and choose **Properties**.

Step 5 In the Community Names (SNMP v1/v2c) Properties dialog box, click **Add New Community**.

Step 6 In the Community Name field, enter a community name.

Step 7 In the Host Address List, enter the host IP address.

Step 8 Click **Apply** and click **OK**.

Set Up SNMP User Names for SNMP V3

If you use SNMP v3 you must configure a user name so that NMSs can access the data your server provides.

Complete the following procedure to configure a user name for SNMP v3.

Before you begin

Ensure Cisco SNMP is added and saved using the procedures Add Cisco SNMP Agent Management Snap-In, on page 45 and Save Cisco SNMP Agent Management Snap-In View, on page 46.

Procedure

Step 1 From the Console Root, choose **Cisco SNMP Agent Management** > **User Names (SNMP v3)** > **Properties**.

Step 2 Click **Add New User**.

Step 3 In the User Name field, enter a username.

Step 4 Click **Save**.

Step 5 The username appears in the Configured Users pane at the top of the dialog box.

Step 6 Click **Apply** and click **OK**.

Set Up SNMP Trap Destinations

You can configure SNMP Trap Destinations for SNMP v1, SNMP v2c, and SNMP v3. A Trap is a notification that the SNMP agent uses to inform the NMS of a certain event.

Complete the following procedure to configure the trap destinations.

Before you begin

Ensure Cisco SNMP is added and saved using the procedures Add Cisco SNMP Agent Management Snap-In, on page 45 and Save Cisco SNMP Agent Management Snap-In View, on page 46.

Procedure

Step 1 From the Console Root, choose **Cisco SNMP Agent Management** > **Trap Destinations** > **Properties**.

Step 2 Click **Add Trap Entity**.

Step 3 Click the SNMP version that your NMS uses.

Step 4 In the Trap Entity Name field, enter a name for the trap entity.

Step 5 Choose the User Name/Community Name that you want to associate with this trap. This list is auto-populated with existing configured users/community names.

Step 6 Enter one or more IP addresses in the IP Address entry field. Click **Insert** to define the destinations for the traps.

Step 7 Click **Apply** and click **Save** to save the new trap destination.

The trap entity name appears in the Trap Entities section at the top of the dialog box.

Step 8 Click **OK**.

Set Up SNMP Syslog Destinations

You can configure Syslog destinations for SNMP from the Cisco SNMP Agent Management Snap-in.

Complete the following procedure to configure Syslog destinations.

Procedure

Step 1 From the Console Root, choose **Cisco SNMP Agent Management** > **Syslog Destinations** > **Properties**.
Step 2 Choose an Instance from the list box.
Step 3 Check **Enable Feed**.
Step 4 Enter an IP address or host name in the Collector Address field.
Step 5 Click **Save**.
Step 6 Click **OK** and restart the logger.

Start Unified CCE Services

The Unified CCE components run as a Windows service on the host computer. You can start, stop, or cycle these services from the **Unified CCE Service Control tool** on the desktop.

Note This procedure is required for activating Unified CCE services. However, you must postpone this task until you install Unified CCE components in all virtual machines given in the deployment model.

Procedure

Step 1 On eachUnified CCE Server machine, open **Unified CCE Service Control**.
Step 2 Start the **Unified CCE component** services.

Configure Unified CVP

This section explains the procedures to configure Unified CVP.

Sequence	Task	Done?
1	Configure Unified CVP Server, on page 48	
2	Configure Unified CVP Reporting Server, on page 52	
3	Configure Cisco Unified CVP Operations Console, on page 57	

Configure Unified CVP Server

This section explains the procedures to configure Unified CVP Server.

Sequence	Task	Done?
1	Validate Network Card, on page 49	
2	Setup Unified CVP Media Server IIS, on page 49	
3	Setup FTP Server, on page 50	

Validate Network Card

Procedure

Step 1 Select **Start** and right-click **Network.**

Step 2 Select **Properties**. Then select **Change Adapter Settings**.

Step 3 Right-click **Local Area Connection** and select **Properties.**

Step 4 Uncheck **Internet Protocol Version 6 (TCP/IPV6)**.

Step 5 Check **Internet Protocol Version 4** and select **Properties**.

Step 6 Confirm the data for Visible IP addresses, Subnet mask, Default gateway and Preferred and alternate DNS servers.

Step 7 Click **OK**.

Setup Unified CVP Media Server IIS

Procedure

Step 1 Navigate to **Start** > **Administrative Tools**.

Step 2 Choose **Server Manager** option navigate to **Manage** > **Add Roles and Features**.

Step 3 Goto **Installation Type** tab, choose **Role based or featue based installation** option and click **Next**.

Step 4 On **Server Selection** window, select server from the list and click **Next**.

Step 5 Check **Web Sever(IIS)** check box to enable IIS and click **Next**.

Step 6 No additional features are necessary to install Web Adaptor, click **Next**.
Displays **Web Server Role(IIS)** tab.

Step 7 Click **Next**.
Displays **Select Role Services** tab.

Step 8 Ensure that the web server components listed below are enabled.

- Web Server
  - Common HTTP Features
    - Default Document
    - Static Content
  - Security

- Request Filtering
- Basic Authentication
- Windows Authentication

- Application development
  - .NET Extensibility 4.6
  - ASP.NET 4.6
  - ISAPI Extensions
  - ISAPI Filters

- Management Tools
  - IIS Management Console
  - IIS Management Compatibility
    - IIS6 Metabase Compatibility
  - IIS Management Scripts and tools
  - Management Service

Step 9 Click **Next**.

Step 10 Ensure that your settings are correct and click **Install**.

Step 11 After installation click **Close**.

Setup FTP Server

Install FTP Server

Procedure

Step 1 Select **Start** > **Administrative Tools**.

Step 2 Select **Server Manager** and click **Manage**.

Step 3 Select **Add Roles and Features** and click **Next**.

Step 4 In the **Installation Type** tab, select **Role-based or feature-based Installation** and click **Next**.

Step 5 Select required server from the list and click **Next**.

Step 6 On the **Server Roles** page, expand **Web Server (IIS)**.

Step 7 Check **FTP Server** and click **Next**.

Step 8 On the **Features** page, click **Next**.

Step 9 On the **Configuration** page, click **Install**.

Enable FTP Server

Procedure

Step 1 Goto **Start** > **Administrative Tools**.

Step 2 Choose **Sever Manager** and click **IIS**.

Step 3 Right-click on the server that you want to enable FTP server and choose **Internet Information Services (IIS) Manager** option from submenu.

Step 4 Goto **Connections** panel:

a) Expand CVP server that you want to add FTP site.
b) Right-click on **Site** and choose **Add FTP Site** option from submenu.

Step 5 Enter **FTP Site Name**.

Step 6 Browse `C:\Inetpub\wwwroot` in **Physical Path** field and click **Next**.

Step 7 Choose **IP Address** of CVP from the drop-down list.

Step 8 Enter **Port** number.

Step 9 Check **No SSL** check box and click **Next**.

Step 10 Check **Anonymus** and **Basic** check boxes in **Authentication** panel.

Step 11 Choose **All Users** from **Allow Access To** drop-down list.

Step 12 Check **Read** and **Write** check boxes and click **Finish**.

Configure Basic Settings for FTP Server

Procedure

Step 1 Navigate to **FTP server** that you have created in **Connections** tab.

Step 2 Goto **Actions** tab and click **Basic Settings**.

Step 3 Click **Connect As**.

Step 4 Choose **Application User (pass-through authentication)** option and click **OK**.

Step 5 Click **OK** in **Edit Site** window.

Configure Unified CVP Reporting Server

Note

- There is one Unified CVP Reporting Server for 2000 agent deployment.
- There are two Unified CVP Reporting Servers for other agent deployments.

This table lists the procedures to configure Unified CVP reporting server.

Sequence	Task	Done ?
1	Validate Network Card, on page 49	?
2	Allocate a Second Virtual Hard Drive, on page 26	?
3	Unified CVP Reporting Users, on page 52	?
4	Create Data Source for Cisco Unified CVP Report Data, on page 54	?

Unified CVP Reporting Users

Create Reporting Users

Who can create a user:

- Initially, the System Application User who is the default Superuser.
- Eventually, any Superuser.

Unified CVP reporting users can sign in to Unified Intelligence Center only if they exist in the Administration console as Superusers or if Active Directory (AD) is configured in the Unified Intelligence Center Administration console for their domain:

- Superusers who are added are considered to be IP Multimedia Subsystem (IMS) users.
- Users who are authenticated through Active Directory are considered to be Lightweight Directory Access Protocol (LDAP) users.

Both IMS users and LDAP users can log in to Unified Intelligence Center reporting and are restricted to the limited Login User role until the Unified Intelligence Center reporting security administrator gives them additional roles and flags them as active users.

Create Superusers

Procedure

Step 1 Log in to the Cisco Unified Intelligence Center Administration Console `(https://<HOST ADDRESS>/oamp)`.

Step 2 Navigate to **Admin User Management > Admin User Management** to open the Users page.

Step 3 Click **Add New** to add and configure a new user or click an existing username to edit the configuration for that user.

This page has three tabs: General, Credentials, and Policy. For information about completing these tabs, see *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html or the Administration console online help.

Step 4 Click **Save**.

Set Up Active Directory Server for LDAP Users

Configure the Active Directory tab in the Cisco Unified Intelligence Center Administration console so that Unified CVP reporting users can log in to the Unified Intelligence Center reporting application with the user name and password that is defined in their domain.

Procedure

Step 1 In the Cisco Unified Intelligence Center Administration application, navigate to **Cluster Configuration** > **Reporting Configuration** and select the Active Directory tab.

Step 2 Complete all fields on this page, referring to the online help for guidance.

Step 3 Click **Test Connection**.

Step 4 When the connection is confirmed, click **Save**.

Sign In to Cisco Unified Intelligence Center Reporting Interface

Who can sign in to the Unified Intelligence Center reporting interface:

- Initially, the System Application User who is the default Superuser.
- Eventually, any Unified CVP user who was created in the Administration Console as an IMS superuser or an LDAP user.

Perform the following procedure to sign in to the Unified Intelligence Center reporting interface.

Procedure

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

Step 2 Navigate to **Control Center** > **Device Control**.

Step 3 Click on the name of the Member node you want to access. This opens the Cisco Unified Intelligence Center login page for that member.

Step 4 Enter your user ID and password. The Overview page appears.

Step 5

What to do next

If you have CVP Reporting as an on-box VM or an external server, refer to sections in the Configure Unified Intelligence Center section for information on creating the data source for Unified CVP and importing CVP report templates.

Create Report Template

Follow these steps to create a Unified CVP Report Template from the Unified Intelligence Center at *https://<hostname of CUICPublisher>:8444/cuic*.

Sequence	Task	Done?
1	Create Data Source for Cisco Unified CVP Report Data, on page 54	
2	Obtain Cisco Unified CVP Report Templates , on page 55	
3	Import Reports, on page 55	

Create Data Source for Cisco Unified CVP Report Data

You can create or edit a data source only if you are assigned with a System Configuration Administrator role.

To create a data source, perform the following steps:

Procedure

Step 1 In the left navigation pane, choose **Configure** > **Data Sources**.

Step 2 In the **Data Sources** window, click **New**.

Step 3 In the **Create Data Source** dialog box, enter the datasource **Name**, **Description**, and select the **Data Source Type**.

Step 4 Click **Next**.

Step 5 In the data source details page, enter the following (Primary Node tab):

Field	Description
Host Settings	
Datasource Host	The hostname or IP address of the target data source.
Port	The port number that allows Unified Intelligence Center to communicate with the database. **Note** The port number is a mandatory field only for the Informix database.
Database Name	Enter the name of the database.
Instance	Enter the instance of the database. **Note** The name of the database instance is a required field only for Informix databases.
Time zone	Select the time zone that the database is located in.
Authentication Settings	
Database User ID	The user ID required to access the database.
Password	The password for the user ID required to access the database.

Field	Description
Charset	The character set that is used by the database.
Max Pool Size	The maximum pool size. **Note** Value ranges from 5 to 200. The default Max Pool Size value is 100 and is common for both the primary and secondary data source tabs.

Step 6 Click **Test Connection** to ensure that the database is accessible and the credentials provided are correct.

Step 7 Click the **Secondary Node** tab to configure a failover for the data source.

Step 8 Check the **Enable Failover** check box to configure a failover for the data source.

Step 9 Enter the required details for the failover data source. (Refer step 5)

Step 10 Click **Save**.

Obtain Cisco Unified CVP Report Templates

Who can obtain import Unified CVP report templates: any user in your organization.

The Unified CVP reporting template XML files are installed with Unified CVP. Locate them and copy them to a Cisco Unified Intelligence Center client workstation.

Perform the following procedure to obtain import Unified CVP report templates.

Procedure

Step 1 In the Unified CVP server, locate the Unified CVP template files. These are XML files that reside on the reporting server in %CVP_HOME%\CVP_Reporting_Templates. You can also find them in the Installation directory \Downloads and Samples\Reporting Templates.

Step 2 Choose the files and copy them to the client computer from where you can launch the Unified Intelligence Center Reporting web application.

Import Reports

You can import the Unified Intelligence Center report, which is in either .xml or .zip file format.

The imported report retrieves data for the following entities:

- Report
- Report Definition
- Value Lists
- Views
- Thresholds
- Drilldowns
- Template Help

Note Each report template help folder has a size limit of 3 MB. If the folder size exceeds this limit, the system does not load the help content.

Note You cannot import Report Filters and Collections.

Ensure that the data source is used to import the Report Definition is configured in Unified Intelligence Center. Also, ensure that data source is used by any value list that is defined in Unified Intelligence Center, if the report definition has any value list defined.

To import reports, perform the following steps:

Procedure

Step 1 In the left navigation pane, choose **Reports**.

Step 2 In the **Reports** listing page, click **Import**.

Step 3 Click **Browse** to select the file (.xml or .zip format) to be imported.

Note Maximum file size for .zip file format is 60 MB and for .xml file format is 3 MB.

Step 4 Select the required file and click **Open**.

Step 5 Select the file location from the **Save to Folder** list to save the file.

Step 6 Click **Upload**.
Once the file is successfully uploaded, the table gets populated with the corresponding report template, current available version, and incoming version of the files being imported.

Step 7 Select a Data Source for the Report Definition only if the Report Definition for the report being imported is not defined in Unified Intelligence Center.

Step 8 Select a Data Source for the Value List that is defined in the Report Definition.

Note Selection of a Data Source for the Value List is mandatory:

- If the Value List does not use the same Data Source as the Report Definition.
- For Real Time Streaming Report Definitions.

Step 9 Select the files to import or overwrite.

- Overwrite—If the report being imported exists in the Unified Intelligence Center.
- Import—If the report being imported is the new set of report files.

Step 10 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.
- Importing manually edited XMLs is not supported.

Configure Cisco Unified CVP Operations Console

Sequence	Task	Done?
1	Validate Network Card, on page 49	
2	Enable Unified CVP Operations Console, on page 57	
3	Configure Unified CVP Call Server Component, on page 58	
4	Configure Unified CVP Server Component, on page 59	
5	Configure Unified CVP Reporting Server, on page 59	
6	Configure Unified CVP Media Server, on page 60	
7	Install Unified CVP licenses, on page 60	
8	Configure Gateways, on page 61	
9	Add Unified CCE Devices, on page 62	
10	Add Unified Communications Manager Devices, on page 62	
11	Add Unified Intelligence Center Devices , on page 63	
12	Transfer Scripts and Media Files, on page 61	
13	Configure SNMP, on page 61	
14	Configure SIP Server Group, on page 63	
15	Configure Dialed Number Patterns, on page 64	

Enable Unified CVP Operations Console

Complete the following procedure on the Unified CVP OAMP server to enable the Unified CVP Operations Console.

Procedure

Step 1 Go to **Start > Run** and type **services.msc**.

Step 2 Check that Cisco CVP OPSConsoleServer service is running. If it is not, right-click that service and click **Start**.

Step 3 Go to **Start > All Programs > Cisco Unified Customer Voice Portal > Operation Console** to open the Unified CVP OPSConsole page. If you are using Microsoft Internet Explorer, you will need to accept the self-signed certificate.

Configure Unified CVP Call Server Component

Note

- There is one Unified CVP server on Side A and one Unified CVP server on side B for the 500 agent deployment.
- There are two Unified CVP servers on Side A and two Unified CVP server on side B for the 1000 agent deployment.
- There are eight Unified CVP servers on Side A and eight Unified CVP server on side B for the 4000 agent deployment.

Procedure

Step 1 On the Unified CVP OAMP server, go to **Start** > **All Programs** > **Cisco Unified Customer Voice Portal**.

Step 2 Click **Operations Console** and log in.

Step 3 Navigate to **Device Management > Unified CVP Call Server**.

Step 4 Click **Add New**.

Step 5 On the General tab, enter the IP address and the hostname of the Cisco Unified CVP Server. Check **ICM**, **IVR**, and **SIP**. Click **Next**.

Step 6 Click the **ICM** tab. For each of the Cisco Unified CVP Call Servers, retain the default port of 5000 for the VRU Connection Port.

Step 7 Click the **SIP** tab:

a) In the Enable outbound proxy field, select **No**.
b) In the Use DNS SRV type query field, select **Yes**.
c) Check **Resolve SRV records locally**.

Step 8 Click the **Device Pool** tab. Make sure the default device pool is selected.

Step 9 (Optional) Click the **Infrastructure** tab. In the Configuration Syslog Settings pane, configure these fields as follows:

a) Enter the IP address or the hostname of the syslog server.

Example:

Prime server

b) Enter **514** for the port number of the syslog server.
c) Enter the name of the backup server to which the reporting server writes log messages.
d) In the Backup server port number field, enter the port number of the backup syslog server.

Step 10 Click **Save & Deploy**.

Step 11 Repeat this procedure for the remaining Unified CVP Servers.

Configure Unified CVP Server Component

Complete the following procedure to configure the VXML Server component for the Cisco Unified CVP Servers.

Procedure

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

Step 2 Click **Add New**.

Step 3 On the General tab, enter the IP address and the hostname of the Cisco Unified CVP Server.

Step 4 Configure the primary and backup CVP Call Servers.

Step 5 Click the **Configuration** tab. In the **Enable reporting for this CVP VXML Server** field, click **Yes** to optionally enable reporting. If you do not want to enable reporting, click **No**.

Step 6 Click the **Device Pool** tab. Make sure the default device pool is selected. If prompted to restart the primary and secondary call servers, click No. Do not restart at this time.

Step 7 Click **Save & Deploy**.

Step 8 Repeat this procedure for all CVP Servers.

Configure Unified CVP Reporting Server

Complete the following procedure to configure the Unified CVP Reporting Server component in the Operations Console.

Note To load balance to the CVP reporting server, there are 2 CVP reporting servers deployed, one on each side. When a customer has 2 reporting servers, the customer should configure CVP Reporting server Side A and associate all the side A CVP call servers, and for Side B reporting server, associate all the CVP call servers belongs to side B, this is because each CVP call server and each VXML server can be associated with only one reporting server. Be aware that the reports cannot span multiple Informix databases. Side A call servers reports only of side A reporting server and side B call servers reports only of side B reporting server.

If the customer chooses to have a single CVP reporting server, the customer should associate all the call servers to the single reporting server. During temporary database outages, messages are buffered to file and are inserted into the database after the database comes back on line. The amount of time that messages can be buffered depends on the system.

Procedure

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

Step 2 Click **Add New**.

Step 3 On the **General** tab, configure the following:

a) Enter the IP address.

b) Enter the hostname.

c) Select all associated Unified CVP Call Servers Available.

Step 4 Configure the following on the **Infrastructure** tab:

a) Accept the default Maximum Threads, Statistics Aggregation Interval, and Log File Properties settings.
b) Enter the IP address or the hostname of the Syslog server to which the reporting server sends syslog events.

Example:

Prime server

c) Enter **514** for the Syslog server port number.
d) Enter the IP address or the hostname of the optional Backup server to which the reporting server sends syslog events.
e) Enter the optional Backup server port number.

Step 5 Click **Save & Deploy**.

Step 6 Repeat Steps 1 through 5 for all CVP Reporting Servers.

Configure Unified CVP Media Server

Procedure

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

Step 2 Click **Add New**.

Step 3 On the **General** tab, configure the following.

a) Enter the IP address and the hostname of the Unified CVP server.
b) Check **FTP Enabled**.
c) Either Check **Anonymous Access** or enter the credentials.
d) Click **Test SignIn** to validate the FTP access.

Step 4 Click **Save**.

Step 5 Repeat Step 1 through 4 for all Media Servers.

Step 6 After you configure all Media Servers, click **Deploy**.

Step 7 Click **Deployment Status** to make sure that you applied the configuration.

Step 8 In the CVP Operations Console, navigate to **Device Management > Media Server**.

Step 9 Change Default Media Server from **None** to any one of the Unified CVP servers. Then click **Set**.

Step 10 Click **Deploy**.

Install Unified CVP licenses

Procedure

Step 1 Sign in to the **CVP Operations Console**.

Step 2 Choose **Bulk Administration** > **File Transfer** > **Licenses**.

Step 3 In the Select device type field, choose **All Unified CVP devices**.

Step 4 Browse and select the license file.

Step 5 Click **Transfer**.

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

Configure Gateways

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 Scripts and Media Files

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

Procedure

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

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

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

Step 4 Click **Default Gateway files**.

Step 5 Click **Transfer** and select **OK** at the popup window.

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

Configure SNMP

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**.

Add Unified CCE Devices

Procedure

Step 1 Log in to the **Unified CVP Operations Console**.
Step 2 Choose **Device Management** > **Unified ICM**.
Step 3 Click **Add New**.
Step 4 On the General tab, configure as follows:

a) Enter the IP address.
b) Enter the Hostname.
c) Check Enable Serviceability.
d) Enter the Username.
e) Enter the Password.
f) Confirm Password.
g) Accept the default port.

Step 5 Click **Save**.
Step 6 Repeat Steps 1 to 5 for all Unified CCE machines.

Add Unified Communications Manager Devices

Procedure

Step 1 Log in to the **CVP Operations Console**.
Step 2 Choose **Device Management** > **Unified CM**.
Step 3 Click **Add New**.
Step 4 On the General tab, configure as follows:

a) Enter the IP address.
b) Enter the Hostname.
c) Check Enable Synchronization.
d) Enter the Username.

e) Enter the Password.
f) Confirm Password.
g) Accept the default port.

Note For Small contact center deployment add the NAT IP address of the unified CM.

Step 5 Click **Save**.

Step 6 Repeat Steps 1 to 5 for all Unified Communications Manager Devices.

Add Unified Intelligence Center Devices

Procedure

Step 1 Log in to the **CVP Operations Console**.

Step 2 Navigate to the Cisco Unified Intelligence Center Device. Choose **Device Management** > **Unified IC**.

Step 3 Click **Add New**.

Step 4 On the General tab, configure as follows:

a) Enter the IP address.
b) Enter the Hostname.
c) Check Enable Serviceability.
d) Enter the Username.
e) Enter the Password.
f) Confirm Password.
g) Accept the default port.
h) Associate all the existing CVP Reporting Servers.

Step 5 Click **Save**.

Configure SIP Server Group

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 the Unified Communications Manager node.
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 SCC deployment as there is no direct SIP trunk created from Communications Manager to CVP in SCC model.

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 each gateway.
d) Click **Add**.
e) Repeat Steps c and d for each gateway. Click **Save**.

Add all VXML gateways as appropriate for deployment and branches. 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**.

Note In the small contact center agent deployment, CUBE(SP) does not support FQDN configuration, therefore, you cannot create SIP server group pointing to CUBE(SP) for each sub customer.

Note
- In the small contact center agent deployment, CUBE(SP) does not support FQDN configuration, therefore, you cannot create SIP server group pointing to CUBE(SP) for each sub customer.
- In 12000 and 24000 agent deployment model, each CUCM cluster should have one SIP Server group with their subscriber nodes.

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**.
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**.
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**.
The agent extension pattern for the sub customer in SCC model. For example, enter 500* where the range agent extensions is 5001 to 500999.	Agent Device Label for the sub customer in the SCC model.	Check Enable Local Static Route. In IP Address/Hostname/Server Group field provide the signaling IP address and port of the CVP adjacency in CUBE(SP) in the format:< IP Address>:<Port number> For each sub customer a unique port must be configured. Check Enable RNA Timeout for Outbound Calls. The timeout is 15 seconds.

Note In 12000 and 24000 agent deployment model, each CUCM cluster should have separate Dialed number Pattern with their agent extension range.

Configure Cisco IOS Enterprise Voice Gateway

Complete the following procedure to configure the Cisco IOS Voice Gateway. Instructions are applicable to both TDM and Cisco UBE Voice gateways, unless otherwise noted.

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

```
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
     no ip address trusted authenticate
     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
 no ip address trusted authenticate
 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 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
```

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 CVP1, 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 70023 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 CVP1, 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 1 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 <gw70mtp>
     associate profile 1 register <gw70conf>
     associate profile 3 register <gw70xcode>

# 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

# Note: Universal transcoder is only needed for cases where you engage the G.729 caller to
G.729 only agent with IVR in middle and performs any supplementary services or use features
like whisper announcement or agent greeting.
```

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 # CVP1A
     rai target ipv4:###.###.###.### resource-group1 # CVP2A
     rai target ipv4:###.###.###.### resource-group1 # CVP1B
     rai target ipv4:###.###.###.### resource-group1 # CVP2B
     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
```

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
sip
     rel1xx disable
     header-passing
     options-ping 60
     midcall-signaling passthru
```

Step 2 Configure default Unified CVP services:

```
#Default 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
```

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
ivr asr-server rtsp://asr-en-us/recognizer
ivr tts-server rtsp://tts-en-us/synthesizer
rtsp client timeout connect 10
rtsp client timeout message 10
mrcp client timeout connect 10
mrcp client timeout message 10
mrcp client rtpsetup enable
vxml tree memory 500
vxml audioerror
vxml version 2.0
```

Step 5 Configure primary and secondary media servers:

```
#Configure the media servers where
# the primary matches the default media server defined in OAMP.
# the secondary is located on the opposite side of the primary.

ip host mediaserver ###.###.###.###          # IP Address for primary media server.
ip host mediaserver-backup ###.###.###.###   # IP Address for secondary media server.
```

Step 6 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 7 Configure ASR TTS:

```
#Configure primary server
ip host asr-en-us <ASR server ip>
ip host tts-en-us <TTS server hostname>
voice class uri TTS sip
pattern tts@<TTS server ip>
voice class uri ASR sip
pattern asr@<ASR server hostname>
ivr asr-server sip:asr@<ASR server hostname*>
ivr tts-server sip:tts@<TTS server hostname*>

dial-peer voice 5 voip
     description FOR ASR calls
     preference1
     session protocol sipv2
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     session target ipv4:<ASR server IP>
     destination uri ASR
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad

dial-peer voice 6 voip
     description FOR TTS calls
     preference1
     session protocol sipv2
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     session target ipv4:<TTS server IP>
     destination uri TTS
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad

#Configure backup server
dial-peer voice 7 voip
     destination uri ASR
     session target ipv4:<ASR backup server IP>
     session protocol sipv2
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry
     2dtmf-relay rtp-nte
     codec g711ulaw
     preference 2
     no vad

dial-peer voice 8 voip
     destination uri TTS
     session target ipv4:<TTS backup server IP>
     session protocol sipv2
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry
     2dtmf-relay rtp-nte
     codec g711ulaw
     preference 2
     no vad
```

Step 8 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 Unified Communications Manager

Follow this sequence of tasks to configure Unified Communications Manager:

Sequence	Task	Done?
1	Configure Unified Communications Manager Publisher, on page 72	
2	Configure Unified Communications Manager Subscriber, on page 73	
3	Install VMware Tools for Windows, on page 82	
4	Unified Communications Manager License, on page 74	
5	Activate Services , on page 75	
6	Validate Clusterwide Domain Configuration, on page 76	
7	Upgrade Cisco JTAPI Client on PG, on page 44	
8	Configure SNMP, on page 106	

Configure Unified Communications Manager Publisher

You must customize the Unified Communications Manager publisher before you customize the subscribers.

Before you begin

Ensure that the Virtual Machine device status shows **Connect at Power On** checked for the Network adapter and Floppy drive.

Procedure

Step 1 Power on the Publisher. This begins the installation based on the information in the .flp file.The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the Publisher machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power on** for the floppy drive.

Note During the customization of the publisher/primary, the username and the password are modified as follows. The customer should change the password.

- Default Password for OS Administrator: `c1sco@123`
- Application UserName: `Administrator`
- Default Password for Application User: `c1sco@123`
- Sftp password: `c1sco@123`
- IPSec password: `c1sco@123`

Configure Unified Communications Manager Subscriber

Launch Unified Communications Manager Publisher to Add the Subscriber

To add the subscriber, you must launch the publisher node.

Procedure

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

Step 2 Enter the username and password and login to the Unified Communications Manager.

Step 3 Select **System** > **Server** > **Add New**.

Step 4 On the Add a Server page, choose **CUCM Voice/Video** for the server type. Click **Next**.

Step 5 On the Server Information page, enter the IP address of the first subscriber.

Step 6 Click **Save**.

Step 7 Repeat Steps 3 - 6 for the second subscriber.

Configure Subscriber

Before you begin

Ensure that the Virtual Machine device status is **Connect at Power On** checked for the Network adapter and Floppy drive

Procedure

Step 1 Power on the Subscriber.
This begins the installation based on the information in the .flp file. The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the CUCM Secondary machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power** on for the floppy drive.

Note During the customization of the subscriber node, the username and the password are modified as follows. The customer should change the password.

- Default Password for OS Administrator: **c1sco@123**
- Application UserName: **Administrator**
- Default Password for Application User: **c1sco@123**
- Sftp password: **c1sco@123**
- IPSec password: **c1sco@123**

Unified Communications Manager License

To configure the Unified Communications Manager license, first add a product instance, then generate and register the license, and then install the license.

Upgrade Unified Communications Manager License

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**.

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

Complete the following procedure to install a license.

Procedure

Step 1 Unzip the license file from the email message.

Step 2 Navigate to **License Management > Licenses**.

Step 3 Under Other Fulfillment Options, choose **Fulfill Licenses from File**.

Step 4 Browse for the license file and click **Install**.

Step 5 Navigate to the **Monitoring > License Usage** page to verify a successful installation.

Activate Services

Complete the following procedure to activate services.

Procedure

Step 1 Launch the Unified Communications Manager in a browser (http://<IP Address of CUCM Node>).

Step 2 From the Cisco Unified Serviceability drop-down list, choose **Tools** > **Service Activation**.

Step 3 From the Server drop-down list, choose the server on which you want to activate the services, and then click **Go**.

The window displays the service names and activation status of the services.

Step 4 Check the following services to activate:

a) Publisher:

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

b) Subscriber:

- Subscriber's for call processing
  - Cisco CallManager
  - Cisco IP Voice Media Streaming App
  - Cisco CTIManager
  - Cisco CTL Provider
  - Cisco AXL Web Service
- Subscriber's for TFTP and Music on Hold

  Note Enable TFTP Service in Publisher node for HCS for CC deployments that doesn't have a dedicated TFTP and MoH server.

  - Cisco TFTP
  - Cisco IP Voice Media Streaming App

Step 5 Click **Save**.

Note Activating Cisco CallManager, will automatically Activate CTIManager and Cisco Dialed Number Analyzer server. Click **OK** when prompted.

Validate Clusterwide Domain Configuration

This validation is required for running calls.

Procedure

Step 1 In the Cisco Unified CM Administration, navigate to **System > Enterprise Parameters**.

Step 2 Scroll down to **Clusterwide Domain Configuration**.

Cluster Fully Qualified Domain Name should match the Server Group name in the Unified CVP SIP Server Groups Configure SIP Server Group, on page 63.

Upgrade Cisco JTAPI Client on PG

If you upgrade Unified Communications Manager (Unified CM) in the contact center, also upgrade the JTAPI client that resides on the PG. To upgrade the JTAPI client, uninstall the old version of the client, restart the server, and reinstall a new version. You install the JTAPI client using the Unified Communications Manager Administration application.

To install the JTAPI client for the Unified CM release that you have upgraded to, see the Install Cisco JTAPI Client on PG, on page 77 topic.

Before you begin

Before you perform this procedure, you must:

- Uninstall the old JTAPI client from the Unified Communications Manager PG
- Restart the PG server.

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 78.

Before you begin

Before you install the JTAPI client, ensure that the previous version is uninstalled.

Procedure

Step 1 Open a browser window on the PG machine.

Step 2 Enter the URL for the Unified Communications Manager Administration utility: http://<*Unified Communications Manager machine name*>/ccmadmin.

Step 3 Enter the username and password that you created while installing and configuring the Unified Communications Manager.

Step 4 Choose **Application** > **Plugins**. Click **Find**.

Step 5 Click the link next to **Download Cisco JTAPI for Windows**.We recommend you to download the 64 bit version. However, if you have already downloaded the 32 bit version, you can proceed to step 7.

Download the JTAPI plugin file.

Step 6 Choose **Save** and save the plugin file to a location of your choice.

Step 7 Open the installer.

Step 8 In the Security Warning box, click **Yes** to install.

Step 9 Choose **Next** or **Continue** through the remaining Setup screens. Accept the default installation path.

Step 10 When prompted for the TFTP Server IP address, enter the CUCM IP address.

Step 11 Click **Finish**.

Step 12 Reboot the machine.

Install Cisco JTAPI Client on PG

Complete the following procedure only if you are installing JTAPI client to connect to Cisco Unified Communications Manager, Release 12.5 and above.

Before you begin

Before you install the JTAPI client, ensure that the previous version is uninstalled.

Procedure

Step 1 Open a browser window on the PG machine.

Step 2 Enter the URL for the Unified Communications Manager Administration utility: http://<*Unified Communications Manager machine name*>/ccmadmin.

Step 3 Enter the username and password that you created while installing and configuring the Unified Communications Manager.

Step 4 Choose **Application** > **Plugins**. Click **Find**.

Step 5 Click the link next to **Download Cisco JTAPI Client for Windows** 64 bit or **Download Cisco JTAPI Client for Windows** 32 bit.

Download the JTAPI plugin file.

Step 6 Choose **Save** and save the plugin file to a location of your choice.

Step 7 Unzip the JTAPI plugin zip file to the default location or a location of your choice.

There are two folders in the unzipped folder `CiscoJTAPIx64` and `CiscoJTAPIx32`.

Step 8 Run the `install64.bat` file in the `CiscoJTAPIx64` folder or run the `install32.bat` file in the `CiscoJTAPIx32` folder.

The default install path for JTAPI client is `C:\Program Files\JTAPITools`.

Step 9 To accept the default installation path, click Enter and proceed.

Follow the instructions. Click Enter whenever necessary as per the instructions.

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.

Configure Unified Intelligence Center Coresident Deployment

Sequence	Task	Done?
1	Configure Unified Intelligence Center Publisher, on page 79	
2	Configure Unified Intelligence Center Subscriber, on page 80	
3	Add Coresident (Cisco Unified Intelligence Center with Live Data and IdS) Machine Type to the System Inventory, on page 81	
4	Install VMware Tools for Windows, on page 82	
5	Configure Unified Intelligence Center Reporting, on page 82	
6	Configure Unified Intelligence Center Administration, on page 85	
7	Configure SNMP, on page 106	
8	Configure Live Data AW-Access, on page 87	
9	Configure Live Data Unified Intelligence Data Sources, on page 89	
10	Configure Live Data Reporting Interval, on page 89	
11	Configure Transport Layer Security , on page 90	
12	Import Reports, on page 55	
13	Add Certificate for HTTPS Gadget, on page 92	

Configure Unified Intelligence Center Publisher

You must customize the Cisco Unified Intelligence Center publisher before you customize the subscriber.

Before you begin

Ensure that the Virtual Machine device status is **Connect at Power On** checked for the Network adapter and Floppy drive

Procedure

Step 1 Power on the Publisher.

This begins the installation based on the information in the .flp file. The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the CUIC Primary machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power** on for the floppy drive.

Note During the customization of the publisher/primary, the username and the password are modified as follows. The customer should change the password.

- Default Password for OS Administrator: **c1sco@123**
- Application UserName: **Administrator**
- Default Password for Application User: **c1sco@123**
- Sftp password: **c1sco@123**
- IPSec password: **c1sco@123**

Configure Unified Intelligence Center Subscriber

Follow the below steps to for both CUIC with Live data and Live Data stand-alone deployment:

Note Ensure that the license is updated before adding the subscriber node.

Launch Publisher to Add Subscriber

Procedure

Step 1 Enter `http://<HOST ADDRESS>/oamp` URL in the browser, where *HOST ADDRESS* is the IP Address or 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 left panel, choose **Device Management** > **Device Configuaration**.

Step 4 Click **Add Member**.

Step 5 Enter hostname or IP address in **Name** field.

Step 6 Enter **Description** for the device.

Step 7 Click **Save**.

Configure Subscriber

Before you begin

Ensure that the Virtual Machine device status is **Connect at Power On** checked for the Network adapter and Floppy drive

Procedure

Step 1 Power on the Subscriber.
This begins the installation based on the information in the .flp file. The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the CUIC Secondary machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power** on for the floppy drive.

Note During the customization of the subscriber node, the username and the password are modified as follows. The customer should change the password.

- Default Password for OS Administrator: **c1sco@123**
- Application UserName: **Administrator**
- Default Password for Application User: **c1sco@123**
- Sftp password: **c1sco@123**
- IPSec password: **c1sco@123**

Add Coresident (Cisco Unified Intelligence Center with Live Data and IdS) Machine Type to the System Inventory

Procedure

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

Step 2 Add the new machine to the System Inventory:

a) Click **Add**.

The **Add Machine** popup window opens.

b) From the Type drop-down menu, select the following machine type:

CUIC_LD_IdS Publisher, for the coresident Unified Intelligence Center, Live Data, and Identity Service machine available in the 2000 agent reference design.

c) In the **Hostname** field, enter the FQDN, hostname, or IP address of the machine.

The system attempts to convert the value you enter to FQDN.

d) Enter the machine's Administration credentials.

e) Click **Save**.

The machine and its related Subscriber or Secondary machine are added to the System Inventory.

What to do next

If you remove a component from your deployment, delete it from your System Inventory. If you add the component again, or add more components, add those components to the System Inventory.

Install VMware Tools for Windows

Procedure

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

Step 2 Click the **Summary** tab.

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

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

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

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

a) To install/upgrade the VMware tools manually, select the **Interactive Tools Upgrade** option, and click **OK**. Follow the on-screen instructions to install/upgrade the VMware tools, and restart the virtual machine when prompted.

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

Configure Unified Intelligence Center Reporting

Complete the following procedures to configure Unified Intelligence Center Reporting.

Configure the SQL User Account

Complete the following procedure on both sides of the Unified CCE Historical database servers and the Unified CCE Real-time database servers to allow SQL authentication and to enable TCP/IP protocol and remote network connections.

Procedure

Step 1 Log in to the Unified CCE Historical and Real-time database servers in your deployment.

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

Step 3 Login using System Administrator login credentials.

Step 4 Expand **Security** tab. Right-click **Logins** and choose **New Login**.

Step 5 In **General** page, enter the following values:

a) Enter **Login Name**.

Example:

user

b) Choose **SQL Server authentication**.
c) Enter **Password** and re-enter the password to confirm.
d) Uncheck **Enforce password policy** check box.

Step 6 In **Server Roles** page, check the **public** check box.

Step 7 In **User Mapping** page, enter the following values:

a) Check the **Real-time database** and **Historical database** check boxes .
b) In the **Database role membership for** area, do the following:
   - For CUIC users, check the **db_datareader** and check box.
   - For Live Data users, check the following check boxes:
     - **db_datareader**
     - **db_datawriter**

Note The database role **public** is checked by default. This role is required for CUIC and Live Data users.

Step 8 Click **OK**.

Configure Unified Intelligence Center Data Sources

Complete the following procedure to allow Unified Intelligence Center to configure Unified CCE Historical Data source and Unified CCE Real-time Data source.

Note You can distribute the reporting load to several Unified CCE AW_HDS databases using the command line interface and conventional name resolution. If there is a need to direct a specific member node to a database host other than the one in configured on the data sources interface, you can use the "set cuic-properties host-to-ip" command to resolve the data source name differently on each node.

Procedure

Step 1 Login to Unified Intelligence Center portal as administrator (http://{hostname})

Step 2 From the navigation pane, click **Configure > Data Sources**.

Step 3 Choose the **Unified CCE Historical** Data Source. Click **Edit** from the ellipsis to open the Data Source page. In the Primary tab, enter the following values

a) In the Datasource Host field, enter the hostname/IP address of the primary historical database server **(AW-HDS-A1).**
b) In the **Port** field, enter 1433 which is a port used for SQL server database.
c) In the **Database Name** field, enter the primary historical database name.

d) In the **Instance** field, leave blank as it is optional for SQL server.
e) In the **Timezone** field, select the time zone for the data stored in the database.
f) In the **Database User ID** field, enter the SQL user account created earlier for CUIC to access the database.
g) In the **Password** and **Confirm Password** fields, enter the password for SQL user account.
h) In the **Charset** drop-down field, choose **ISO-8859-1** (Latin 1 encoding)
i) In the **Permissions** pane, accept the default values

Step 4 Click on the **Secondary** tab and enter the following values.

a) Check **Failover Enabled**
b) In the Datasource Host field, enter the hostname/IP address of the secondary historical database server **(AW-HDS-B1)**.
c) In the **Port** field, enter 1433 which is a port used for SQL server database.
d) In the **Database Name** field, enter the secondary historical database name.
e) In the **Instance** field, leave blank as it is optional for SQL server.
f) In the **Timezone** field, select the time zone for the data stored in the database.
g) In the **Database User ID** field, enter the SQL user account created earlier for CUIC to access the database.
h) In the **Password** and **Confirm Password** fields, enter the password for SQL user account.
i) In the **Charset** drop-down field, choose **ISO-8859-1** (Latin 1 encoding)
j) In the **Permissions** pane, accept the default values.

Step 5 Click **Test Connection** to ensure the data source is online and click **Save** .

Step 6 Choose the **Unified CCE Realtime** Data Source. Click **Edit** to open the **Data Source** > **Edit** page. In the Primary tab, enter the following values.

a) In the Datasource Host field, enter the hostname/IP address of the primary realtime database server **(AW-HDS-A2).**
b) In the **Port** field, enter 1433 which is a port used for SQL server database.
c) In the **Database Name** field, enter the primary realtime database name.
d) In the **Instance** field, leave blank as it is optional for SQL server.
e) In the **Timezone** field, select the time zone for the data stored in the database.
f) In the **Database User ID** field, enter the SQL user account created earlier for CUIC to access the database.
g) In the **Password** and **Confirm Password** fields, enter the password for SQL user account.
h) In the **Charset** drop-down field, choose **ISO-8859-1** (Latin 1 encoding)
i) In the **Permissions** pane, accept the default values

Step 7 Click on the **Secondary** tab and enter the following values.

a) Check **Failover Enabled**.
b) In the Datasource Host field, enter the hostname/IP address of the secondary realtime database server **(AW-HDS-B2)**.
c) In the **Port** field, enter 1433 which is a port used for SQL server database.
d) In the **Database Name** field, enter the secondary realtime database name.
e) In the **Instance** field, leave blank as it is optional for SQL server.
f) In the **Timezone** field, select the time zone for the data stored in the database.
g) In the **Database User ID** field, enter the SQL user account created earlier for CUIC to access the database.
h) In the **Password** and **Confirm Password** fields, enter the password for SQL user account.
i) In the **Charset** drop-down field, choose **ISO-8859-1** (Latin 1 encoding)
j) In the **Permissions** pane, accept the default values

Step 8 Click **Test Connection** to ensure the data source is online and click **Save**.

What to do next

After configuring Unified Intelligence Center, you can import stock templates using the Import functionality and customize the stock reports based on your requirements. The stock templates are designed to present Unified CCE /CC data. Navigate to User Guide for the Cisco Unified Intelligence Center Reporting Application. Under Chapter **Reports** see section **Stock Report Templates** to import Unified CCE Report templates.

Configure Unified Intelligence Center Administration

Complete the following procedure to 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) For Host Address for the Primary Active Directory Server, enter the IP address of the domain controller.
b) For Port, enter the port number for the domain controller.
c) Complete the **Manager Distinguished Name** fields that are required for the customer.
d) Enter and confirm the password with which the Manager accesses the domain controller.
e) For User Search Base, specify users and the domain name and any sub-domain names .
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 s*AMAccountName*, 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.

Unified Intelligence Center License and Sign-In

Sign In to Administration Console

Who can sign in to the administration console: The System Application User who is the default Superuser.

To upload the license, you must sign in to the Unified Intelligence Center Administration Console. This is the OAMP interface for Unified Intelligence Center. The first person who signs in to the Administration application must do so using the user ID and password that were defined for the System Application User during the installation. This user is the initial Superuser for Unified Intelligence Center Administration.

Procedure

Step 1 Enter this URL: `http://<HOST ADDRESS>/oamp`, where HOST ADDRESS is the IP address or hostname of your Controller node.

Step 2 Enter the System Application User ID and password that you defined during installation.

Upload License

Who can upload the license: The System Application User who is the default Superuser.

As soon as the System Application User signs in, the user must upload the license file. The file is uploaded to the Controller publisher node and, within a minute, is automatically replicated to all nodes in the cluster.

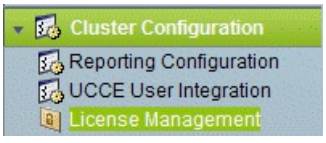
The partner must obtain a unique license and apply it to the imported Unified Intelligence Center servers at the customer site.

Procedure

Step 1 In Cisco Unified Intelligent Center Administration, choose **Cluster Configuration** > **License Management**.

to open the **License File Management** page.

Figure 3: License File Management



Step 2 Click **Browse**.

Step 3 Navigate to the location where the *.lic file was saved.

Step 4 Click **Apply License** to load the license.

A message appears indicating that the license file was uploaded successfully and will be distributed to other nodes (if any) in the cluster in approximately one minute.

Note The databases are polled once a minute for changes. The license replication is not immediate but occurs within a minute.

What to do next

Create Reporting Users, on page 52

Configure Live Data AW-Access

Live Data AW DB access commands allow you to configure and view Unified CCE AW DB (real-time distributor) access for Unified CCE Live Data Product Deployment Selection. You can also test the connection.

Procedure

Step 1 Log in to **CUIC Live Data Console** and run the following command:

set live-data aw-access primary *addr port db user pwd* [*test*]

set live-data aw-access secondary *addr port db user pwd* [*test*]

Table 7: Command Description

Command	Description	Example
addr	Specifies the hostname or IP address of the primary or secondary Unified CCE AW (Maximum 255 characters).	10.10.10.10 or AWmachinename.domain.com
port	Specifies the listening port of the database server (ranges 1-65535).	1433 db
db	Specifies the database name (maximum 128 characters).	inst_awdb
user	Specifies the login user (maximum 128 characters) For more information about creating user, see Configure the SQL User Account , on page 82	user
pwd	Specifies the login password (maximum 128 characters).	password
test	This parameter is optional. Tests the connection to the primary or secondary AW DB. Checks weather AW DB access for configured users and provides the results.	

Step 2 Run the following command to view the primary and secondary Unified CCE AW DB access information. Optional, test the connection from Live Data to each AW DB, check if configured user (on each node) has appropriate AW DB access:

show live-data aw-access primary *addr port db user pwd* [*test*]

show live-data aw-access secondary *addr port db user pwd* [*test*]

Configure Live Data Machine Services

Procedure

Step 1 Log in to **CUIC Live Data Console**.

Step 2 Run the below command to configure the latest information from Live Data with Machine Service table.

`set live-data machine-services` *awdb-user awdb-pwd*

Note This command is not valid for coresident deployments. If you have a coresident deployment, use the System Inventory in the Unified CCE Administration tool.

Table 8: Command Description

Command	Description	Example
awdb-user	Specifies the AW database domain user, who has write-access permission.	administrator@domain.com
awdb-pwd	Specifies the AW database user password.	password

Step 3 Run the below command to view Live Data entries in the **Machine Services** table:

`show live-data machine-services` *awdb-user awdb-pwd*

Note Enter FQDN host name in correct format. The machine (host) name must start with an alphanumeric character string with a maximum length of 32 characters. The machine name allows only characters such as period (.), underscore (_), dash (-), and alphanumeric characters. If the host name contains invalid characters or the name exceeds 32 characters, an error message appears.

Step 4 After you updated the host name of the Live Data Server, you must re-run the following commands, to update the Live Data machine services with the new host name.

`set live-data machine-services` *awdb-user awdb-pwd*

`set live-data cuic-datasource` *cuic-addr cuic-port cuic-user cuic-pwd*

Configure Live Data Unified Intelligence Data Sources

Before you begin

- Ensure that AW distributor and Cisco Unified Intelligence Center Publisher are in service
- Ensure that AW DB connection information is updated on the same node, where you want to configure Live Data CUIC data source
- Configure Live Data endpoints in the **Machine Service** table

Procedure

Step 1 Run the following command to configure the data source of Live Data in Cisco Unified Intelligence Center:

`set live-data cuic-datasource` *cuic-addr cuic-port cuic-user cuic-pwd*

Table 9: Command Description

Command	Description	Example
cuic-addr	Specifies the Cisco Unified Intelligence Center publisher node's Fully Qualified Domain Name (FQDN).	10.10.10.10 or CUIC + LiveDatamachinename.domain.com **Important** Given node should be in service.
cuic-port	Specifies the Cisco Unified Intelligence Center REST API port. Typically this port is 8444.	
cuic-user	Specifies the user name to use for authentication with Cisco Unified Intelligence Center. By default, Cisco Unified Intelligence Center requires that you specify **CUIC** as the domain with the user name.	`CUIC\administrator`
cuic-pwd	Specifies the password to use for authentication with Cisco Unified Intelligence Center.	password

Step 2 Run the following command to display Data Source:

`show live-data cuic-datasource` *cuic-addr cuic-port cuic-user cuic-pwd*

Configure Live Data Reporting Interval

Procedure

Step 1 Log in to **CUIC Live Data Console**.

Step 2 Run the following command to set Live Data reporting interval in minutes format:

```
set live-data reporting-interval reporting-interval-in-minutes
```

Table 10: Command Description

Command	Description	Example
reporting-interval-in-minutes	Specifies the reporting interval in minutes format. The valid values are 5, 10, 15, 30, and 60 minutes.	5

Step 3 After Live Data reporting interval is set, run the below command to restart the publisher and subscriber node (Restart the inactive node first and active node next):

```
utils system restart
```

Step 4 Run the below command to view Live Data reporting interval:

```
show live-data reporting-interval
```

Configure Transport Layer Security

Follow the procedures to set TLS Server and TLS Client minimum version.

Import Reports

You can import the Unified Intelligence Center report, which is in either .xml or .zip file format.

The imported report retrieves data for the following entities:

- Report
- Report Definition
- Value Lists
- Views
- Thresholds
- Drilldowns
- Template Help

Note Each report template help folder has a size limit of 3 MB. If the folder size exceeds this limit, the system does not load the help content.

Note You cannot import Report Filters and Collections.

Ensure that the data source is used to import the Report Definition is configured in Unified Intelligence Center. Also, ensure that data source is used by any value list that is defined in Unified Intelligence Center, if the report definition has any value list defined.

To import reports, perform the following steps:

Procedure

Step 1 In the left navigation pane, choose **Reports**.

Step 2 In the **Reports** listing page, click **Import**.

Step 3 Click **Browse** to select the file (.xml or .zip format) to be imported.

Note Maximum file size for .zip file format is 60 MB and for .xml file format is 3 MB.

Step 4 Select the required file and click **Open**.

Step 5 Select the file location from the **Save to Folder** list to save the file.

Step 6 Click **Upload**.
Once the file is successfully uploaded, the table gets populated with the corresponding report template, current available version, and incoming version of the files being imported.

Step 7 Select a Data Source for the Report Definition only if the Report Definition for the report being imported is not defined in Unified Intelligence Center.

Step 8 Select a Data Source for the Value List that is defined in the Report Definition.

Note Selection of a Data Source for the Value List is mandatory:

- If the Value List does not use the same Data Source as the Report Definition.
- For Real Time Streaming Report Definitions.

Step 9 Select the files to import or overwrite.

- Overwrite—If the report being imported exists in the Unified Intelligence Center.
- Import—If the report being imported is the new set of report files.

Step 10 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.
- Importing manually edited XMLs is not supported.

Add Certificate for HTTPS Gadget

Add a certificate for a secure HTTP (HTTPS) gadget to allow the gadget to load into the Finesse desktop and successfully perform HTTPS requests to the Finesse server.

This process allows HTTPS communication between the Finesse gadget container and the third-party gadget site for loading the gadget and performing any API calls that the gadget makes to the third-party server.

Note A gadget that loads using HTTPS may still use HTTP communication between that gadget and the application server where it resides. If all traffic must be secure, the gadget developer must ensure that HTTPS is used to make API calls to the application server.

The certificate must be signed with a common name. The gadget URL in the desktop layout must use the same name (whether it uses an IP address or a fully qualified domain name) as the name with which the certificate is signed. If the certificate name and the name in the gadget URL do not match, the connection is not trusted and the gadget does not load.

Before you begin

Set up security certificates for finesse, Cisco Unified Intelligence Center and Live Data server to server communication. Import certificates into servers as shown in the table below:

Server	Import Certificates
Finesse	Live Data and Cisco Unified Intelligence Center
Cisco Unified Intelligence Center	Live Data

Procedure

Step 1 Download the tomcat-trust.pem certificate from the third-party gadget host.

a) Sign in to Cisco Unified Operating System Administration on the third-party gadget host (`http://host or IP address/cmplatform` where `host` or `IP address` is the hostname or IP address of third-party gadget host).
b) Choose **Security** > **Certificate Management**.
c) Click **Find**.
d) Click **Common Name** hyperlink for the required tomcat trust.
e) Click **Download.PEM File**.

Step 2 Upload the certificate to the Finesse Publisher server.

a) Sign in to Cisco Unified Operating System Administration on Finesse Publisher server (`http://host or IP address/cmplatform` where `host` or `IP address` is the hostname or IP address of the finesse server).
b) Choose **Security** > **Certificate Management**.
c) Click **Upload Certificate**.
d) Choose **Tomcat Trust** from **Certificate Purpose** drop-down list.
e) Click **Common Name** hyperlink for the required tomcat trust.
f) Click **Browse** to choose the downloaded tomcat-trust.pem file.

g) Click **Upload File**.

Step 3 Restart **Cisco Tomcat** and **Cisco Finesse Tomcat** services on the Finesse Publisher server.

Step 4 Ensure the certificates are synchronized in Finesse Subscriber server.

Step 5 Restart **Cisco Tomcat** and **Cisco Finesse Tomcat services** on Finesse Subscriber server.

Configure Cisco Finesse

This table lists the configuration procedures for Cisco Finesse:

Sequence	Task	Done?
1	Configure the Cisco Finesse Primary Node, on page 93	
2	-	
3	Configure Cisco Finesse Secondary Node, on page 98	
4	Install VMware Tools for Windows, on page 82	
5	Configure Cisco Finesse Administration, on page 99	
6	Configure SNMP, on page 106	

Configure the Cisco Finesse Primary Node

Note You must configure the Cisco Finesse primary node before you customize the secondary node.

Before you begin

Ensure that the Virtual Machine device status is **Connect at Power On** checked for the Network adapter and Floppy drive

Procedure

Step 1 Power on the primary node. To begin the installation based on the information in the .flp file.
The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the Finesse Primary machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power** on for the floppy drive.

Note During the customization of the primary, the username and the password are modified as follows. The customer should change the password.

- Default Password for OS Administrator: **c1sco@123**
- Application UserName: **Administrator**
- Default Password for Application User: **c1sco@123**
- Sftp password: **c1sco@123**
- IPSec password: **c1sco@123**

After rebooting, the VM installation is complete with all the parameters provided in the spreadsheet for the VM.

Configure Settings for the CTI Server and Administration and Data Server

- Configure Contact Center Enterprise CTI Server Settings in the Cisco Finesse Primary Node, on page 94
- Configure Contact Center Enterprise Administration and Data Server Settings, on page 97
- Restart the Cisco Tomcat Service, on page 97

Configure Contact Center Enterprise CTI Server Settings in the Cisco Finesse Primary Node

Access the administration console on the primary Finesse server to configure the A and B Side CTI servers.

Note After you restart Finesse, it can take approximately 6 minutes for all server-related services to restart. Therefore, wait for 6 minutes before you attempt to access the Finesse administration console.

Note If you are using HTTPS, the first time you access the administration console, you see a browser security warning. To eliminate browser security warnings each time you sign in, trust the self-signed certificate provided with Finesse or obtain and upload a CA certificate.

Procedure

Step 1 Sign in to the administration console on the primary Finesse server:

https://*FQDN of Finesse server*/cfadmin

Step 2 Sign in with the Application User credentials defined during installation.

Step 3 In the Contact Center Enterprise CTI Server Settings area, enter the CTI server settings as described in the following table. Refer to your configuration worksheet if necessary.

Field	Description
A Side Host/IP Address	Enter the hostname or IP address of the A Side CTI server. This value is typically the IP address of the Peripheral Gateway (PG). The CTI server runs on the PG.
A Side Port	Enter the port number of the A Side CTI server. The value of this field must match the port configured during the setup of the A Side CTI server.
Peripheral ID	Enter the ID of the Agent PG Routing Client (PIM). The Agent PG Peripheral ID should be configured to the same value for the A and B Side CTI servers.
B Side Host/IP Address	Enter the hostname or IP address of the B Side CTI server.
B Side Port	Enter the port of the B Side CTI server. The value of this field must match the port configured during the setup of the B Side CTI server.

Step 4 Click **Save**.

Contact Center Enterprise Administration and Data Server Settings

Use the Unified CCE Administration & Data Server Settings gadget to configure the database settings. These settings are required to enable authentication for Finesse agents and supervisors.

Note To connect to the AW Database (AWDB) in the Unified CCE Administration, Cisco Finesse supports both SQL and Windows authentication.

The Cisco Finesse Java Database Connectivity (JDBC) driver is configured to use NTLMv2. Therefore, Finesse can connect to the administration database even if the administration database is configured to use only NTLMv2.

Primary Administration & Data Server is configured on Side A and Secondary Administration & Data Server is configured on Side B. Make sure Cisco Finesse server on both sides connect to Primary Administration & Data Server on side A and fall back to Secondary Administration & Data Server on side B only when Primary Administration & Data Server goes down.

After you change and save any value on the Contact Center Enterprise Administration & Data Server Settings gadget, restart the Cisco Finesse Tomcat Service on the primary and secondary Finesse server. If you restart the Cisco Finesse Tomcat Service, agents must sign out and sign in again. To avoid this, you can make Contact Center Enterprise Administration & Data Server settings changes and restart the Cisco Finesse Tomcat service during hours when agents are not signed in to the Cisco Finesse desktop.

The following table describes the fields on the Unified CCE Administration & Data Server Settings gadget:

Table 11: Field Descriptions

Field	Description
Primary Host/IP Address	The hostname or IP address of the Unified CCE Administration & Data Server.
Backup Host/IP Address	(Optional) The hostname or IP address of the backup Unified CCE Administration & Data Server.
Database Port	The port of the Unified CCE Administration & Data Server. The default value is 1433. **Note** Cisco Finesse expects the primary and backup Administration & Data Server ports to be the same, hence the Finesse administration console exposes one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers.
AW Database Name	The name of the AW Database (AWDB). For example, *ucceinstance*_awdb).
Domain	(Optional) The domain name of the AWDB.
Username	The username required to sign in to the AWDB. **Note** If you specify a domain, this user refers to the Administrator Domain user that the AWDB uses to synchronize with the logger. In which case, the AWDB server must use Windows authentication and the configured username must be a domain user. If you do not specify a domain, this user must be an SQL user.
Password	The password required to sign in to the AWDB.

For more information about these settings, see the *Administration Guide for Cisco Unified Contact Center Enterprise* and the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise*.

Actions on the Unified CCE Administration & Data Server Settings gadget:

- **Save:** Saves your configuration changes
- **Revert:** Retrieves the most recently saved enterprise database settings

When you update any of the following fields and click Save, Cisco Finesse attempts to connect to the AWDB:

- Primary Host/IP Address

- Backup Host/IP Address
- Database Port
- AW Database Name

If Cisco Finesse cannot connect to the AWDB, an error message appears and you are asked if you still want to save. If you click **Yes**, the settings are saved. If you click **No**, the settings are not saved. You can change the settings and try again or click **Revert** to retrieve the previously saved settings.

When you update the Username or Password fields and click **Save**, Cisco Finesse attempts to authenticate against the AWDB. If authentication fails, an error message appears and you are asked if you still want to save. Click **Yes** to save the settings or click **No** to change the settings. Click **Revert** to retrieve the previously saved settings.

Note Finesse will not come into service in case of AWDB errors when connecting Cisco Finesse 11.5(1) and higher versions to Unified CCE 11.5(1) and higher versions.

Configure Contact Center Enterprise Administration and Data Server Settings

Configure the Unified CCE Administration & Data Server settings to enable authentication for Finesse agents and supervisors.

Procedure

Step 1 If you are not already signed in, sign in to the administration console.

Step 2 In the Unified CCE Administration & Data Server Settings area, enter the Administration & Data Server settings as described in the preceding table. For more information, see Table 11: Field Descriptions, on page 96. Refer to your configuration worksheet if necessary.

Step 3 Click **Save**.

What to do next

The CTI test functionality documented in the *Configure Unified CCE CTI Server Settings* topic depends on AWDB connectivity to determine the CTI version. Or else, the test will not go through.

Restart the Cisco Tomcat Service

After you change and save any value on Unified CCE Administration server settings, you must restart the Cisco Tomcat Service on the primary Cisco Finesse server.

Procedure

Step 1 Enter **utils service stop Cisco Tomcat** command, to stop the Cisco Tomcat service.

Step 2 Enter **utils service start Cisco Tomcat** command, to start the Cisco Tomcat service.

Configure Cisco Finesse Secondary Node

Launch the Finesse Administration Console to Configure the Secondary Finesse

To add the secondary node, you must launch the primary node and add the secondary node to the cluster.

Procedure

Step 1 Launch the Cisco Finesse primary node in a browser (`http://Primary Node FQDN/cfadmin`), where the primary node or IP address is that of your host.

Step 2 Select **Settings > Cluster Settings**. (Cluster settings are based on the default configuration and assumes that you have not changed the page for the Cluster Settings tool.)

Step 3 Add the IP address for the Cisco Finesse secondary node.

Step 4 Click **Save**.

Step 5 Restart Cisco Tomcat as follows:

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

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

Install Cisco Finesse on the Secondary Node

Before you begin

Ensure that you select the **Connect at Power on** check box of the virtual machine for network adapter and floppy drive.

Procedure

Step 1 Power on the secondary node to begin the installation based on the information in the .flp file.
The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the virtual machine. Log into the Cisco Finesse secondary machine, using the credentials for the administration user. The machine opens to the CLI interface.

Step 3 Right-click the virtual machine and choose **Edit settings** and uncheck **Connect at Power on** for the floppy drive.

Note During the customization of the secondary node, the username and the password is modified as follows. You can change the password:

- Default password for OS Administrator: **c1sco@123**
- Application username: **Administrator**
- Default password for application user: **c1sco@123**
- Sftp password: **c1sco@123**
- IPsec password: **c1sco@123**

Configure Cisco Finesse Administration

- Obtain and Upload CA Certificate, on page 99
- Deploy Certificate in Browsers, on page 100
- Accept Security Certificates, on page 103

Obtain and Upload CA Certificate

Note This procedure only applies if you are using HTTPS and is optional. If you are using HTTPS, you can choose to either obtain and upload a CA certificate or use the self-signed certificate provided with Finesse.

To eliminate browser security warnings each time you sign in, obtain an application and root certificate signed by a CA. Use the Certificate Management utility from Cisco Unified Operating System Administration.

To open Cisco Unified Operating System Administration in your browser, enter:

https://*FQDN of primary Finesse server*:8443/cmplatform

Sign in using the username and password for the Application User account created during Finesse installation.

Note You can find detailed explanations in the Security topics of the *Cisco Unified Operating System Administration Online Help*.

Procedure

Step 1 Generate a CSR.

a) Click **Security** > **Certificate Management** > **Generate CSR**.

b) From the Certificate Name drop-down list, choose **tomcat** and click **Generate CSR**.

Step 2 Download the CSR.

a) Select **Security** > **Certificate Management** > **Download CSR**.

b) From the Certificate Name drop-down list, choose **tomcat** and click **Generate CSR**.

Step 3 Generate and download a CSR for the secondary Unified CCX server.

To open Cisco Unified Operating System Administration for the secondary server in your browser, enter:

https://*FQDN of secondary Finesse server*:8443/cmplatform

Step 4 Use the CSRs to obtain the CA root certificate, intermediate certificate, and signed application certificate from the Certificate Authority.

Note To set up the certificate chain, you must upload the certificates in the order described in the following steps.

Step 5 When you receive the certificates, click **Security** > **Certificate Management** > **Upload Certificate**.

Step 6 Upload the root certificate.

a) From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
b) In the **Upload File** field, click **Browse** and browse to the root certificate file.
c) Click **Upload File**.

Step 7 Upload the intermediate certificate.

a) From the **Certificate Purpose** drop-down list, choose **tomcat-trust**.
b) In the **Upload File** field, click **Browse** and browse to the intermediate certificate file.
c) Click **Upload File**.

Step 8 Upload the application certificate.

a) From the **Certificate Purpose** drop-down list, choose **tomcat**.
b) In the **Upload File** field, click **Browse** and browse to the application certificate file.
c) Click **Upload File**.

Step 9 After the upload is complete, sign out from the Platform Admin page of Finesse.

Step 10 Access the CLI on the primary Finesse server.

Step 11 Enter the command **utils service restart Cisco Finesse Notification Service** to restart the Cisco Finesse Notification service.

Step 12 Enter the command **utils service restart Cisco Finesse Tomcat** to restart the Cisco Finesse Tomcat service.

Step 13 Upload the application certificate to the secondary Finesse server.

The root and the intermediate certificates uploaded to the primary server are replicated to the secondary server.

Step 14 Access the CLI on the secondary Finesse server and restart the Cisco Finesse Notification Service and the Cisco Finesse Tomcat Service.

Deploy Certificate in Browsers

Deploy Root Certificate for Browsers

In environments where group policies are enforced via the Active Directory domain, the root certificate can be added automatically to each user's browser. 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 browser.

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 browser.

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.

Set Up CA Certificate for Chrome and Edge Chromium (Microsoft Edge) Browsers

Procedure

Step 1 In the browser, go to **Settings**.

Step 2 In the Chrome browser, select **Advanced Settings** > **Privacy and Security**, click **Manage Certificates**.

Step 3 In the Microsoft Edge browser, select **Privacy, search, and services**. Under **Security**, click **Manage Certificates**.

Step 4 Click **Trusted Root Certification Authorities** tab.

Step 5 Click **Import** and browse to the *ca_name*.cer file.
In the **Trusted Root Certification Authorities** tab, ensure that the new certificate appears in the list.

Step 6 Restart the browser for the certificate to install.

Accept Security Certificates

Ensure that the pop-ups are enabled for the Finesse desktop.

After you enter the Finesse desktop URL in your browser, the procedure to add a certificate is as follows:

Install certificates on Windows operating system:

The procedure to add a certificate varies for each browser. The procedure for each browser is as follows:

Internet Explorer

Note If you are using a Windows client, signed in as a Windows user, you must run Internet Explorer as an administrator to install the security certificates. In your Start menu, right-click Internet Explorer and select Run as administrator.

Contact your administrator if you do not have the required permissions to install the security certificates.

1. A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)** link to open the Finesse sign in page. The Finesse sign in screen appears with a certificate error in the address bar.
2. Click on the certificate error that appears in the address bar and then click **View Certificates**.
3. In the **Certificate** dialog box, click **Install Certificate** to open the **Certificate Import Wizard**.
4. Select **Current User** to install the certificate for the current user only, or select **Local Machine** to install the certificate for all Windows users.
5. On the **Certificate Import Wizard**, click **Next**.
6. Select **Place all certificates in the following store** and click **Browse**.
7. Select **Trusted Root Certification Authorities** and click **OK**.
8. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears.
9. Click **Yes** to install the certificate. The **Certificate Import** dialog box appears.
10. Click **OK** and close the **Certificate Import** dialog box.
11. Close the browser tab. The accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.

Note To remove the certificate error from the desktop, you must close and reopen your browser.

Firefox

1. On **Your connection is not secure** page, click **Advanced** > **Add Exception**.

Note Ensure that the **Permanently store this exception** box is checked.

2. Click **Confirm Security Exception**.
3. On and click **Sign In**.
4. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.
5. On the browser tab, click **I Understand the Risks** > **Add Exception**. Ensure that the **Permanently store this exception** box is checked.
6. Click **Confirm Security Exception**. The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.

Chrome and Edge Chromium (Microsoft Edge)

1. A page appears that states your connection is not private. To open the Finesse sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.
2. Enter your agent ID or username, password, and extension, and then click **Sign In**.
3. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.
4. On the browser tab,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

   The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

Note If you click the certificate link and do not accept it, the certificate link stays enabled in the **SSL Certificate Not Accepted** dialog box. The certificate error appears every time you sign in. The procedure to permanently accept the certificate is as follows.

5. Click on the certificate error that appears in the address bar and then,

In Chrome, select **Certificate (Invalid)**.

In Microsoft Edge, select **Certificate (not valid)**.

The **Certificate** dialog box appears.

6. In the **Details** tab, click **Copy to File**. The **Certificate Export Wizard** appears.
7. Click **Next**.
8. Keep the default selection **DER encoded binary X.509 (.CER)** and click **Next**.
9. Click **Browse** and select the folder in which you want to save the certificate, enter a recognizable file name and click **Save**.
10. Browse to the folder where you have saved the certificate (**.cer** file), right-click on the file, and click **Install Certificate**. The **Certificate Import Wizard** appears.
11. Keep the default selection **Current User** and click **Next**.
12. Select **Place all certificates in the following store** and click **Browse**. The **Select Certificate Store** dialog box appears.
13. Select **Trusted Root Certification Authorities** and click **OK**.
14. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears that asks if you want to install the certificate.
15. Click **Yes**. A **Certificate Import** dialog box that states the import was successful appears.

Close the browser and sign in to Finesse. The security error does not appear in the address bar.

Install certificates on macOS:

The procedure to download a certificate varies for each browser. The procedure for each browser is as follows:

Chrome and Edge Chromium (Microsoft Edge)

1. A warning page appears which states that your connection is not private. To open the Finesse Console sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.
2. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (Not Valid)**.

   A certificate dialog box appears with the certificate details.
3. Drag the **Certificate** icon to the desktop.
4. Double-click the certificate. The **Keychain Access** application opens.
5. In the right pane of Keychains dialog, browse to the certificate, right-click on the certificate, and select **Get Info** from the options that are listed. A dialog appears with more information about the certificate.
6. Expand **Trust**. From the **When using this certificate** drop-down, select **Always Trust**.

7. Close the dialog box that has more information about the certificate. A confirmation dialog box appears.
8. Authenticate the modification of Keychains by providing a password.
9. The certificate is now trusted, and the certificate error does not appear on the address bar.

Firefox

1. In your Firefox browser, enter the Finesse desktop URL. A warning page appears which states that there is a security risk.
2. Click **Advanced** and then click **View Certificate** link. The **Certificate Viewer** dialog box appears.
3. Click **Details** and then click **Export**. Save the certificate (**.crt** file) in a local folder.

Note If **.crt** file option is not available, select **.der** option to save the certificate.

4. From the menu, select **Firefox** > **Preferences**. The **Preferences** page is displayed.
5. In the left pane, select **Privacy & Security**.
6. Scroll to the **Certificates** section and click **View Certificates ...**. The **Certificate Manager** window is displayed.
7. Click **Import** and select the certificate.
8. The certificate is now authorized, and the certificate error does not appear on the address bar.

Configure SNMP

Procedure

Step 1 Log in to the Cisco Unified Serviceability *(https://hostname of primary server:8443/ccmservice)* using administrator credentials.

Step 2 Select **SNMP** > **V1/V2c** > **Community String**.

Step 3 From **Server** drop-down list, select the server for which you want to configure a community string and click **Find**.

Step 4 Click **Add New** to add new community string.

a) Enter **Community String**.

Example:

public.

b) In **Host IP Addresses Information** field, choose **Accept SNMP Packets from any host**.
c) From **Access Privilages** drop-down list, select **ReadWriteNotify** option.
d) Check **Apply to All Nodes** check box to apply community string to all nodes in the cluster.
Information message will be displayed.
e) Click **OK**.
f) Click **Save**.

A message is displayed, that indicates that changes will not take effect until you restart the SNMP primary agent. To continue the configuration without restarting the SNMP primary agent, click **Cancel**. To restart the SNMP primary agent service, click **OK**.

g) Click **OK**.

Step 5 Select **SNMP** > **V1/V2c** > **Notification Destination**.

Step 6 From **Server** drop-down list, select the server for which you want to configure a notification destination and click **Find**.

Step 7 Click **Add New** button to add new notification destination.

a) From **Host IP Addresses** drop-down list, select **Add New**.
b) In **Host IP Address** field, enter the Prime Collaboration server IP address .
c) In the **Port Number** field, enter the notification receiving port number.

Note Default port number is 162.

d) In **SNMP Version Information** field, select the SNMP Version V2C.
e) In **Notification Type Information** field; from **Notification Type** drop-down list, select **Trap**.
f) In **Community String Information** field; from **Community String** drop-down list, select Community String created in Step 4 from the drop-down list.
g) Check the **Apply to All Nodes** check box to apply community string to all nodes.

Information message will be displayed.

h) Click **OK**.
i) Click **Insert**.

A message is displayed, that indicates that changes will not take effect until you restart the SNMP primary agent. To continue the configuration without restarting the SNMP primary agent, click **Cancel**. To restart the SNMP primary agent service, click **OK**.

j) Click **OK**.

Create a Customer Instance for the 4000 Agent Deployment Model

Follow this sequence of tasks to create the customer instance to deploy 4000 agent for Cisco HCS for CC. After each task, return to this page to mark the task “done” and continue the sequence.

Table 12: Create customer instance for 4000 agent deployment of Cisco HCS for CC for Contact Center

Sequence	Task	Done?
1	Upgrade VMware Tools, on page 16	
2	Set Up Virtual Machine Startup and Shutdown, on page 16	
3	Create a Domain Controller Server, on page 17	
4	Configure Cisco Unified CCE Rogger, on page 108	
5	Configure Unified CCE AW-HDS-DDS, on page 31	

Sequence	Task	Done?
6	Configure Unified CCE PG, on page 36	
7	Configure Unified CVP, on page 48	
8	Configure Cisco IOS Enterprise Voice Gateway, on page 66	
9	Configure Unified Communications Manager, on page 72	
10	Configure Unified Intelligence Center , on page 109	
11	Configure Live Data Reporting System, on page 118	
12	Configure Cisco Finesse, on page 93	
13	Configure Cisco Identity Service, on page 110	

What to do next

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

- CA certificates, see CA Certificates, on page 131

Configure Cisco Unified CCE Rogger

This table lists the configuration procedures you must perform to configure Cisco Unified CCE Rogger.

Sequence	Task	Done?
1	Configure Network Cards, on page 21	
2	Verify the Machine in Domain, on page 23	
3	Configure the Domain Manager, on page 24	
4	Configure Unified CCE Encryption Utility, on page 25	
5	Configure SQL Server for CCE Components, on page 25	
6	Allocate a Second Virtual Hard Drive, on page 26	
7	Configure the Unified CCE Logger, on page 27	
8	Configure the Unified CCE Router, on page 29	
9	Load Base Configuration, on page 108	
10	Verify Cisco Diagnostic Framework Portico, on page 45	
11	Cisco SNMP Setup, on page 45	

Load Base Configuration

Complete this procedure to import base configuration parameters.

Procedure

Step 1 Based on your timezone, download the HCS-CC_12.5.1-Day1_4000_NA.zip or HCS-CC_12.5.1-Day1_4000_UK.zip file. Save it locally and unzip it.

Step 2 Download the Domain_Update_Tool.zip file. Save it locally and unzip it.

Step 3 Copy the configuration folder to the local drive of Unified CCE Rogger on Side A.

Step 4 Open the ICMDBA Tool on the Unified CCE Rogger on Side A.

Step 5 Select the Unified CCE Rogger and expand the tree to <instance name>_sideA.

Step 6 Select Data on the menu bar and click **Import**.

Step 7 Browse to locate the configuration folder and click **Open**.

Step 8 Click **OK** and then click **Import**.

Step 9 Click Start and then click **OK** on all messages.

Step 10 Navigate to the folder Domain_Update_Tool and right-click UpdateDomain.PS1. and Run with PowerShell. Respond as follows:

a) For Server name, enter the computer name of the Unified CCE Rogger Side A.
b) For Database name, enter <instance_sideA (Logger database)>.
c) For Domain Name, enter the customer's domain name.

Step 11 Return to the ICMDBA tool. Select Logger <instance name> database for the side that you want to synchronize.

Step 12 Click **Data** in menu bar and select **Synchronize** and perform the following:

a) In **Synchronize** window, click **Add** in **Source** pane.
b) Enter hostname for Unified CCEE Rogger of source in **Server Name** field and click **OK**.
c) Click **Add** in **Destination** pane.
d) Enter hostname for Unified CCE Rogger of destination in **Server Name** field and click **OK**.
e) Click **Synchronize**.

Step 13 Click **Start**. After synchronization click **OK**.

Configure Unified Intelligence Center

Follow these tasks to configure Unified Intelligence Center.

Sequence	Task	Done?
1	Configure Unified Intelligence Center Publisher, on page 79	
2	Configure Unified Intelligence Center Subscriber, on page 80	
3	Install VMware Tools for Windows, on page 82	
4	Configure Unified Intelligence Center Reporting, on page 82	
5	Configure Unified Intelligence Center Administration, on page 85	
6	Configure SNMP, on page 106	

Configure Live Data Reporting System

Sequence	Task	Done?
1	Configure Live Data AW-Access, on page 87	
2	Configure Live Data Machine Services, on page 88	
3	Configure Live Data Unified Intelligence Data Sources, on page 89	
4	Configure Live Data Reporting Interval, on page 89	
5	Configure Transport Layer Security , on page 90	
6	Import Reports, on page 55	
7	Add Certificate for HTTPS Gadget, on page 92	

Configure Cisco Identity Service

Sequence	Task	Done?
1	Configure Ids Publisher , on page 110	
2	Set IdS Subscriber Node, on page 111	
3	Configure Ids Subscriber , on page 111	

Configure Ids Publisher

You must customize the Cisco Identity Service publisher before you customize the subscribers.

Before you begin

Ensure that the Virtual Machine device status shows **Connect at Power On** checked for the Network adapter and Floppy drive.

Procedure

Step 1 Power on the Publisher. This begins the installation based on the information in the .flp file.The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the Publisher machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power on** for the floppy drive.

Set IdS Subscriber Node

You must provide the publisher node the address of the subscriber node. You do this with the **set ids subscriber** command.

Procedure

Step 1 Log in to your publisher IdS node.

Step 2 Run the following command to set the subscriber node:

set ids subscriber *name*
name

Specifies the hostname or ip address of the IdS subscriber node address.

What to do next

You can use these Cisco IdS CLI commands only in an IdS standalone deployment. You run these commands on the IdS publisher node.

Required Minimum Privilege Level: Ordinary

Use this command to show IdS subscriber node information.

show ids subscriber

There are no required parameters.

Required Minimum Privilege Level: Advanced

Use this command to unset IdS subscriber node configuration.

unset ids subscriber

There are no required parameters.

Configure Ids Subscriber

Before you begin

Ensure that the Virtual Machine device status is **Connect at Power On** checked for the Network adapter and Floppy drive

Procedure

Step 1 Power on the Subscriber.

This begins the installation based on the information in the .flp file. The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the CUCM Secondary machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power on** for the floppy drive.

Create Customer Instance for 12000 Agent Deployment Model

Follow this sequence of tasks to create the customer instance to deploy 12000 agent for Cisco HCS for CC. After each task, return to this page to mark the task "done" and continue the sequence.

Table 13: Create customer instance for 12000 agent deployment of Cisco HCS for CC

Sequence	Task	Done?
1	Upgrade VMware Tools, on page 16	
2	Set Up Virtual Machine Startup and Shutdown, on page 16	
3	Create a Domain Controller Server, on page 17	
4	Configure Unified CCE Logger , on page 112	
5	Configure Unified CCE Router, on page 114	
6	Configure Unified CCE AW-HDS, on page 114	
7	Configure Unified CCE HDS-DDS, on page 116	
8	Configure Unified CCE PG, on page 36	
9	Configure Unified CVP, on page 48	
10	Configure Cisco IOS Enterprise Voice Gateway, on page 66	
11	Configure Unified Communications Manager, on page 72	
12	Configure Unified Intelligence Center , on page 109	
13	Configure Live Data Reporting System, on page 118	
14	Configure Cisco Finesse, on page 93	
15	Single Sign-on Administration, on page 300	
16	Configure Cisco Identity Service, on page 110	

What to do next:

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

- CA certificates, see CA Certificates, on page 131

Configure Unified CCE Logger

This section explains the configuration procedures you must perform for the Unified CCE Logger.

Sequence	Task	Done?
1	Configure Network Cards, on page 21	
2	Verify the Machine in Domain, on page 23	
3	Configure the Domain Manager, on page 24	
4	Configure Unified CCE Encryption Utility, on page 25	
5	Configure SQL Server for CCE Components, on page 25	
6	Allocate a Second Virtual Hard Drive, on page 26	
7	Configure the Unified CCE Logger, on page 27	
8	Load Base Configuration, on page 113	
9	Verify Cisco Diagnostic Framework Portico, on page 45	
10	Cisco SNMP Setup, on page 45	

Load Base Configuration

Complete this procedure to import base configuration parameters.

Procedure

Step 1 Based on your timezone, download the HCS-CC_12.5.1-Day1_12000_NA.zip or HCS-CC_12.5.1-Day1_12000_UK.zip file. Save it locally and unzip it.

Step 2 Download the Domain_Update_Tool.zip file. Save it locally and unzip it.

Step 3 Copy the configuration folder to the local drive of Unified CCE Logger on Side A.

Step 4 Open the ICMDBA Tool on the Unified CCE Logger on Side A.

Step 5 Select the Unified CCE Logger and expand the tree to <instance name>_sideA.

Step 6 Select Data on the menu bar and click **Import**.

Step 7 Browse to locate the configuration folder and click **Open**.

Step 8 Click **OK** and then click **Import**.

Step 9 Click Start and then click **OK** on all messages.

Step 10 Navigate to the folder Domain_Update_Tool and right-click UpdateDomain.PS1. and Run with PowerShell. Respond as follows:

a) For Server name, enter the computer name of the Unified CCE Logger Side A.
b) For Database name, enter <instance_sideA (Logger database)>.
c) For Domain Name, enter the customer's domain name.

Step 11 Return to the ICMDBA tool. Select Logger <instance name> database for the side that you want to synchronize.

Step 12 Click **Data** in menu bar and select **Synchronize** and perform the following:

a) In **Synchronize** window, click **Add** in **Source** pane.

b) Enter hostname for Unified CCE Logger of source in **Server Name** field and click **OK**.
c) Click **Add** in **Destination** pane.
d) Enter hostname for Unified CCE Logger of destination in **Server Name** field and click **OK**.
e) Click **Synchronize**.

Step 13 Click **Start** and then click **OK** on all messages.

Configure Unified CCE Router

This section explains the configuration procedures you must perform for the Unified CCE Router.

Sequence	Task	Done?
1	Configure Network Cards, on page 21	
2	Validate Network Card, on page 49	
3	Configure Unified CCE Encryption Utility, on page 25	
4	Configure the Unified CCE Router, on page 29	
5	Verify Cisco Diagnostic Framework Portico, on page 45	
6	Cisco SNMP Setup, on page 45	

Configure Unified CCE AW-HDS

This section explains the configuration procedures you must perform for the Unified CCE AW-HDS for Sides A and B.

Table 14: Configuring Unified CCE AW-HDS for Side A and Side B

Sequence	Task	Done?
1	Configure Network Cards, on page 21	
2	Verify the Machine in Domain, on page 23	
3	Configure Unified CCE Encryption Utility, on page 25	
4	Configure SQL Server for CCE Components, on page 25	
5	Allocate a Second Virtual Hard Drive, on page 26	
6	AW-HDS, on page 115	
7	Verify Cisco Diagnostic Framework Portico, on page 45	
8	Cisco SNMP Setup, on page 45	
9	Set the HCS for CC Deployment Type, on page 34	

AW-HDS

Configure AW-HDS

Complete the following procedure to install the Unified CCE Administration Server & Real-time, Historical Data Server (AW-HDS).

Procedure

Step 1 Choose **Component Management**>**Administration & Data Servers**.

Step 2 Click **Add**.

Step 3 On the **Deployment** window, choose the current instance.

Step 4 On the **Add Administration & Data Servers** window, configure as follows:

a) Click **Enterprise**.
b) Click **Large** deployment size.
c) Click **Next**.

Step 5 On the **Server Role in Large Deployment** window, configure as follows:

a) Choose the option **Administration Server and Real-time and Historical Data Server (AW-HDS)**.
b) Click **Next**.

Step 6 On the **Administration & Data Servers Connectivity** window, configure as follows:

a) Select **Primary Administration & Data Server**.
b) Enter the hostname of the secondary AW-HDS in the **Secondary Administration & Data Server** field.
c) Enter the site name in **Primary/Secondary Pair (Site) Name** field.

Note Ensure that the site name match with the site name defined under **PG Explorer** > **Agent Peripheral** > **Agent Distribution** .

d) Click **Next**.

Step 7 On the **Database and Options** window, configure as follows:

a) In the **Create Database(s)** on Drive field, select the secondary drive (typically **D** or **E**).
b) Check the **Configuration Management Service (CMS) Node**.
c) Check **Internet Script Editor (ISE) Server**.
d) Click **Next**.

Step 8 On the **Central Controller Connectivity** window, configure as follows:

a) For Router Side A enter the host name/IP address machine where Router A resides.
b) For Router Side B enter the host name/IP address machine where Router B resides.
c) For Logger Side A enter the host name/IP address machine where Logger A resides.
d) For Logger Side B enter the host name/IP address machine where Logger B resides.
e) Enter the **Central Controller Domain Name** .

f) Click **Central Controller Side A Preferred** .
g) Click **Next** .

Step 9 Review the **Summary** window, and click **Finish**.

Note Do not start services until all Unified CCE components are installed.

Configure Unified CCE HDS-DDS

This section explains the configuration procedures you must perform for the Unified CCE HDS-DDS for Sides A and B.

Table 15: Configuring Unified CCE HDS-DDS for Side A and Side B

Sequence	Task	Done?
1	Configure Network Cards, on page 21	
2	Validate Network Card, on page 49	
3	Configure Unified CCE Encryption Utility, on page 25	
4	Configure SQL Server for CCE Components, on page 25	
5	Allocate a Second Virtual Hard Drive, on page 26	
6	HDS-DDS, on page 116	
7	Verify Cisco Diagnostic Framework Portico, on page 45	
8	Cisco SNMP Setup, on page 45	

HDS-DDS

- Create Instance, on page 31
- Create HDS Database, on page 32
- Configure HDS-DDS, on page 116
- Database and Log File Size, on page 34

Configure HDS-DDS

Complete the following procedure to install the Cisco Unified CCE Administration Server & Real-time, Historical Data Server (AW-HDS).

Procedure

Step 1 Choose **Component Management**>**Administration & Data Servers**.

Step 2 Click **Add**.

Step 3 On the **Deployment** window, choose the current instance.

Step 4 On the **Add Administration & Data Servers** window, configure as follows:

a) Click **Enterprise**.
b) Click **Large** deployment size.
c) Click **Next**.

Step 5 On the **Server Role in Large Deployment** window, configure as follows:

a) Choose the option **Historical Data Server and Detailed Data Server (HDS-DDS)**.
b) Click **Next**.

Step 6 On the **Administration & Data Servers Connectivity** window, configure as follows:

a) Select **Primary Administration & Data Server**.
b) Enter the hostname of the secondary HDS-DDS in the **Secondary Administration & Data Server** field.
c) Enter the site name in **Primary/Secondary Pair (Site) Name** field.

Note Ensure that the site name match with the site name defined under **PG Explorer** > **Agent Peripheral** > **Agent Distribution** .

d) Click **Next**.

Step 7 On the **Database and Options** window, configure **Create Database(s)** on **Drive** field, select the secondary drive (typically **D** or **E**).

Step 8 On the **Central Controller Connectivity** window, configure as follows:

a) For Router Side A enter the host name/IP address machine where Router A resides.
b) For Router Side B enter the host name/IP address machine where Router B resides.
c) For Logger Side A enter the host name/IP address machine where Logger A resides.
d) For Logger Side B enter the host name/IP address machine where Logger B resides.
e) Enter the **Central Controller Domain Name** .
f) Click **Central Controller Side A Preferred** .
g) Click **Next** .

Step 9 Review the **Summary** window, and click **Finish**.

Note Do not service until all Unified CCE components are installed.

Configure Unified Intelligence Center

Follow these tasks to configure Unified Intelligence Center.

Sequence	Task	Done?
1	Configure Unified Intelligence Center Publisher, on page 79	
2	Configure Unified Intelligence Center Subscriber, on page 80	
3	Install VMware Tools for Windows, on page 82	
4	Configure Unified Intelligence Center Reporting, on page 82	
5	Configure Unified Intelligence Center Administration, on page 85	

Sequence	Task	Done?
6	Configure SNMP, on page 106	

Configure Live Data Reporting System

Sequence	Task	Done?
1	Configure Live Data AW-Access, on page 87	
2	Configure Live Data Machine Services, on page 88	
3	Configure Live Data Unified Intelligence Data Sources, on page 89	
4	Configure Live Data Reporting Interval, on page 89	
5	Import Reports, on page 55	
6	Add Certificate for HTTPS Gadget, on page 92	

Create Customer Instance for 24000 Agent Deployment Model

Follow this sequence of tasks to create the customer instance to deploy 24000 agent for Cisco HCS for CC. After each task, return to this page to mark the task "done" and continue the sequence.

Table 16: Create customer instance for 24000 agent deployment of Cisco HCS for CC

Sequence	Task	Done?
1	Upgrade VMware Tools, on page 16	
2	Set Up Virtual Machine Startup and Shutdown, on page 16	
3	Create a Domain Controller Server, on page 17	
4	Configure Unified CCE Logger , on page 112	
5	Configure Unified CCE Router, on page 114	
6	Configure Unified CCE AW-HDS, on page 114	
7	Configure Unified CCE HDS-DDS, on page 116	
8	Configure Unified CCE PG, on page 36	
9	Configure Unified CVP, on page 48	
11	Configure Cisco IOS Enterprise Voice Gateway, on page 66	
12	Configure Unified Communications Manager, on page 72	

Sequence	Task	Done?
13	Configure Unified Intelligence Center , on page 109	
14	Configure Live Data Reporting System, on page 118	
15	Configure Cisco Finesse, on page 93	
16	Single Sign-on Administration, on page 300	
17	Configure Cisco Identity Service, on page 110	

What to do next:

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

- CA certificates, see CA Certificates, on page 131

Load Base Configuration

Complete this procedure to import base configuration parameters.

Procedure

Step 1 Based on your timezone, download the HCS-CC_12.5.1-Day1_24000_NA.zip or HCS-CC_12.5.1-Day1_24000_UK.zip file. Save it locally and unzip it.

Step 2 Download the Domain_Update_Tool.zip file. Save it locally and unzip it.

Step 3 Copy the configuration folder to the local drive of Unified CCE Logger on Side A.

Step 4 Open the ICMDBA Tool on the Unified CCE Logger on Side A.

Step 5 Select the Unified CCE Logger and expand the tree to <instance name>_sideA.

Step 6 Select Data on the menu bar and click **Import**.

Step 7 Browse to locate the configuration folder and click **Open**.

Step 8 Click **OK** and then click **Import**.

Step 9 Click Start and then click **OK** on all messages.

Step 10 Navigate to the folder Domain_Update_Tool and right-click UpdateDomain.PS1. and Run with PowerShell. Respond as follows:

a) For Server name, enter the computer name of the Unified CCE Logger Side A.
b) For Database name, enter <instance_sideA (Logger database)>.
c) For Domain Name, enter the customer's domain name.

Step 11 Return to the ICMDBA tool. Select Logger <instance name> database for the side that you want to synchronize.

Step 12 Click **Data** in menu bar and select **Synchronize** and perform the following:

a) In **Synchronize** window, click **Add** in **Source** pane.
b) Enter hostname for Unified CCE Logger of source in **Server Name** field and click **OK**.
c) Click **Add** in **Destination** pane.
d) Enter hostname for Unified CCE Logger of destination in **Server Name** field and click **OK**.
e) Click **Synchronize**.

Step 13 Click **Start** and then click **OK** on all messages.

Create Customer Instance for Small Contact Center Agent Deployment Model

Follow these sequence of tasks to create the customer instance to deploy small agent for Cisco HCS for CC for Contact Center. After each task, return to this page and mark the task “done” and continue the sequence.

Table 17: Create Customer Instance for core components

Sequence	Task	Done
1	Upgrade VMware Tools, on page 16	
2	Set Up Virtual Machine Startup and Shutdown, on page 16	
3	Create DNS Server for Finesse in Small Contact Center Deployment, on page 124	
4	Configure Unified CCE Rogger for Small Contact Center Agent Deployment , on page 121	
5	Configure Unified CCE AW-HDS-DDS, on page 31	
6	Configure VRU Peripheral Gateway, on page 40	
7	Configure Unified CVP, on page 48	
8	Configure CUBE Enterprise for Small Contact Center Deployment Model, on page 127	
9	Configure Unified Intelligence Center , on page 109	
10	Configure Live Data Reporting System, on page 110	

Table 18: Configure Dedicated Components Sub Customer Option

Sequence	Task	Done
1	Set Up Virtual Machine Startup and Shutdown, on page 16	
2	Configure Unified CCE PG, on page 36	
3	Configure Unified Communications Manager, on page 72	
4	Increase the SW MTP and SW Conference Resources, on page 299	
5	Configure Cisco Finesse, on page 93	
6	Configure Cisco Identity Service, on page 110	

Table 19: Configure Shared Components Sub Customer Option

Sequence	Task	Done
1	Set Up Virtual Machine Startup and Shutdown, on page 16	
2	Configure Unified CCE PG, on page 36	
3	Configure Shared Unified Communications Manager, on page 123	
4	Configure Cisco Finesse, on page 93	
5	Configure Cisco Identity Service, on page 110	

After creating customer instance for shared core components and sub customer components for small contact center agent deployment:

- Configure unified CCDM to integrate with the Internet Script Editor. See Integration of Small Contact Center Agent Deployment for Partition Internet Script Editor with CCDM, on page 169.
- To establish secure connection between a client and a server, use one of the following security certificates:
  - CA certificates, see CA Certificates, on page 131

Configure Unified CCE Rogger for Small Contact Center Agent Deployment

This section explains the configuration procedures you must perform for the Unified CCE Rogger.

Sequence	Task	Done?
1	Configure Network Cards, on page 21	
2	Verify the Machine in Domain, on page 23	
3	Configure the Domain Manager, on page 24	
4	Configure Unified CCE Encryption Utility, on page 25	
5	Configure SQL Server for CCE Components, on page 25	
6	Allocate a Second Virtual Hard Drive, on page 26	
7	Configure the Unified CCE Logger, on page 27	
8	Configure Unified CCE Router for Small Contact Center, on page 122	
9	Load Base Configuration, on page 122	
10	Verify Cisco Diagnostic Framework Portico, on page 45	
11	Cisco SNMP Setup, on page 45	

Load Base Configuration

Complete this procedure to import base configuration parameters.

Procedure

Step 1 Based on your timezone, download the HCS-CC_12.5.1-Day1_SCC_NA.zip or HCS-CC_12.5.1-Day1_SCC_UK.zip file. Save it locally and unzip it.

Step 2 Download the Domain_Update_Tool.zip file. Save it locally and unzip it.

Step 3 Copy the configuration folder to the local drive of Unified CCE Rogger on Side A.

Step 4 Open the ICMDBA Tool on the Unified CCE Rogger on Side A.

Step 5 Select the Unified CCE Rogger and expand the tree to <instance name>_sideA.

Step 6 Select Data on the menu bar and click **Import**.

Step 7 Browse to locate the configuration folder and click **Open**.

Step 8 Click **OK** and then click **Import**.

Step 9 Click Start and then click **OK** on all messages.

Step 10 Navigate to the folder Domain_Update_Tool and right-click UpdateDomain.PS1. and Run with PowerShell. Respond as follows:

a) For Server name, enter the computer name of the Unified CCE Rogger Side A.
b) For Database name, enter <instance_sideA (Logger database)>.
c) For Domain Name, enter the customer's domain name.

Step 11 Return to the ICMDBA tool. Select Logger <instance name> database for the side that you want to synchronize.

Step 12 Click **Data** in menu bar and select **Synchronize** and perform the following:

a) In **Synchronize** window, click **Add** in **Source** pane.
b) Enter hostname for Unified CCE Rogger of source in **Server Name** field and click **OK**.
c) Click **Add** in **Destination** pane.
d) Enter hostname for Unified CCE Rogger of destination in **Server Name** field and click **OK**.
e) Click **Synchronize**.

Step 13 Click **Start** and then click **OK** on all messages.

Configure Unified CCE Router for Small Contact Center

Complete the following procedure to configure the Unified CCE Router.

Procedure

Step 1 Launch the Unified CCE Web Setup.

Step 2 Sign in as the domain user with local Administrator permission.

Step 3 Navigate to **Component Management** > **Routers**.

Step 4 Click **Add** to set up the Call Router.

Step 5 In the Deployment window, select the appropriate **Side**.

Step 6 Select **Duplexed** and click **Next**.

Step 7 In the **Router Connectivity** window, configure the Private Interface and Public (Visible) Interfaces. Click **Next**.

Step 8 In the **Enable Peripheral Gateways** field, enter the number assigned to the PGs to enable it.

Use a hyphen to indicate a range and commas to separate values. For example, "2-4, 6, 79-80" enables PG2, PG3, PG4, PG6, PG79, and PG80. Spaces are ignored.

Note Enter only the IDs of the PGs which exist in the system. Adding unused PG IDs can cause incorrect Router failover handling.

Step 9 For PGs 81-150, click **Advanced** to expand it and enter the PG numbers to be used.

Step 10 In the **Router Options** window, configure the following, and click **Next** .

a) Check **Enable Database Routing**
b) Check **Enable Quality of Service (QoS)**. (Applicable to Side A only.)

Step 11 In **Router Quality of Service** window, click **Next** .

Step 12 In the **Summary** window, make sure that the Router summary is correct, then click **Finish** .

Note Do not start service until all Unified CCE components are installed.

Configure Shared Unified Communications Manager

Follow this sequence of tasks to configure shared Unified Communications Manager:

Sequence	Task	Done?
1	Configure Unified Communications Manager Publisher, on page 72	
2	Configure Unified Communications Manager Subscriber, on page 73	
3	Install VMware Tools for Windows, on page 82	
4	Unified Communications Manager License, on page 74	
5	Activate Services , on page 75	
6	Validate Clusterwide Domain Configuration, on page 76	
7	Upgrade Cisco JTAPI Client on PG, on page 44	
8	Configure SNMP, on page 106	
9	Setup Partition, on page 437	
10	Setup Calling Search Space, on page 437	
11	Associate CSS and Partition with Phones and Lines, on page 437	

Sequence	Task	Done?
12	Associate CSS with Trunk, on page 438	

Create DNS Server for Finesse in Small Contact Center Deployment

Few VOS machines (like Finesse) require a DNS server resolution to be locally available in the same network for successful VOS installation. Install DNS in the Sub customer network for Small Contact Center deployment.

Complete the following procedures to create DNS server:

- Enable DNS Server, on page 19
- Configure DNS Server, on page 125

Enable DNS Server

Procedure

Step 1 Go to **Start** > **Server Manager**.

Step 2 In the **Server Manager** window, select **Manage** > **Add Roles and Features**.

Step 3 In the **Before You Begin** tab, click **Next**.

Step 4 In the **Installation Type** tab, choose **Role based or feature based installation** option and click **Next**.

Step 5 The **Server Selection** tab, displays the list of servers that are running on Windows Server. Select a server from this list and click **Next**.

Step 6 On the **Server Roles** tab, do the following:

a) Select the **Active Directory Domain Services** if you intend to promote a domain controller.

b) In the **Add Features that are required for Active Directory Domain Services?** dialog box, ensure the following tools are listed and then click **Add Features**.

- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AS LS Tools
      - [Tools] AS DS Snap-Ins and Command-Line Tools
      - [Tools] Active Directory Administrative Center

Step 7 Select **DNS Server**.

Step 8 In the **Add Features that are required for DNS Server?** dialog box, ensure the following tools are listed and then click **Add Features**.

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] DNS Server Tools

Step 9 In the **Features** tab, ensure **Remote Server Administration Tools and Role Administration Tools** are selected and click **Next**.

Step 10 In the **AD DS** tab, click Next.

Step 11 In the **DNS Sever** tab, click Next.

Step 12 n the **Confirmation** tab, click Install.
The **Result** tab displays the progress of the DNS server installation.

Step 13 After the installation completes, click on the **Promote this server to a domain controller** link to make the server a domain controller.

Step 14 In the **Deployment Configuration** tab, select **Add a New Forest,** enter a valid fully qualified domain DNS name, and click **Next**.

Note Enter a valid domain name that adheres to the naming conventions listed at https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and

Step 15 In the **Domain Controller Options** tab, enter the following and click **Next**:

a) From the **Forest functional level** drop-down list, select Windows Server version based on your AD version.

b) From the **Domain functional level** drop-down list, select Windows Server version based on your AD version.

Note You can also choose to set the forest functional level to an older Windows Server version.

c) Ensure that the **Domain Name System (DNS) Server** and the **Global Catalog (GC)** check box is checked.

d) Set the **Directory Services Restore Mode** password.

Step 16 In the **Additional Options** tab, enter the **NetBios** name and click **Next**.

Step 17 In the **Paths** tab, enter the paths where you would like to store the database, log files, and SYSVOL.

Step 18 In the **Review Options** tab, click **Next**.

Step 19 In the **Prerequisites Check** tab, you can read through the warning if any and click **Install**.
The **Results** page displays whether the installation was a success. The server will automatically reboot in 10 minutes.

Configure DNS Server

Procedure

Step 1 Navigate to **Start** > **Administrative Tools** > **DNS**.

Step 2 Expand the **Server** on Left side pane.

Step 3 Right-click on Forward Lookup Zones and Click **New Zone**.

Step 4 In the New Zone Wizard, Click **Next**.

Step 5 In the Zone type window, choose **Primary zone**. Click **Next**.

Step 6 In the Zone Name window, Enter the *Fully qualified DNS name*. Click **Next**.

Step 7 In Zone File window, Choose **Create a new file with this file name**. Click **Next**.

Step 8 In the Dynamic Update window, Choose **Do not allow dynamic updates**. Click **Next**

Step 9 Click **Finish**.

Step 10 Right-click on Reverse Lookup Zones and Click **New zone**.

Step 11 In the New Zone Wizard, Click **Next**

Step 12 In the Zone type window, choose **Primary zone**. Click **Next**.

Step 13 In the Reverse Lookup Zone Name, choose **IPv4 Reverse Lookup Zone**. Click **Next**.

Step 14 Enter the *first three octets of IP address* in **Network** field. Click **Next**.

Note For Small Contact Center deployment model customer needs to add reverse lookup zone for both shared and Internal IP's, only if customer is using shared DNS for finesse Installation.

Example:

Create Reverse Lookup zone for 10.10.10.X (Shared IP) and 20.20.20.X (Internal IP).

Step 15 In Zone File window, Choose **Create a new file with this file name**. Click **Next**.

Step 16 In the Dynamic Update window, Choose **Do not allow dynamic updates**. Click **Next**.

Step 17 Click **Finish**.

Configure Host in DNS Server

Procedure

Step 1 Navigate to **DNS Manager**.

Step 2 Right click on the **Forward domain zone**. Select **New Host (A or AAAA)**.

Step 3 Enter Host Name.

Step 4 Enter IP address of the host.

Step 5 Check the **Create associated pointer (PTR) Record** check box. Click **Add host**.

Step 6 Click **Ok**. Click **Done**

Note For Small Contact Center Deployment model, if the customer is using shared DNS for finesse installation perform the following steps:

a. Add finesse internal IP (not the natted IP) in both Forward and Reverse lookup zone of shared DNS.

b. Add the unique finesse hostname in DNS server where ip address can be same.

c. After successfull installation of finesse primary and secondary, remove the host entry from Reverse look up zone of finesse internal IP.

d. Add the natted IP for finesse hostname in the DNS server, this supports SSO.

Note Live Data is not supported with shared DNS configuration for dedicated sub-customer option.

e. The OS customization of Finesse servers for all sub customers should be done in sequential manner not in parallel.

Configure CUBE Enterprise for Small Contact Center Deployment Model

Configure VRF

The Multi-VRF feature allows you to configure and maintain more than one instance of routing and forwarding tables within the same CUBE device and segregate voice traffic based on the VRF.

Configure VRF for Sub-customer 1:

```
ip vrf SUB-Customer1
rd 20.20.20.10:1
```

This creates a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y)

Configure VRF for Sub-customer 2:

```
ip vrf SUB-Customer2
rd 20.20.20.10:2
```

Assign Interface to VRF

To assign an interface to the VRF, perform the following instructions :

```
interface GigabitEthernet2
 ip vrf forwarding Customer1
```

Associates the VRF with the interface. If there is an IP address associated with the interface, it will be cleared and you will be prompted to assign the IP address again.

```
 ip address 10.10.10.5 255.255.255.0
```

Configure Global Settings

```
 voice service voip
 no ip address trusted authenticate
```

```
 address-hiding
 mode border-element
```

Configure Codec List

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

Configure Default Services

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

Configure VRF Specific RTP Port Ranges

For VoIP RTP connections, you can configure each VRF to have its own set of RTP port range under voice service VoIP. A maximum of ten VRF port ranges are supported. Different VRFs can have overlapping RTP port range.

The VRF based RTP port range limits, including the minimum and maximum port numbers, are the same as the global RTP port range. All the three port ranges, global, media-address, and VRF based can coexist on CUBE. The preference order of the RTP port allocation is as follows:

- VRF based port range
- Media-address based port range
- Global RTP port range

```
 media-address voice-vrf SUB-Customer1 port-range 25000 28000
 media-address voice-vrf SUB-Customer2 port-range 25000 28000
```

Configure IP Route

```
ip route vrf SUB-Customer1 0.0.0.0 0.0.0.0 20.20.20.1
ip route vrf SUB-Customer2 0.0.0.0 0.0.0.0 20.20.20.1
```

Configure Dial Peer

Control and media on a dial-peer have to bind with same VRF. Else, while configuring, the CLI parser will display an error.

Configure Incoming Dial Peer for CVP

```
dial-peer voice 23991 voip
 description Incoming dial-peer for CVP
 service survivability
 session protocol sipv2
 session transport udp
 incoming called-number .T
 voice-class codec 1
 voice-class sip rel1xx disable
 voice-class sip bind control source-interface GigabitEthernet1
```

```
voice-class sip bind media source-interface GigabitEthernet1
dtmf-relay rtp-nte
```

Configure Outbound Dial Peer for CVP

```
dial-peer voice 1001 voip
description outgoing dial-peer for CVP
translation-profile outgoing strip-digit
destination-pattern .T
session protocol sipv2
session target ipv4:10.10.10.10
session transport udp
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet1
voice-class sip bind media source-interface GigabitEthernet1
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```

Configure Incoming Dial Peer for Sub-customer1 VRF1

```
dial-peer voice 21991 voip
description "Incoming Dial-peer for VRF1"
service survivability
session protocol sipv2
session transport udp
incoming called-number [12][03][27].......
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.100
voice-class sip bind media source-interface GigabitEthernet2.100
dtmf-relay rtp-nte
```

Incoming Dial Peer for Sub-customer2 VRF2

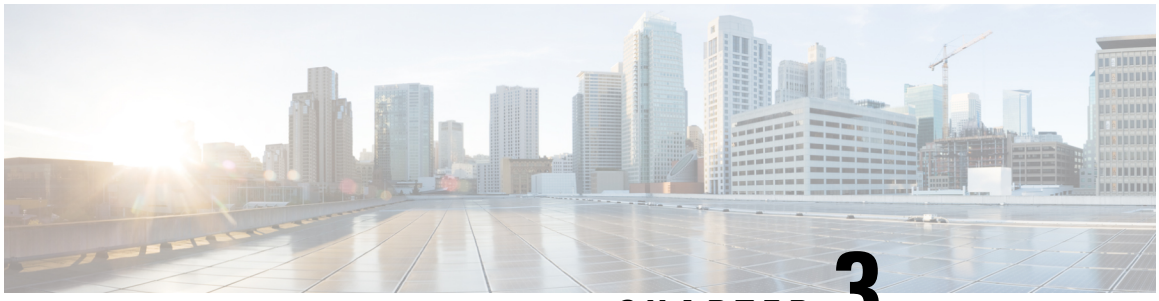
```
dial-peer voice 22991 voip
description "Incoming dial-peer for VRF2"
service survivability
session protocol sipv2
session transport udp
incoming called-number 1[03][16].......
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet3
voice-class sip bind media source-interface GigabitEthernet3
dtmf-relay rtp-nte
```

Configure Dial-Peer for Sub-customer1 VRF1

```
dial-peer voice 21001 voip
description from CVP towards VRF1 to CUCM Sub-Customer1
destination-pattern 101....
session protocol sipv2
session target ipv4:20.20.20.31
session transport udp
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.100
voice-class sip bind media source-interface GigabitEthernet2.100
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```

Configure Dial-Peer for Sub-customer2 VRF2

```
dial-peer voice 22001 voip
description from CVP towards VRF2 to CUCM Sub-Customer2
destination-pattern 201....
session protocol sipv2
session target ipv4:20.20.20.31
session transport udp
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.200
voice-class sip bind media source-interface GigabitEthernet2.200
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```



CHAPTER 3

Integration of Customer Instance with Shared Management

Certificates for Unified Contact Center Enterprise Web Administration

Note

- You must import self-signed certificates of solution components into the AW machines, if you are not using CA-signed certificates.
- Make sure that the certificates in the keystore pertain to the fully qualified domain name (FQDN) of the servers. If you have changed the domain name or hostname, be sure to update the certificates in the keystore.

CA Certificates

The following table outlines the CA certificate tasks for each component.

Components	Tasks
Unified CCE Components	1. Generate CSR, on page 133 2. Create Trusted CA-Signed Server or Application Certificate , on page 133 3. Upload and Bind CA-Signed Certificate, on page 135
Customer Voice Portal (CVP) Call Server/CVP Reporting Server[1]	See *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html
Email and Chat	See *Enterprise Chat and Email Installation and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html
Cisco Unified Communications Manager (CUCM)	See *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html
Cisco Unified Intelligence Center (CUIC)	Obtain and Upload Third-party CA Certificate, on page 141
Cisco Finesse	See *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html Deploy Certificate in Browsers, on page 100
Live Data	Obtain and Upload Third-party CA Certificate, on page 141
Cisco Identity Service (IdS)	1. From the IdS server, generate and download a Certificate Signing Requests (CSR). 2. Obtain Root and Application certificates from the third-party vendor. 3. Upload the appropriate certificates to the IdS server. For more information, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html. Ensure to run the instructions in IdS server.
Cloud Connect	Obtain and Upload Third-party CA Certificate, on page 141
Virtualized Voice Browser (VVB)	See *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html

Components	Tasks
Customer Collaboration Platform	See *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

[1] CA certificate instructions for CVP Reporting Server are similar to CVP call server.

Generate CSR

This procedure explains how to generate a Certificate Signing Request (CSR) from Internet Information Services (IIS) Manager.

Procedure

Step 1 Log in to Windows and choose **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

Step 2 In the **Connections** pane, click the server name.
The server **Home** pane appears.

Step 3 In the **IIS** area, double-click **Server Certificates**.

Step 4 In the **Actions** pane, click **Create Certificate Request**.

Step 5 In the **Request Certificate** dialog box, do the following:

a) Specify the required information in the displayed fields and click **Next**.
b) In the **Cryptographic service provider** drop-down list, leave the default setting.
c) From the **Bit length** drop-down list, select 2048.

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

Create Trusted CA-Signed Server or Application Certificate

You can create CA-signed certificate in any one of the following ways:

- Create certificate internally. Do the following:
  1. Set up Microsoft Certificate Server for Windows Server, on page 142
  2. Download the CA-signed certificate on each component server. Do the following:
     a. Open the CA server certificate page (*https://<CA-server-address>/certsrv*).
     b. Click **Request a Certificate** and then click **advanced certificate request**. Then do the following:
        1. Copy the Certificate Request content in the **Base-64-encoded certificate request** box.
        2. From the **Certificate Template** drop-down list, choose Web Server.
        3. Click **Submit**.
        4. Choose **Base 64 encoded**.
        5. Click **Download certificate** and save it to the desired destination folder.

c. On the CA server certificate page, click **Download a CA Certificate, Certificate Chain, or CRL**, and then do the following:

1. Select the Encoding method as **Base 64**.
2. Click **Download CA Certificate** and save it to the desired destination folder.

3. Import the Root CA and Intermediate Authority certificates into Windows trust store of every component. For more information on how to import CA certificates into Windows trust store, see *Microsoft* documentation.
4. Import the Root CA and Intermediate Authority certificates into Java keystore of every component. For more information, see Import CA Certificate into AW Machines, on page 134.

- Obtain certificate from a trusted Certificate Authority (CA). Do the following:

1. Send the CSR to a trusted Certificate Authority (CA) for sign-off.
2. Obtain the CA-signed application certificate, Root CA certificate, and Intermediate Authority certificate (if any).
3. Import the Root CA and Intermediate Authority certificates into Windows trust store of every component. For more information on how to import CA certificates into Windows trust store, see *Microsoft* documentation.
4. Import the Root CA and Intermediate Authority certificates into Java keystore of every component. For more information, see Import CA Certificate into AW Machines, on page 134.

Import CA Certificate into AW Machines

Procedure

Step 1 Log in to the AW-HDS-DDS Server.

Step 2 Run the following command:

```
cd %JAVA_HOME%\bin
```

Step 3 Copy the Root or intermediate certificates to a location in AW Machine.

Step 4 Run the following command and remove the existing certificate:

```
keytool.exe -delete -alias <AW FQDN> -keystore ..\lib\security\cacerts
```

Step 5 Enter the truststore password when prompted.

The default truststore password is **`changeit`**.

Note To change the truststore password, see Change Java Truststore Password, on page 143.

Step 6 At the AW machine terminal, run the following command:

- `cd %JAVA_HOME%\bin`
- `keytool -import -file <path where the Root or intermediate certificate is stored> -alias <AW FQDN> -keystore ..\lib\security\cacerts`

Step 7 Enter the truststore password when prompted.

Step 8 Go to Services and restart Apache Tomcat.

Upload and Bind CA-Signed Certificate

Upload CA-Signed Certificate to IIS Manager

This procedure explains how to upload a CA-Signed certificate to IIS Manager.

Before you begin

Ensure that you have the Root certificate, and Intermediate certificate (if any).

Procedure

Step 1 Log in to Windows and choose **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

Step 2 In the **Connections** pane, click the server name.

Step 3 In the **IIS** area, double-click **Server Certificates**.

Step 4 In the **Actions** pane, click **Complete Certificate Request**.

Step 5 In the **Complete Certificate Request** dialog box, complete the following fields:

a) In the **File name containing the certification authority's response** field, click the **…** button.
b) Browse to the location where signed certificate is stored and then click **Open**.
c) In the **Friendly name** field, enter the FQDN of the server.

Step 6 Click **OK** to upload the certificate.
If the certificate upload is successful, the certificate appears in the **Server Certificates** pane.

Bind CA-Signed Certificate to IIS Manager

Bind CCE Web Applications

This procedure explains how to bind a CA Signed certificate in the IIS Manager.

Procedure

Step 1 Log in to Windows and choose **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

Step 2 In the **Connections** pane, choose **<server_name>** > **Sites** > **Default Web Site**.

Step 3 In the **Actions** pane, click **Bindings...**.

Step 4 Click the type **https** with port 443, and then click **Edit...**.

Step 5 From the **SSL certificate** drop-down list, select the uploaded signed Certificate Request.

Step 6 Click **OK**.

Step 7 Navigate to **Start** > **Run** > **services.msc** and restart the IIS Admin Service.

If IIS is restarted successfully, certificate error warnings do not appear when the application is launched.

Bind Diagnostic Framework Service

This procedure explains how to bind a CA Signed Certificate in the Diagnostic Portico.

Procedure

Step 1 Open the command prompt.

Step 2 Navigate to the Diagnostic Portico home folder using:

cd <ICM install directory>:\icm\serviceability\diagnostics\bin

Step 3 Remove the current certificate binding to the Diagnostic Portico tool using:

DiagFwCertMgr /task:UnbindCert

Step 4 Open the signed certificate and copy the hash content (without spaces) of the Thumbprint field. Run the following command:

DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>

If certificate binding is successful, it displays "The certificate binding is VALID" message.

Step 5 Validate if the certificate binding was successful using:

DiagFwCertMgr /task:ValidateCertBinding

Note DiagFwCertMgr uses port 7890 by default.

If certificate binding is successful, it displays "The certificate binding is VALID" message.

Step 6 Restart the **Diagnostic Framework** service by running the following command:

sc stop "diagfwsvc"

sc start "diagfwsvc"

If Diagnostic Framework restarts successfully, certificate error warnings do not appear when the application is launched.

Self-Signed Certificates

The following table lists components from which self-signed certificates are generated and components into which self-signed certificates are imported.

Note To establish a secure communication, run the commands (given in the links below) in the Command Prompt as an Administrator (right click over the **Command Prompt** and select **Run as administrator**).

Import Self-signed Certificates to Target Server	Generate Self-signed Certificates from Source Component Server	Links
AW Machines	Unified CCE Components (Router, Logger[2], Rogger[3], PGs, and HDS)	Import CCE Component Certificates, on page 137 Import Diagnostic Framework Portico Certificate into AW Machines, on page 138
	Cisco Finesse	Import VOS Components Certificate, on page 139
	Cisco Unified Intelligence Center (CUIC) Publisher and Subscriber	
	Cisco Identity Service (IdS) Publisher and Subscriber	
	Cloud Connect	
	Customer Collaboration Platform	
Logger	AW	Import CCE Component Certificates, on page 137
Rogger		

[2] Router and Logger are applicable only for 12000 Agent deployments.
[3] Applicable only for 2000 and 4000 Agent deployments.

Related Topics

Import CCE Component Certificates, on page 137
Import Diagnostic Framework Portico Certificate into AW Machines, on page 138

Import CCE Component Certificates

This procedure explains how to import self-signed certificates from a source CCE component sever to a target server.

Important The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the CCE components in the CCE Inventory.

Procedure

Step 1 Log in to the required CCE component server.

Step 2 From the browser (*https://<FQDN of the CCE component server>*), download the certificate.

If you want to regenerate a certificate instead of using the existing certificate, run the following commands:

a) From the **Cisco Unified CCE Tools** folder, launch the **SSL Encryption Utility**.
b) Go to the **Certificate Administration** tab and click **Uninstall**.

c) Click **Yes** to confirm uninstallation of certificate.

A message is displayed upon successful uninstallation of the certificate.

d) Click **Install** to generate a new certificate.

Step 3 Copy the certificate to a location in the target server.

Step 4 Run the following command at the target server (machine terminal):

- `cd %JAVA_HOME%\bin`
- `keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of component Server> -keystore ..\lib\security\cacerts`

Step 5 Enter the truststore password when prompted.

The default truststore password is **changeit**.

Note To change the truststore password, see Change Java Truststore Password, on page 143.

Step 6 Go to Services and restart Apache Tomcat on target servers.

Import Diagnostic Framework Portico Certificate into AW Machines

Generate Diagnostic Framework Portico self-signed certificate on each CCE component server and import them into all AW Machines.

Procedure

Step 1 Log in to the CCE component server.

Step 2 From the Cisco Unified CCE Tools, open the Diagnostic Framework Portico.

Step 3 Download the self-signed certificate from the browser.

Step 4 Copy the certificate to a location in AW Machine.

Step 5 Run the following command at the AW machine terminal:

- `cd %JAVA_HOME%\bin`
- `keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of the CCE component Server> -keystore ..\lib\security\cacerts`

Note The alias name of the CCE component server must be different from the alias name given while creating the CCE component server's self-signed certificate.

Step 6 Enter the truststore password when prompted.

The default truststore password is **changeit**.

Note To change the truststore password, see Change Java Truststore Password, on page 143.

Step 7 Go to Services and restart Apache Tomcat.

Import VOS Components Certificate

This procedure explains how to import self-signed certificates from a source VOS component sever to a target server.

Important The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the respective component servers in the CCE Inventory.

Procedure

Step 1 Sign in to the **Cisco Unified Operating System Administration** on the source component server using the URL (*https://<FQDN of the Component server>:8443/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 not on the list, click **Generate Self-signed**. When the certificate generation is complete, reboot your server.
- 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.)

Step 5 Download the self-signed certificate that contains hostname of the primary server.

Step 6 Copy the certificate to a location in the target server.

Step 7 Run the following command as an administrator at the target server (machine terminal):

- `cd %JAVA_HOME%\bin`
- `keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of component Server> -keystore ..\lib\security\cacerts`

Step 8 Enter the truststore password when prompted.

The default truststore password is **`changeit`**.

Step 9 Go to Services and restart Apache Tomcat.

Certificates for Live Data

Certificates and Secure Communications

For secure Cisco Finesse, Cisco Unified Intelligence Center, and Live Data server-to-server communication, perform any of the following:

- Use the self-signed certificates provided with Live Data.

Note When using 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.

- Obtain and install a Certification Authority (CA) certificate from a third-party vendor.
- Produce a Certification Authority (CA) certificate internally.

Self-Signed Certificates and Third-Party CA Certificates

For secure Cisco Finesse, Cisco Unified Intelligence Center, and Live Data server-to-server communication, you must set up security certificates (Applicable for both Self-Signed and Third-Party CA Certificates):

- For Cisco Finesse and Cisco Unified Intelligence Center servers to communicate with the Live Data server, you must to import the Live Data certificates and Cisco Unified Intelligence Center certificates into Cisco Finesse, and the Live Data certificates into Cisco Unified Intelligence Center.

On Server	Import Certificates From
Finesse	Live Data and Cisco Unified Intelligence Center
Live Data	None
Cisco Unified Intelligence Center	Live Data

Export Self-Signed Live Data Certificates

Live Data installation includes the generation of 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 Live Data and Cisco Unified Intelligence Center, as described in this procedure. You must export from both Side A and Side B of the Live Data and Cisco Unified Intelligence Center servers. You must then import the certificates into Finesse, importing both Side A and Side B certificates into each side of the Finesse servers.

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 you are using self-signed certificate, do the following:
  a. Click **Generate New**.

b. When the certificate generation is complete, restart the Cisco Tomcat service and the Cisco Live Data NGNIX service.

c. Restart this procedure.

Step 5 Click **Download .pem file** and save the file to your desktop.

Be sure to perform these steps for both Side A and Side B.

Step 6 After you have downloaded the certificates from Cisco Unified Intelligence Center, sign in to Cisco Unified Operating System Administration on the Live Data server (http://hostname of LiveData server/cmplatform), and repeat steps 2 to 5. This is applicable only for Standalone LiveData.

What to do next

You must now import the Live Data and Cisco Unified Intelligence Center certificates into the Finesse servers.

Import Self-Signed Live Data Certificates

To import the certificates into the Finesse servers, use the following procedure.

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration on the Finesse server using the following URL:

http://*FQDN of Finesse server*:8443/cmplatform

Step 2 From the **Security** menu, select **Certificate Management**.

Step 3 Click **Upload Certificate**.

Step 4 From the **Certificate Name** drop-down list, select **tomcat-trust**.

Step 5 Click **Browse** and browse to the location of the Cisco Unified Intelligence Center certificate (with the **.pem** file extension).

Step 6 Select the file, and click **Upload File**.

Step 7 After you have uploaded the Cisco Unified Intelligence Center certificate repeat steps 3 to 6 for Live Data certificates.This is applicable only for standalone Live Data.

Step 8 After you upload both the certificates, restart Cisco Finesse Tomcat on the Finesse server.

What to do next

Be sure to perform these steps for both Side A and Side B.

Obtain and Upload Third-party CA Certificate

You can use a Certification Authority (CA) certificate provided by a third-party vendor to establish an HTTPS connection between the Live Data, Cisco Finesse, Cisco Unified Intelligence Center servers, and Cloud Connect servers.

To use third-party CA certificates:

- From the **Cisco Unified Operating System Administrator** of Live Data, Cisco Finesse, Cisco Unified Intelligence Center, and Cloud Connect servers, generate and download a Certificate Signing Requests (CSR).
- Obtain root and application certificates from the third-party vendor.
- Upload the appropriate certificates to the Live Data, Unified Intelligence Center, Cisco Finesse, and Cloud Connect servers.

Follow the instructions provided in the *Unified CCE Solution: Procedure to Obtain and Upload Third-Party CA certificates (Version 11.x)* technical note 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 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**, **Certification Authority Web Enrollment**, **Certificate Enrollment Web Service**, and **Certificate Enrollment Policy Web Service** boxes are 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**, **Certification Authority Web Enrollment**, **Certificate Enrollment Web Service**, and **Certificate Enrollment Policy Web Service** boxes 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 In the following tabs, leave the default values, and click **Next**.

a. **CA for CES**

b. **Authentication Type for CES**

c. **Service Account for CES**

d. **Authentication Type for CEP**

Step 16 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.

Change Java Truststore Password

This procedure explains how to change a truststore password in a Windows machine.

Procedure

Step 1 Log in to the Windows machine.

Step 2 Run the following command:

```
cd %JAVA_HOME%\bin
```

Step 3 Change the truststore password by running the following command:

```
keytool.exe -storepasswd -keystore ..\lib\security\cacerts
Enter keystore password:  <old-password>
New keystore password:  <new-password>
Re-enter new keystore password:  <new-password>
```

Single Sign-on Integration

Establish Trust Relationship for Cisco IdS

To enable applications to use Cisco Identity Service (Cisco IdS) for Single Sign-On, perform the metadata exchange between the Cisco IdS and the Hosted Identity Provider (IdP).

- Download the SAML SP Metadata file, `sp.xml`, on the Cisco IdS publisher primary node.
  1. Open Identity Service Management by doing either of the following:
     - Open the Identity Service Management window: `https://<Unified CCX server address>:8553/idsadmin`.
     - In Administration, navigate to **System** > **Single Sign-On** and click **Identity Service Management**.
  2. On the **Settings** > **IdS Trust** tab, download the SAML SP Metadata file, `sp.xml`.
- Download the Identity Provider Metadata file, federationmetadata.xml, from the IdP. For example,
  1. For AD FS, download the Identity Provider Metadata file from the IdP at the location:

     `https://<ADFSServer FQDN>/federationmetadata/2007-06/federationmetadata.xml`.
  2. On the **Identity Service Management** page, upload the Identity Provider Metadata file that was downloaded in the previous step.

The SAML SSO uses trust authentication certificates to exchange authentication and authorization details between the IdP (such as AD FS) and the Cisco IdS. This secures the communication between the servers.

Note

- Cisco IdS supports SAML self-signed certificates for authentication.
- If the IdP certificates are automatically rolled-over, manually renewed, or updated by the administrator, then re-establish the trust relationship between the IdS and the IdP.

Integrate the Customer Instance to the Shared ADFS

Integrate Cisco IdS to the Shared Management AD FS

Procedure

Step 1 In AD FS, be sure that the default Authentication Type is set to Forms. (Cisco Identity Service requires the Identity Provider to provide form-based authentication.) See the Microsoft AD FS documentation for details.

Step 2 In AD FS server, open **AD FS Management**.

Step 3 Right-click **AD FS** -> **Trust Relationships** -> **Relying Party Trust**.

Step 4 From the menu, choose **Add Relying Party Trust** to launch the **Add Relying Party Trust Wizard**.

Step 5 In the **Select Data Source** step, choose the option **Import data about the relying party from a file**.

Step 6 **Browse** to the `sp.xml` file that you downloaded from Cisco Identity Server and complete the import to establish the relying party trust.

Step 7 Select the step **Specify Display Name**, and add a significant name you can use to identify the Relying Party Trust.

Step 8 For AD FS in Windows Server, select the option **I do not want to configure multi-factor authentication settings for the relying party at this time** in the Step **Configure Multi-factor Authentication Now**.

Step 9 In the Step Choose Issuance Authorization Rules, select the option **Permit all users to access this relying party** and click **Next**.

Step 10 Click **Next** again to finish adding the relying party.

Step 11 Right-click on the **Relying Party Trust** and click **Properties**. Select the **Identifiers** tab.

Step 12 On the **Identifiers** tab, configure the following:

Field	Description
Display name	The unique name of the identifier.
Relying party identifier	FQDN of the publisher node of Cisco Identity Server from which you downloaded the Cisco IdS metadata file.
	FQDN of the subscriber node of Cisco Identity Server.

Step 13 Still in **Properties**, select the **Advanced** tab.

Step 14 Select **secure hash algorithm** as **SHA-1** and then click **OK**.

Note In the following steps, you configure two claim rules to specify the claims that are sent from AD FS to Cisco Identity Service as part of a successful SAML assertion:

- A claim rule with the following custom claims, as AttributeStatements, in the assertion:
  - **uid** - Identifies the authenticated user in the claim sent to the applications.
  - **user_principal** - Identifies the authentication realm of the user in the assertion sent to Cisco Identity Service.
- A second claim rule that is a NameID custom claim rule specifying the fully qualified domain name of the AD FS server and the Cisco IdS server.

Follow the steps to configure these rules.

Step 15 In **Relying Party Trusts**, right-click on the Relying Party Trust you created, and click **Edit Claim Rules**.

Step 16 Follow these steps to add a rule with **Send LDAP Attributes as Claims** as the Claim rule template.

a) In the **Issuance Transform Rules** tab, click **Add Rule**.
b) In the Step **Choose Rule Type**, select the claim rule template **Send LDAP Attributes as Claims** and click **Next**.
c) In the **Configure Claim Rule** step, in the **Claim rule name** field, enter **NameID**.
d) Set the **Attribute store** drop-down to **Active Directory**.

e) Set the table **Mapping of LDAP attributes to outgoing claim types** to the appropriate **LDAP Attributes** and the corresponding **Outgoing Claim Type** for the type of user identifier you are using:

- When the identifier is stored as a **SAM-Account-Name** attribute:
  1. Select an **LDAP Attribute**of **SAM-Account-Name**, and set the corresponding **Outgoing Claim Type** to **uid** (lowercase).
  2. Select a second **LDAP Attribute** of **User-Principal-Name** and set the corresponding **Outgoing Claim Type** to **user_principal** (lowercase).
- When the identifier is a UPN:
  1. Select an **LDAP Attribute**of **User-Principal-Name**, and set the corresponding **Outgoing Claim Type** to **uid** (lowercase).
  2. Select a second **LDAP Attribute** of **User-Principal-Name** and set the corresponding **Outgoing Claim Type** to **user_principal** (lowercase).

Note The SAM-Account-Name or UPN choice is based on the User ID configured in the AW.

Step 17 Follow these steps to add a second rule with the template **custom claim rule**.

a) Select **Add Rule** on the **Edit Claim Rules** window.
b) Select **Send Claims Using Custom Rule**.
c) Set the name of rule to the **fully qualified domain name (FQDN)** of the Cisco Identity Server publisher (primary) node.
d) Add the following rule text:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 =>
 issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
 Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
 Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
 =
 "http://<AD FS Server FQDN>/adfs/services/trust",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
 =
 "<fully qualified domain name of Cisco IdS>");
```

e) Edit the script as follows:

- Replace **<ADFS Server FQDN>** to match exactly (including case) the ADFS server FQDN (fully qualified domain name.)
- Replace **<Cisco IdS server FQDN>** to match exactly (including case) the Cisco Identity Server FQDN.

Step 18 Add the following rules for Federated Scenario:

a) Add the rule for Name ID:

- In the **Issuance Transform Rules** tab, click **Add**.

- Select the claim rule template as **Pass Through or Filter an Incoming Claim**.
- In the **Configure Claim Rule** field, enter the claim rule name.
- Select **Incoming Claim type** to **Name ID**.
- Select Incoming name_ID format to Transient Identifier, then click **Finish**.

b) Add the rule for uid:

- In the **Issuance Transform Rules** tab, click **Add**.
- Select the claim rule template as **Pass Through or Filter an Incoming Claim**.
- In the **Configure Claim Rule** field, enter the claim rule name.
- In the **Incoming Claim type** field, enter **`uid`**, then click **Finish**.

c) Add the rule for user_principal:

- In the **Issuance Transform Rules** tab, click **Add**.
- Select the claim rule template as **Pass Through or Filter an Incoming Claim**.
- In the **Configure Claim Rule** field, enter the claim rule name.
- In the **Incoming Claim type** field, enter **`user_principal`**, then click **Finish**.

Step 19 Click **OK**.

Federate the Customer ADFS to the Shared Management ADFS

Add Claim Description for Customer ADFS

Procedure

Step 1 Open **AD FS Management Console**, select **Service** > **Claim Descriptions**.

Step 2 Right click **Claim Descriptions** and select **Add Claim Descriptions**.

Step 3 Create uid claim description:

a) Enter the display name as **`uid`**.
b) Enter the claim identifier as **`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/uid`**.
c) Check the **Publish this claim description in federation metadata as a claim type that this Federation Service can accept** check box.
d) Check the **Publish this claim description in federation metadata as a claim type that this Federation Service can send** check box, then click **OK**.

Step 4 Create user_principal claim description:

a) Enter the display name as **`user_principal`**.
b) Enter the claim identifier as **`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/user_principal`**.

c) Check the **Publish this claim description in federation metadata as a claim type that this Federation Service can accept** check box.
d) Check the **Publish this claim description in federation metadata as a claim type that this Federation Service can send** check box, then click **OK**.

Important After creating claim descriptions, update federation metadata of the claim provider trust in Hosted AD FS.

Add Claim Rules for Relying Party Trust in the Customer ADFS

Use this procedure to add the Claim rules for the Relying Party Trust in the Customer ADFS:

Procedure

Step 1 Open **AD FS Management Console**.

Step 2 Select **Trust Relationships** > **Relying Party Trusts**.

Step 3 Select and right click the appropriate Relying party trust, then select **Edit Claim Rules**.

Step 4 Add a rule with **Send LDAP Attributes as Claims** as the Claim rule template.

a) In the **Issuance Transform Rules** tab, click **Add Rule**. Select the claim rule template **Send LDAP Attributes as Claims**.
b) For **Configure Claim Rule**, set the rule name as **NameID**.
c) Select **Attribute store** to **Active Directory**.
d) Map the LDAP attribute **User-Principal-Name** to the **Outgoing Claim Type** of **user_principal** (lowercase).
e) Select one of the possible LDAP attributes that identifies application users and map it to **uid** (lowercase).

Note The rule that you create can use one of several possible LDAP attributes to identify the user. The exact mapping depends on which attribute the rule uses:

- When the identifier is stored as a **SAMAccountName** attribute:
  - The Outgoing Claim Type **uid** maps to the LDAP attribute **SAM-Account-Name**.
  - The Outgoing Claim Type **user_principal** maps to the LDAP attribute **User-Principal-Name**.
- When the identifier is a UPN:
  - The Outgoing Claim Type **uid** maps to the LDAP attribute **User-Principal-Name**.
  - The Outgoing Claim Type **user_principal** maps to the LDAP attribute **User-Principal-Name**.

Step 5 Add another rule with the template **custom claim rule**.

a) Select **Add Rule** on the **Edit Claim Rules** window.
b) Select **Send Claims Using Custom Rule**.
c) Set the name of rule to the **fully qualified domain name (FQDN)** of the Cisco Identity Server publisher (primary) node.
d) Add the following rule text:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 =>
 issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
 Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
 Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
 =
 "http://<AD FS Server FQDN>/adfs/services/trust",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
 =
 "<fully qualified domain name of Cisco IdS>");
```

- Set **<AD FS Server FQDN>** to match exactly (including case) the AD FS FQDN.
- Set **<fully qualified domain name of Cisco IdS>** to match exactly (including case) the Cisco Identity Server FQDN.

Step 6 Click **OK**.

Add Claim Rules for Claim Provider Trust in the Shared Management ADFS

Note Add the claim rules for Claim Provider Trust in Hosted (Shared Management) ADFS (the ADFS where Cisco IDS is registered).

Procedure

Step 1 Open **AD FS Management Console**.

Step 2 Select **Trust Relationships** > **Claim Provider Trusts**.

Step 3 Select and right click the appropriate Claims provider trust, then select **Edit Claim Rules**.

Step 4 In the **Acceptance Transform Rules** tab, click **Add**.

Step 5 Add the rule for Name ID:

a) Select the claim rule template as **Pass Through or Filter an Incoming Claim**.
b) In the **Configure Claim Rule** field, enter the claim rule name.
c) Select **Incoming Claim type** to **Name ID**.
d) Select Incoming name_ID format to Transient Identifier, then click **Finish**.

Step 6 Add the rule for uid:

a) Select the claim rule template as **Transform an Incoming Claim**.
b) In the **Configure Claim Rule** field, enter the claim rule name.
c) Select **Incoming Claim type** to **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/uid**.
d) Select **Outgoing Claim type** to **uid**, then click **Finish**.

Step 7 Add the rule for user_principal:

a) Select the claim rule template as **Transform an Incoming Claim**.

b) In the **Configure Claim Rule** field, enter the claim rule name.
c) Select **Incoming Claim type** to **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/user_principal**.
d) Select **Outgoing Claim type** to **`user_principal`**, then click **Finish**.

Optionally Customize the ADFS Sign-In Page in Windows Server to Hide Federated Domains List

Follow the procedure to automatically redirect the end-user to their organization. This is required when your Contact Center solution has multi-domain federations with partners and does not want to display the list of IdPs that it is federated with.

Procedure

Step 1 Open the **Windows Powershell** of Hosted AD FS.

Step 2 Enter the **`Set-ADFSClaimsProviderTrust -TargetName "<adfsCPName>" -OrganizationalAccountSuffix @("<mydomain>")`** command.

In the mentioned command, **<adfsCPName>** represents **AD FS Claim Provider Trust Name** and **<mydomain>** represents **Organization Domain Name**.

Enable Signed SAML Assertions

Enable Signed SAML Assertions for the Relying Party Trust (Cisco Identity Service).

Procedure

Step 1 Click **Start** and type **powershell** in the Search field to display the Windows Powershell icon.

Step 2 Right-click on the Windows Powershell program icon and select **Run as administrator**

Note All PowerShell commands in this procedure must be run in Administrator mode.

Step 3 Run the command, **Set-ADFSRelyingPartyTrust -TargetName <Relying Party Trust Display Name> -SamlResponseSignature "MessageAndAssertion"**.

Note Set <Relying Party Trust Display Name> to exactly match (including case) the Identifier tab of the Relying Party Trust properties.

For example:

```
Set-ADFSRelyingPartyTrust -TargetName CUICPub.PCCERCDN.cisco.com
-SamlResponseSignature "MessageAndAssertion".
```

Step 4 Navigate back to the Cisco Identity Service Management window.

Step 5 Click **Settings**.
By default **IdS Trust** tab is displayed.

Step 6 On the Download SAML SP Metadata and Upload IdP Metadata windows, click Next as you have already established trust relationship between IdP and IdS.

Step 7 On the AD FS authentication window, provide the login credentials.

Step 8 On successful SSO setup, the message "SSO Configuration is tested successfully" is displayed.

Note If you receive the error message "An error occurred", ensure that the claim you created on the AD FS is enabled.

If you receive the error message "IdP configuration error: SAML processing failed", ensure that the rule has the correct names for Ids and AD FS.

Unified CCDM Integration

Unified CCDM is generally hosted on shared management level across multiple customer instances. This chapter describes how to configure multiple customer instances from a shared Unified CCDM.

This section describes the following steps:

- Configure Unified CCE Servers in Unified CCDM Cluster, on page 151
- Configure Unified CVP Servers in Unified CCDM Cluster, on page 159
- Create Users in Active Directory, on page 161
- Configure Unified CCE for Partitioned Internet Script Editor, on page 161
- Deployment Specific Configurations, on page 163
- Configure IDP, on page 169

Configure Unified CCE Servers in Unified CCDM Cluster

Unified CCE components must be configured before Unified CCDM can connect to them for Provisioning. Complete the following procedures to configure Unified CCE for Unified CCDM connectivity

- Unified CCE Prerequisites, on page 151
- Setup Unified CCE Servers in Unified CCDM Cluster, on page 156
- Create an Equipment Mapping, on page 158

Unified CCE Prerequisites

Before you integrate Unified CCE with Unified CCDM, you must setup SQL agents and CMS server. Complete the following procedures for prerequisites configurations.

- Configure Unified CCE AW Database(AWDB) for Unified CCDM, on page 151
- Configure the Unified CCE AW for Provisioning, on page 152

Configure Unified CCE AW Database(AWDB) for Unified CCDM

Before configuring AWDB, ensure that you create a two-way trust relationship between forests if:

- your CCDM and the Unified CCE domains are in seperate forests
- your customer domains and Unified CCE domains are in seperate forests

- your customer domains and CCDM domains are in seperate forests

If you use SQL Server Authentication to connect Unified CCDM to

Unified CCE

, no configuration of the Administrative Workstation Database (AWDB) is required. If you do not use the SQL authentication, you must configure the AWDB to connect the Unified CCDM to Unified CCE.

Complete the following procedure to configure AWDB:

Procedure

Step 1 Log in to the Unified CCE Admin Workstation Server with local administrative privileges.

Step 2 Open **SQL Server Management Studio** and click **Connect** to establish connection with the server.

Step 3 Expand **Security** folder and choose **Logins**.

Step 4 Right-click Logins and choose **New Logins**.

Step 5 To add SQL logins for both the Side A and Side B Unified CCDM Servers (this includes Web server, CCDM Domain administrator and Database server on both the sides).

Configure the General page as follows:

a. In the Login Name field, enter the name for the machine in the following format: <DOMAIN>\<Unified CCDM-HOSTNAME>$.

b. Choose Windows Authentication unless you are connecting to a server on another domain.

c. Select Default language as **English**.

Configure the User Mapping page as follows:

a. In the Users mapped to this login field, check hcs_awdb database.

b. In the Database role membership for field, check the following roles to grant to the AWDB login: **public** and **db_datareader**.

Step 6 Click **OK**.

Step 7 Repeat steps 1 to 6 for Side B if Unified CCE AW server is dual-sided.

Configure the Unified CCE AW for Provisioning

For each Unified CCE instance that Unified CCDM Resource Management connects to must meet the following criteria:

-
- Configure an Application Instance on the Unified CCE distributor machine (AW) for Unified CCDM to connect to Unified CCE. Configure the Application Instance with Application Type as **Cisco Voice**.

Note The application instance for CCDM is provided as part of the load base configuration. For more information, see Application Instance List from Load Base Configuration, on page 30. The default name of the Application Instance is **CCDM** as per the Load Base configuration.

- If the AW is dual-sided, each Unified CCE AW must connect to a different RMI registry port on the Unified CCDM Database Server.

Each Unified CCE instance requires a distinct primary distributor AW to connect to Unified CCDM resource management.

Set Up CMS Server on Unified CCE

A new application connection must be defined on each configured Unified CCE

instance for each Database Server. This ensures that in a dual-sided system, the alternate side can also connect to the Unified CCE in a failover scenario.

Complete the following procedure to set up the Configuration Management Service (CMS) server on each Unified CCE:

Before you begin

Before configuring the Unified CCDM server cluster you must ensure that the CMS Server(s) are set up correctly on each Unified CCE for each Unified CCDM Database Server. Firstly, check that the CMS Node option was selected when the Admin Workstation was configured. You can determine if this was the case by looking for a cmsnode and a cms_jserver process running on the Unified CCE.

Procedure

Step 1 In Unified CCE Admin Workstation Server Side A, open **CMS Control** application.

Step 2 Under **Application** tab, click **Add** and configure the following in the **Application Connection Details** page.

a) **Administration & Data Server Link** - Enter the name of the Unified CCDM Database Server. This should be in all capital letters, with Server appended, for example, CCDMDBServer.

b) **Administration & Data Server RMI Registry Port** - Enter the Unified CCE AW port number for the Unified CCDM provisioning service to connect to. This is usually 2099. If the Unified CCDM provisioning service connects to multiple Unified CCE instances, it is required that each instance should use a different port.

When you configure CMS server onUnified CCE at Side B, use a different RMI registry port.

c) **Application link** - Enter the name of the Unified CCDM Database Server. This should be in all capital letters, with Client appended, for example, CCDMDBClient.

d) **Application RMI registry port** - Enter the Unified CCDM Database Server port number for the Unified CCE AW to connect to.

This should be rather the same as for the Administration & Data Server RMI Registry Port. Each Unified CCE AW must connect to a different port on the Unified CCDM Database Server. You should record this information for future use.

e) **Application host name**- Enter the server name, for example, Unified CCDM.
f) Click **OK** to save the changes and to close the **Application Connection Details**.

Step 3 Click **OK** to save your changes and to close the **CMS Control Console**.

Step 4 Repeat steps 1-3 to set up CMS Server on Cisco Unified CCE Admin Workstation Server (Side A) for Unified CCDM Database Server Side B.

Enure that you use the same ports used for Side A Unified CCDM Database Server under **Application Connection Details**.

Note If the CMS JServer process fails to connect Unified CCDM, restart the Unified CCE Enterprise Distributor service.

Create Conditional Forwarders for Customer Domain

Complete the following procedure to create conditional forwarder.

Before you begin

Note You need to complete this procedure only for Cisco Hosted Collaboration Solution for Contact Center deployments.

Procedure

Step 1 Go to DNS Manager.
Step 2 Click the **Conditional Forwarder**.
Step 3 Right-click and select **New Conditional Forwarder**.
Step 4 Enter the DNS domain name.
Step 5 In the IP address field, click and enter the NAT IP address of the Service Provider domain.
Step 6 Click **OK**.

Create Forwarders for Customer Domain

Complete the following procedure to create forwarders.

Before you begin

Note You need to complete this procedure only for Cisco Hosted Collaboration Solution for Contact Center deployments.

Procedure

Step 1 Go to DNS Manager.
Step 2 Right-click the domain name.
Step 3 Click **Properties**.
Step 4 Click the **Forwarders** tab and then click **Edit**.
Step 5 In the IP address field, click and enter the NAT IP address of the Service Provider domain.
Step 6 Click **OK** to create forwarders and then click **Apply** and **Ok**.

Create Conditional Forwarders for Service Provider Domain

Complete the following procedure to create conditional forwarder.

Procedure

Step 1 Go to DNS Manager.
Step 2 Click the **Conditional Forwarder**.
Step 3 Right-click and select **New Conditional Forwarder**.
Step 4 Enter the DNS domain name.
Step 5 In the IP address field, click and enter the NAT IP address of the customer domain.
Step 6 Click **OK**.

Create Forwarders for Service Provider Domain

Procedure

Step 1 Go to DNS Manager.
Step 2 Right-click the **Domain Name**.
Step 3 Click **Properties**.
Step 4 Click the **Forwarders** tab and then click **Edit**.
Step 5 In the IP address field, click and enter the NAT IP address of the customer domain.
Step 6 Click **OK** to create forwarders and then click **Apply** and **Ok**.

Create Two-Way Forest Trust

Complete the following procedure from the customer domain controller to create a two-way forest trust:

Procedure

Step 1 Right-click the domain under the **Active Directory Domains and Trusts**.

Step 2 Click **Properties**.

Step 3 Click the **Trust** tab and then click **New Trust**.

Step 4 Click **Next**.

Step 5 Enter the service provider domain name and click **Next**.

Step 6 Select the **Forest Trust** option and click **Next**.

Step 7 Select the option **Two-way Trust** and click **Next**.

Step 8 Select the option **Both this domain and specified domain** and click **Next**.

Step 9 Enter the authentication username for the customer and a password for the specified domain and click **Next**.

You must have the administrator privileges to create the trust.

Step 10 Select the option **Forest-wide authentication** and then click **Next** until you reach Confirm Outgoing Trust.

Step 11 Select the option **Yes, confirm the outgoing trust**, and click **Next**.

Step 12 Select the option **Yes, confirm the incoming trust**, and click **Next**.

Step 13 Click **Finish**.

Launch the Integrated Configuration Environment

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

Procedure

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

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

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

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

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

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

Setup Unified CCE Servers in Unified CCDM Cluster

Complete the following procedure to configure Unified CCE for Unified CCDM:

Procedure

Step 1 Launch **Integrated Configuration Environment** on Unified CCDM Database Server Side A, see Launch the Integrated Configuration Environment, on page 156.

Step 2 In the ICE Cluster Configuration tool, from **Tool** drop-down list, select **Cluster Configuration**.

Step 3 Click **Configure Cisco Unified Contact Enterprise Servers**.

Step 4 From **Select Task** drop-down list, select **Add a New Instance** and click **Next**.

Step 5 In **Specify Resource Name**, specify a name for the instance you want to configure. Click **Next**.

Step 6 In **Select Required Components**, select the required components in the deployment and click **Next**.

- **Admin Workstation** - This is a required component in all configurations.
- **Provision Components (ConAPI/Unified config)** - Select this option if you require resource management.

Step 7 In **Configure Redundancy**, select whether you want to configure a single-sided or a dual-sided setup.

Step 8 In **Configure AW Server**, enter the primary server name and IP address.

Note If Unified CCE is dual-sided, then enter the secondary server name and the IP address also.

Step 9 In **Configure Connection Details**, enter authentication details to connect to the Admin Workstation database.

a) **Windows Authentication**: This is a default authentication mode.

b) **SQL Authentication**: Specify the SQL Server User name and the corresponding password to connect to the databases.

Step 10 In **Select Unified CCE Instance**, select the AW instance for the deployment and click **Next**.

Step 11 In **Configure Cisco Unified Contact Center Enterprise Server** window, configure **Unified Config Web Services** as follows:

- Enter the domain username and password for primary Unified CCE Admin workstation server in **Configure Primary Unified Config Web Service** page and click **Next**.
- If Unified CCE is dual-sided, then enter the domain username and password for secondary Unified CCE Admin Workstation server in **Configure Secondary Unified Config Web Service** page and Click **Next**.

Note Use the domain account credentials to login, username format must be *username@domain.com*.

Step 12 If you selected the option ConAPI Server (Provisioning) option in Step 4, enter the following details:

- **Local Registry Port** - Enter the port number of the Unified CCE for the Unified CCDM Provisioning service to connect. Default port is 2099. Ensure that you enter the same Unfied CCDM Database Server port number configured in the Application RMI registery port of the Set Up CMS Server on Unified CCE , on page 153.
- **Remote Registry Port** - Enter the port number of the Unified CCDM Database Server for the Unified CCE to connect. Default port is 2099. Ensure that you enter the same Unified CCE AW port number configured in the Administration & Data Server RMI Registry Port of the Set Up CMS Server on Unified CCE , on page 153.
- **Local Port** - Select this as the designated port for live provisioning traffic between the Unified CCE and Unified CCDM servers. Assign a unique port for each Unified CCE. Configure the firewall between the Unified CCE and Unified CCDM server to allow two-way traffic on this port.

Note If Unified CCE is dual-sided, enter the same port details configured for Side B in Set up CMS Server on Unified CCE.

Step 13 In **Configure ConAPI Application Instance** dialog box, enter the following details and click **Next**:

- **Application Name** - Name of the application to be used for provisioning Unified CCE from Unified CCDM. Enter the value as **CCDM** (pre-configured as part of load base configurations).
- **Application Key** - Use the password for the application you specified above.

Step 14 In **Multi Media Support** dialog box, select **Yes** if you are using a Cisco Unified WIM and EIM application instance to provide support for non-voice interactions. The default is **No**.

Step 15 In **Purge On Delete** dialog box, select **Yes** if you want to purge items from the Unified CCE automatically when they are deleted from Unified CCDM. The default is **Yes**.

Step 16 In the Supervisor Active Directory Integration dialog box, select **Yes** if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors. The default is **No**. If you select **Yes**, enter the following:

a. In **Configure Active Directory Connections**, enter the addresses of both primary and secondary domain controllers and configure the required security settings to connect. Click **Next**.

b. In the **Select Supervisor Active Directory Location**, select the required active directory and click **Next**.

Step 17 Review the details in the Summary page and click **Next** to apply the changes to the model.

Step 18 When the Unified CCE is successfully configured click **Exit** to close the wizard and then click **Save** to retain your changes to the database.

Create an Equipment Mapping

Complete the following procedure to create an equipment mapping between a tenant and the Unified CCE equipment.

Note To create a equipment mapping for SCC deployment, see Deployment Specific Configurations, on page 163.

Procedure

Step 1 Launch **Integrated Configuration Environment** on Unified CCDM Database Server Side A, see Launch the Integrated Configuration Environment, on page 156.

Step 2 From **Tool** drop-down list, select **Cluster Configuration**. Select **Equipment Mapping** tab.

Step 3 In the folder tree, right-click on root folder and select **Add Tenant**.

Step 4 Provide name for the new tenant.

Step 5 Create tenant for all customer.

Example:

Cust1CCE

Step 6 Select newly added Customer Tenant, in adjoining pane, check Unified Contact Center equipment check-box that you want to associate with the selected tenant.

Step 7 In the right-hand pane, choose **Default Import Location**.

Using Default Import Location, all the resources imported to selected tenant in Unified CCDM.

Step 8 Click **Save**.

Configure Unified CVP Servers in Unified CCDM Cluster

Setup Unified CVP Servers in Unified CCDM Cluster

The Configure Cisco Unified CVP Servers wizard configures Cisco Unified CVP server clusters. A Cisco Unified CVP server cluster consists of a Unified CVP Operations Console and, optionally, one or more call servers. To configure a Cisco Unified CVP server cluster:

Procedure

Step 1 Launch **Integrated Configuration Environment** on Unified CCDM Database Server Side A, see Launch the Integrated Configuration Environment, on page 156.

Step 2 In ICE Cluster Configuration tool, select the **Setup** tab and click **Configure Cisco Unified CVP Servers** to start the wizard.

Step 3 Select **Add a New Instance** and click **Next**.

Step 4 In **Specify Unified CVP Operations Console Resource Name** dialog box, specify a name for the Unified CVP operations console and click **Next**.

Step 5 In **Select Version** dialog box, specify the version of Unified CVP that is running on the CVP cluster you are configuring and click **Next**.

Step 6 In **Configure Unified CVP Operations Console** dialog box, enter the following:

- **Primary Server**:
  - **Sever Name**: This is the non-domain qualified machine name where the Cisco Unified CVP Operations Console is deployed.
  - **Server Address**: This defaults to Server Name. You can change this to an IP Address or a domain qualified name of the server.
- **Secondary Server**: This option is always disabled.

Step 7 Click **Next**.

Step 8 In **Configure Primary Unified Config Web Service** dialog box (only shown when the selected Unified CVP version is 10.0 or later), enter the following details:

- **URL**: This is the auto-generated URL of the primary unified config web service on the Unified CVP cluster
- **User Name**: This is a username with appropriate access to the Unified CVP that the web service is running on
- **Password**: This is the password for the user

Step 9 Click **Next**.

Step 10 In **Select Number of Call Servers** dialog box, specify the number of CVP call servers in the CVP cluster and click **Next**.

Note All CVP call servers must be on the same Unified CCE as the Unified CVP operations console.

Step 11 If you specified at least one call server:

a. In **Specify Unified CVP Call Server 1 Resource Name** dialog box, enter a name for the call server.

b. In **Configure Unified CVP Call Server 1** dialog box, enter the following:

- **Primary Server**:
  - **Sever Name**: This is the non-domain qualified machine name where the Cisco Unified CVP call server.
  - **Server Address**: This defaults to Server Name. You can change this to an IP Address or a domain qualified name of the server.
- **Secondary Server**: This option is always disabled.

c. Click **Next**.

Note Repeat this step to configure more than one call server.

Step 12 Optional, In **Configure** Unified CCE **Server** dialog box, select the Unified CCE servers that is linked to the configured unified CVP instance.

Step 13 The **Summary** dialog box, provides the brief details of the Unified CVP cluster being configured and the settings you have chosen.

Step 14 Check the details, click **Next**.

Step 15 A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.

Step 16 Click the **Save** icon.

Equipment Mapping for CVP with CCDM

For small contact center deployment model once the CVP integrated, by default CVP will get imported under unallocated folder.

Procedure

Step 1 Open **Integrated Configuration Environment** application, select **Cluster Configuration** > **Equipment Mapping** tab.

Step 2 In the folder tree, right-click on **Root** and click on **Add Tenant** and provide the name for Tenant.

Note You can also use existing Unified CCE Customer tenant to map unified CVP.

Step 3 Create Tenant for all CVP customer instances.

Example:

Cust1CVP

Step 4 Select newly added Tenant, in the adjoining pane, check the check box next to each item of Unified CVP that you want to associate with the selected Tenant.

Step 5 In right hand pane, select **Default Import Location** to import all the resources to selected tenant in Unified CCDM.

Step 6 Click **Save**.

Create Users in Active Directory

You must create a user in active directory to create a tenant or sub-customer from CCDM.

Procedure

Step 1 Log in to **Active Directory Domain**.

Step 2 Open **Active Directory Users and Computers** and click **User**.

Step 3 Right-click **User** and select **New** > **User**

Step 4 Enter **First Name**, **Last Name**, **user logon name** and click **Next**.

Step 5 Enter **Password** and retype the same password in **Confirm Password** field.

Step 6 Check **user cannot change password** check box.

Step 7 Check **Password never expires** check box and click **Next**.

Step 8 Click **Finish**.

Configure Unified CCE for Partitioned Internet Script Editor

Cisco's Internet Script Editor (ISE) can be integrated with Unified CCDM, which allows routing scripts and the resources within those routing scripts to be partitioned using Unified CCDM security. ISE users can see only the scripts and the resources within those scripts that they are authorized to access, according to the Unified CCDM security model. For example, when creating a routing script element to route to a dialed number, the ISE user will only see the dialed numbers that the corresponding Unified CCDM user is authorized to access. Similarly, when viewing the available routing scripts, the ISE user will only see the scripts available to the corresponding Unified CCDM user.

ISE integration with Unified CCDM uses the Unified CCDM Analytical Data Web Service to implement the secure partitioning, and requires specific configuration settings in both Unified CCE and Unified CCDM in order to work properly.

Note

- Secure partitioning using Unified CCDM is currently only supported for the Cisco Internet Script Editor (ISE). Users of the standard Script Editor on the Unified CCE AW will still see all resources on their associated Unified CCE instance.
- For Small contact Center Deployment model, see Integration of Small Contact Center Agent Deployment for Partition Internet Script Editor with CCDM, on page 169

- Configure Unified CCE Admin Workstation for Internet Script Editor, on page 162
- Create User, on page 212
- Assign Roles to Users, on page 214
- Install Internet Script Editor , on page 163
- Provision Routing Script Using Internet Script Editor, on page 272

Configure Unified CCE Admin Workstation for Internet Script Editor

Complete the following procedure to configureUnified CCE Admin Workstation for Internet Script Editor integration with Unified CCDM

Procedure

Step 1 Log In to Unified CCE Web Setup and navigate to **Component Management** >**Administration & Data server**, check the **Administrator** & **Data server** check-box and click **Edit**.

Step 2 Click **Next** until you see Database and Options tab, in Database and Options tab select the following options.

a) Select **Internet Script Editor (ISE) Server.**
b) Select **Authorization Server**.
c) Enter the name of the Authorization Server.
This is the Unified CCDM App/Web Server that will be used to apply Unified CCDM security to partition the resource data.
d) Enter the port that has Unified CCDM Analytical Data Services Web Service hosted.
By default, this port is 8087. If this is changed for your installation, enter the value that your installation uses.
e) Click **Next**.

Step 3 In Central Controller Connectivity tab enter the following details.

a) Enter the IP addresses for Router Side A, Router Side B, Logger Side A, Logger Side B, in **Central Controller Connectivity** section
b) Enter the domain name in **Central Controller Domain**.
c) Select the radio button **Central Controller Side A preferred** in **Central Controller Preferred Side** and click **Next**

Step 4 In **Summary** tab, click **Finish**

Step 5 Ensure that the firewall is configured on the server running the Unified CCE AW to allow inbound traffic from ISE on the appropriate port.

Step 6 Ensure that the specified Authorization Server port on the Unified CCDM Authorization Server has been configured in the firewall to allow inbound HTTPS traffic.

Install Internet Script Editor

Procedure

Step 1 Download the Internet Script Editor from AW machine `https://localhost/install/iScriptEditor.htm`

Step 2 Save `iscripteditor.exe` in a shared location for the particular customer/sub customer.

Step 3 Double-click `iscripteditor.exe` file.
Displays **Cisco ICM Internet Script Editor Setup** window

Step 4 Click **Next**.

Step 5 Select the folder to install files and click **Next**.

Step 6 After installation, click **Finish**.

Deployment Specific Configurations

Integration of Small Contact Center Agent Deployment for UCCE with CCDM

Create Customer Definition

Procedure

Step 1 Log in to AW machine and Open the **Configuration Manager**.

Step 2 Select **Explorer Tools** > **ICM Instace Explorer**.

Step 3 Click **Retrieve** and select the ICM Instance for SCC Deployment.

Step 4 Click **Add Customer Definition**.

Step 5 In **Name** field, enter the name of the sub customer definition.

Example:

SubCust1

Step 6 From **Network VRU** drop-down list, select **CVP_Network_VRU** option.

Step 7 Click on **Save**.

Note Repeat the same steps for all Sub Customer.

Map Equipment for Small Contact Center Deployment

Complete the following procedure to create an equipment mapping between a tenant or folder and the Unified CCE equipment for Small Contact Center.

Before you begin

Integrate AW with CCDM. For more information on How to Integrate AW, See Setup Unified CCE Servers in Unified CCDM Cluster, on page 156

Procedure

Step 1 In the ICE Cluster Configuration tool, select **Equipment Mapping** tab.

Step 2 In the folder tree, right-click on root, click **Add Tenant** and provide the name for tenant.

Create tenant for all sub customers.

Example:

SubCust1

Step 3 Select the newly created Sub Customer Tenant and In the adjoining pane select the check box or check boxes next to each item of Unified CCE equipment that you want to associate with the selected Tenant.

Step 4 In right-hand side pane, choose **Customer Resource Mapping** and click + icon.

Step 5 From **Type** drop-down list, select **Remote Tenant** option.

Step 6 From **Resource** drop-down list, select the customer definition created for sub customer.

Step 7 Click **Active Directory Configuration** tab and configure as follows:

a) Check **Configure Active Directory Settings** check-box.
b) In **Primary Domain Controller** field, enter Sub-customer Domain Controller IP address.
c) Click **Next** and ensure that domain controller name is correct.
d) Click **Update**.

Step 8 Select **Small Contact Center Settings** tab and configure as follows:

a) Check **Enable Small Contact Center** check-box.
b) In **Department Name** field, enter department name for the sub-customer domain.
c) Click **Create Department**.

Step 9 Click **OK**.

Step 10 Repeat the above steps for all sub customers.

Step 11 Click the unallocated folder and select the Unified CCE folder that is integrated. In the adjoining pane, check each item of Unified CCE equipment check-box that you want to associate with the selected Tenant and check **Default Import** check box.

Note By Default all the Configuration under Unified CCE will get imported under **Unallocated** folder.

Step 12 Click on **Save**

Resource Allocation for Small Contact Center Agent Deployment

- Move Resource to Sub Customer Tenant, on page 167
- Map Labels to the Network VRU Type, on page 168

* Configuration done by Sub Customer User

** Configurations provided in load base configuration which gets imported to Unallocated folder

*** Configurations are moved to sub customer domain from unallocated folder and configurations are done by service provider

Parameters	Configuration done by Sub Customer	Configuration done by Service Provider	Notes
Peripheral and Routing Client		** & ***	Peripherals, routing client of CUCM and MR are moved under Sub Customer Tenant.
Logical Interface Controller		** & ***	Logical Interface Controller for CUCM and MR peripheral are moved under Sub Customer Tenant.
Physical Interface Controller		** & ***	Physical Interface Controller for CUCM and MR peripheral are moved under Sub Customer Tenant.
Network VRU		**	Network VRU for Type10 and Type2 are given in Day1 configuration. Default, it is available under Unallocated Folder.
ECC Variable	*	**	ECC Variables are given in Day1 Configuration. Default, it is available under Unallocated Folder. and also the array size should be within the limitation

Parameters	Configuration done by Sub Customer	Configuration done by Service Provider	Notes
Network VRU Script	*	** & ***	Network VRU Script given in Day1 configuration. Default, it is available under Unallocated Folder. **Note** Since it is mapped to the customer definition "HCS for CC" in day1 config , this can be used by the subcustomer whose customer definition is HCS for CC. Sub customer user creates Network VRU Script specific to sub customer in his own Tenant.
Application Instance		** & ***	This item cannot be moved under any Tenant/folder, but service provider can create based on Customer request in AW
Media Class		**	
Media Routing Domain		**	Default MRDs given in Day1 Configuration. Default, it is available under Unallocated Folder.
Agent	*		
Agent Team	*		
Agent Desktop	*		

Parameters	Configuration done by Sub Customer	Configuration done by Service Provider	Notes
Call Type	*		
Department	*		
Dialed Number	*		
Enterprise Skill Group	*		
Label	*		Labels given in the day1 configuration will be imported under Unallocated folder. Service provider will map the label with Network VRU Type in the AW, based on Customer's request. For more information on how to map label to the network VRU Types, see Map Labels to the Network VRU Type, on page 168.
Person	*		
Precision Attribute	*		
Precision Queue	*		
Skill Group	*		
User Variable	*		
Outbound		***	All the Outbound configuration will be done in AW by the Service Provider and those configurations will be moved to Sub Customer Tenant.

Move Resource to Sub Customer Tenant

Procedure

Step 1 Log In to CCDM Portal with Tenant Administrator Credentials.

Step 2 Click the burger icon and select **Resource Manager** > **Unallocated** > **SCC Tenant Folder**.

Step 3 Click on the tree structure and select the parameters which should be move to sub customer Tenant.

Example:

Select Routing Client specific to sub-customer.

Step 4 Click on **Move** and select the **Sub Customer Tenant**.

Step 5 Click on **Save** and click on **OK**.

Repeat the steps for all the parameters that has to be moved under Sub Customer Tenant.

Map Labels to the Network VRU Type

Note This action will be performed by the Service Provider based on Sub Customer's request.

Procedure

Step 1 Login to AW machine.

Step 2 Navigate to **Configuration Manager -> Explore Tools -> Network VRU Explorer**.

Step 3 Click on **Retrieve** expand the **unassigned** tree structure.

Step 4 Right Click on the label that you want to map to Network VRU Type10.

Step 5 Click on **Cut** option.

Step 6 Select and right click the Network VRU Type 10 to which you want to map the label.

Step 7 Click on **paste** and Click on **Save**.

Associate Department with an Agent

Procedure

Step 1 Log in to CCDM portal.

Step 2 Click the burger icon.

Step 3 Select **Provisioning** > **Resource Manager**.

Step 4 Select the **Tenant** > **Agent**.

Step 5 Click on the tenant which we you want to associate to the department.

Step 6 Click **Advanced** tab.

Step 7 From **Department** drop-down list, select the required department.

Step 8 Click **Save**.

Naming Convention for the Resources in Small Contact Center Agent Deployment Model

This table describes the examples of the naming conventions to be followed for the resources in the small contact center agent deployment model.

Parameters	Sub Customer1	Sub Customer2
Dialed Numbers	Enterprise Name: 9220000001<RoutingClient> , Dialed Number String: 9220000001 OR Enterprise Name: PlayAgentGreeting<RoutingClient> Dialed Number String: PlayAgentGreeting	Enterprise Name: 9330000001<RoutingClient> , Dialed Number String: 9330000001 OR Enterprise Name: PlayAgentGreeting<RoutingClient> Dialed Number String: PlayAgentGreeting
Call Type	Enterprise Name: CT1Cust1	Enterprise Name: CT1Cust2
Agent	Enterprise Name: 10101010 LogIn Name: 10101010 Agent ID: 6001	Enterprise Name: 20202020 LogIn Name: 20202020 Agent ID: 6001
Skill Group	Enterprise Name: Skg1Cust1 Peripheral Number: 7001	Enterprise Name: Skg1Cust2 Peripheral Number: 7001
Network VRU Script	Enterprise Name: AgentGreetingCust1 VRU Script Name: PM,-a,,Cust1	Enterprise Name: AgentGreetingCust2 VRU Script Name: PM,-a,,Cust2
Network VRU Labels	Name: 9999500001 Label: 9999500001<RoutingClient>	Name: 9999500001 Label: 9999500001<RoutingClient>
Routing Script	Name: Script1	Name: Script1

Integration of Small Contact Center Agent Deployment for Partition Internet Script Editor with CCDM

Complete the following procedure in the sequence to configure CCDM to integrate with the Internet Script Editor.

Note These steps should be repeated for each sub customer.

- Configure Unified CCE Admin Workstation for Internet Script Editor, on page 162
- Create User, on page 212
- Assign Permission to Sub-customer Tenant and User, on page 214
- Install Internet Script Editor , on page 163
- Provision Routing Script Using Internet Script Editor, on page 272

Configure IDP

- Configure Metadata Exchange to IDP, on page 170
- Add Identity Server on Hosted AD FS, on page 170
- Add the Claim Rules, on page 171
- Configure AD FS for Federated Scenario, on page 173

Configure Metadata Exchange to IDP

Procedure

Step 1 Open ICE tool.

Step 2 From the **Tool** drop-down list, select **System Properties**.

Step 3 Select **Global Properties** > **Login Authentication Configuration**.

Step 4 In the **AD FS Metadata URL** field, enter the metadata URL of the AD FS server.
https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml

Step 5 From the **Enabled Login Types**, check the **ADFS Logins (adfs)** check box.

Step 6 Click **Save**.

Step 7 Open command prompt and perform `iisreset` in all CCDM servers.

Add Identity Server on Hosted AD FS

Follow the procedure to manually add the Unified CCDM identity server:

Procedure

Step 1 Open **AD FS Management Console**.

Step 2 Select **Trust Relationships** > **Relying Party Trusts**.

Step 3 Select **Add Relying Party Trusts**, then click **Start**.

Step 4 Select **Enter data about the relying party manually**, then click **Next**.

Step 5 Enter the appropriate display name, then click **Next**.

Example:

Unified CCDM Identity Server

Step 6 Select **AD FS profile**, then click **Next**.

Step 7 In the **Configure Certificate** step, click **Next**.

Note Unified CCDM does not support an optional token encryption certificates.

Step 8 Check the **Enable support for the WS-Federation Passive protocol** check box.

Step 9 In the **Relying Party WS-Federation Passive Protocol URL** field, enter the following URL of identity server AD FS endpoint:

```
https://<CCDM web server fqdn name>/identity/adfs
```

Note The URL must use AD FS trusted SSL certificate.

Step 10 Click **Next**.

Step 11 In the **Relying party trust identifier** pane, enter the following URL of the identity server:

```
https://<CCDM web server fqdn name>/identity
```

Step 12 Click **Add**, then click **Next**.

Step 13 Do not configure multi-factor authentication settings for the relying party trust, then click **Next**.

Step 14 Select **Permit all user to access this relying trust party**, and click **Next**.

Step 15 Review the settings, click **Next** to add the relying party trust to the AD FS configuration database.

Note To edit claim rules immediately, check the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** check box.

Step 16 Click **Close**.

Step 17 Repeat the steps for each identity server.

Add the Claim Rules

Follow the procedure on Hosted AD FS to add the claim rules for Unified CCDM:

Procedure

Step 1 Select **Unified CCDM trust**, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 From the **Claim Rule Template** drop-down list, select **Send LDAP Attributes as Claims**, then click **Next**.

Step 4 Add the required claims individually.

Claim Rule Name	Store	LDAP Attribute	Outgoing Claim Type	Mandatory
AD: SID as NameID	Active Directory	objectSid (type directly)	Name ID	Yes
AD: UPN as Name	Active Directory	User-Principal-Name	Name	Yes
AD: GivenName	Active Directory	Given-Name	Given Name	Optional
AD: Surname	Active Directory	Surname	Surname	Optional
AD: Email	Active Directory	E-Mail-Addresses	E-Mail-Address	Optional

Important Name ID of each claim rule must be unique. Therefore, always use SID as Name ID.

Step 5 Click **Finish**.

Step 6 Click **Add Rule**, and select the **Transform an Incoming Claim** and complete the Add Transform Claim Wizard:

Claim Rule Name	Incoming Claim Type	Outgoing Claim Type	Mandatory
TFN: Windows Account Name as Name	Windows Account Name	Name	Yes

Step 7 After adding the claim rules, click **Finish**.

Automatic User Provisioning

This is an alternate procedure to provision users.

Procedure

Step 1 Select **Unified CCDM trust**, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 Select **Send Group Membership as a Claim** as the claim rule template, and click **Next**.

Step 4 Add the following additional claims rules:

Claim Rule Name	User's Group	Outgoing Claim Type	Outgoing Claim Value
AD: Role = Supervisor	<windows group>	Role	Supervisor
AD: Role = Advanced	<windows group>	Role	Advanced

Step 5 After adding the claim rules, click **Finish**.

Set up AD FS

Procedure

Step 1 Open **AD FS Management Console**.

Step 2 Select **Trust Relationships** > **Claim Provider Trusts**.

Step 3 Select **Active Directory** > **Edit Claim Rules**.

Step 4 In the **Edit Claim Rules for Active Directory** dialog box, click **Add Rule**.

Step 5 From the **Claim Rule Template** drop-down list, select **Send LDAP Attributes as Claims**, then click **Next**.

Step 6 In the **Claim Rule Name** field, enter the Pass-thru DN.

Step 7 From the **Attribute Store** drop-down list, select the **Active Directory**.

Step 8 Map the LDAP Attribute to the Ongoing Claim type.

In the **LDAP Attribute (Select or type or add more)** column, enter **`distinguishedname`**. In the **Ongoing Claim Type (Select or type or add more)** column, enter **`http://temp.org/claims/DistinguishedName`**.

Step 9 Click **Finsh** and **OK**, restart the server.

Map Tenants to AD FS

Procedure

Step 1 Select **Unified CCDM trust**, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 In the **Add Transform Claim Rule Wizard** window, select **Send Claims Using a Custom Rule**, then click **Next**.

Step 4 Enter the claim rule name.

Claim rule name format: `AD: Tenant(<TenantPath>)`

Step 5 Enter the following custom rule text.

```
c:[Type == "http://temp.org/claims/DistinguishedName", Value =~ "^.*()$"]
=> issue(Type = "http://egain.net/claims/identity/tenant", Value = "/");
```

Example:

```
c:[Type == "http://temp.org/claims/DistinguishedName", Value =~ "^.*()$"]
=> issue(Type = "http://egain.net/claims/identity/tenant", Value = "qacce");
```

Step 6 Click **Finish**.

Configure AD FS for Federated Scenario

Note Create the Federated trust between Hosted AD FS and Customer AD FS.

Add Claim Rules for Relying Party Trust

Note Add the claim rules for Relying Party Trust in Customer AD FS.

Procedure

Step 1 Select the Relying party trust at the Customer AD FS, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 From the **Claim Rule Template** drop-down list, select **Send LDAP Attributes as Claims**, then click **Next**.

Step 4 Add the required claims individually:

Claim Rule Name	Store	LDAP Attribute	Outgoing Claim Type	Mandatory
AD: SID as Primary SID	Active Directory	objectSid (type directly)	Primary SID	Yes
AD: UPN as Name	Active Directory	User-Principal-Name	Name	Yes

Claim Rule Name	Store	LDAP Attribute	Outgoing Claim Type	Mandatory
AD: GivenName	Active Directory	Given-Name	Given Name	Optional
AD: Surname	Active Directory	Surname	Surname	Optional
AD: Email	Active Directory	E-Mail-Addresses	E-Mail-Address	Optional

Important Name ID of each claim rule must be unique. Therefore, always use SID as Name ID.

Step 5 Click **Finish**.

Step 6 Add another rule, from the **Claim Rule Template** drop-down list, select **Pass Through or Filter an Incoming Claim**, then click **Next**.

Claim Rule Name	Incoming Claim Type	Select Pass through all claim values	Mandatory
AD: Windows Account Name	Windows account name	Yes	Yes

Step 7 After adding the claim rules, click **Finish**.

Automatic User Provisioning

This is an alternate procedure to provision users.

Procedure

Step 1 Select the Relying party trust at the Customer AD FS, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 Select **Send Group Membership as a Claim as the claim rule template**, and click **Next**.

Step 4 Add the following claims rules:

Claim Rule Name	User's Group	Outgoing Claim Type	Outgoing Claim Value
AD: Role = Supervisor	<windows group>	Role	Supervisor
AD: Role = Advanced	<windows group>	Role	Advanced

Step 5 After adding the claim rules, click **Finish**.

Add Claim Rules for Claim Provider Trust

Note Add the claim rules for Claim Provider Trust in Hosted AD FS.

Procedure

Step 1 Select the Claims provider trust at the Hosted AD FS, then click **Edit Claim Rules**.

Step 2 In the **Acceptance Transform Rules** tab, click **Add Rule**.

Step 3 In the **The Add Transform Claim Rule Wizard** window, select **Pass Through or Filter an Incoming Claim**, then click **Next**.

Step 4 Add the required claim rule individually:

Claim Rule Name	Incoming Claim Type	Select Pass through all claim values	Mandatory
SID	Primary SID	Yes	Yes
Name	Name	Yes	Yes
GivenName	Given Name	Yes	Optional
Surname	Surname	Yes	Optional
EmailAddress	E-Mail-Address	Yes	Optional
Windows Account Name	Windows account name	Yes	Optional
Name ID	Name ID	Yes	Optional

Important
- Name ID of each claim rule must be unique. Therefore, always use SID as Name ID.
- For the Windows account name claim, select **Pass through only claim values that start with a specific value**.

Step 5 Once the claims have been set up, click **Finish**.

Automatic User Provisioning

This is an alternate procedure to provision users.

Procedure

Step 1 Select the Claims provider trust at the Hosted AD FS, then click **Edit Claim Rules**.

Step 2 In the **Acceptance Transform Rules** tab, click **Add Rule**.

Step 3 In the **The Add Transform Claim Rule Wizard** window, select **Pass Through or Filter an Incoming Claim**, then click **Next**.

Step 4 Add the following claims rules:

Claim Rule Name	Incoming Claim Type	Select Pass through only a specific claim value	Incoming Claim Value
Role = Advanced	Role	Yes	Advanced

Claim Rule Name	Incoming Claim Type	Select Pass through only a specific claim value	Incoming Claim Value
Role = Supervisor	Role	Yes	Supervisor

Step 5 Create custom rule, select **Send Claims Using a Custom Rule** as the claim rule template, then click **Next**.

- Enter the claim rule name.
- Enter the Custom Rule in the following format:

```
=> issue(Type = "http://egain.net/claims/identity/tenant", Value = "/<tenantname>",
Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"]
 = "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified");
```

Step 6 After adding the claim rules, click **Finish**.

Add Pass through Claims

Note Add the claim rules for Relying Party Trust in Hosted AD FS.

Procedure

Step 1 Select the Relying party trust at the Hosted AD FS, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 In the **The Add Transform Claim Rule Wizard** window, select **Transform an Incoming Claim**, then click **Next**.

Step 4 Add the required claim rule individually:

Claim Rule Name	Incoming Claim Type	Outgoing Claim Type	Mandatory
Federation: Transform Primary SID as Name ID	Primary SID	Name ID	Yes

Step 5 In the **The Add Transform Claim Rule Wizard** window, select **Pass Through or Filter an Incoming Claim**, then click **Next**.

Step 6 Add the required claim rule individually:

Claim Rule Name	Incoming Claim Type	Select Pass through all claim values	Mandatory
Name	Name	Yes	Yes
GivenName	Given Name	Yes	Optional
Surname	Surname	Yes	Optional

Claim Rule Name	Incoming Claim Type	Select Pass through all claim values	Mandatory
EmailAddress	E-Mail-Address	Yes	Optional
Windows Account Name	Windows account name	Yes	Optional
Name ID	Name ID	Yes	Optional

Important
- Name ID of each claim rule must be unique. Therefore, always use SID as Name ID.
- For the Windows account name claim, select **Pass through only claim values that start with a specific value**.

Step 7 After the claims have been set up, click **Finish**.

Automatic User Provisioning

This is an alternate procedure to provision users.

Procedure

Step 1 Select the Relying party trust at the Hosted AD FS, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 In the **The Add Transform Claim Rule Wizard** window, select **Pass Through or Filter an Incoming Claim**, then click **Next**.

Step 4 Add the following claims rules:

Claim Rule Name	Incoming Claim Type	Pass through any specific claim value	Incoming Claim Value
Role = Advanced	Role	Yes	Advanced
Role = Supervisor	Role	Yes	Supervisor

Step 5 Create custom rule, select **Send Claims Using a Custom Rule** as the claim rule template, then click **Next**.
- Enter the claim rule name.
- Enter the Custom Rule in the following format:

```
c:[Type == "http://egain.net/claims/identity/tenant"]=> issue(claim = c);
```

Step 6 After adding the claim rules, click **Finish**.

Cisco UCDM Integration

Basic Configuration of Unified Communication Domain Manager

Add Customer

Procedure

Step 1 Log in to Cisco Unified Communications Domain Manager as provider or reseller admin.

Step 2 Ensure that hierarchy path is set to appropriate level.

Note You can add customers under both provider and reseller. To add a customer under provider you must login as provider. To add customer under reseller you can login as either provider or reseller.

Step 3 Navigate to **Customer Management** > **Customer**.

Step 4 Provide necessary details in the following:

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

Step 5 Click **Save**.

Note If you want to delete customer and retain Unified Communication Manager configurations, see Disassociate Unified Communication Manager from UCDM, on page 296.

Setup Cisco Unified Communication Manager Servers

Procedure

Step 1 Log in to Cisco Unified Communications Domain Manager as provider or reseller or customer admin.

Step 2 Ensure that hierarchy path is set to appropriate level.

Note Shared instances should be created at provider or reseller level and dedicated instances should be created at customer level.

Step 3 Navigate to **Device Management** > **CUCM** > **Servers**.

Step 4 Click **Add**.

Step 5 Enter **CUCM Server Name**.

Step 6 Check **Publisher** check box to configure publisher node.

Step 7 Enter **Cluster Name**.

Note Uncheck **Publisher** check box, choose **Cluster Name** from the drop-down list to integrate subscriber node.

Step 8 In **Network Address** tab:

a) Choose **Service_Provider_Space** from **Address Space** drop-down list.
b) Enter IP address of CUCM in **IPV4 Address** field.
c) Enter **Hostname**, default hostname is CUCM Server name.
d) Enter **Domain**.
e) Enter **description**.

Step 9 In **Credentials** tab:

a) Choose **Admin** from **Credential Type** drop-down list.
b) Enter CUCM user ID in **User ID** text box.
c) Enter CUCM password in **Password** text box.
d) Choose appropriate access type from **Access Type** drop-down list.
e) Enter **description**.

Step 10 Click **Save**.

Configure Network Device List

Procedure

Step 1 Login to Cisco Unified Communications Domain Manager as a provider or reseller admin.

Step 2 Navigate to **Customer Management** > **Network Device Lists**. Choose a particular customer from hierarchy tree.

Step 3 Click **Add**.

Step 4 Enter **Network Device List Name**.

Step 5 Enter **Description** for Network Device List.

Step 6 Default, IP address of HCM-F is selected from **Cisco HCM-F** drop-down list.

Step 7 Expand **Cisco Unified CM** tab and choose **cisco unified communication manager** instance from the drop-down list.

Step 8 Click **Save**.

Add Site

Procedure

Step 1 Log in to Cisco Unified Communications Domain Manager as a Provider, Reseller, or, Customer admin.

Step 2 Ensure that hierarchy path is set to appropriate level.

Step 3 Navigate to **Site Management** > **Sites**.

Step 4 Click **Add**.

Step 5 Provide necessary details in the following:

a) Enter **Site Name**.
b) Enter **Description**.
c) Check **Create Local Admin** check box.
d) Enter **Default Admin Password** and confirm in **Confirm Password** text box.
e) Choose **Country** from drop-down list.
f) Choose **Network Device List** from the drop-down list.

Step 6 Click **Save**.

Note In dedicated options for Small Contact Centers, one customer and a site per customer is created in UCDM for each sub-customer. In shared options for Small Contact Centers, one customer and a site in UCDM are shared across multiple sub-customers.

Add Customer Dial Plan

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer.

Step 2 Ensure that hierarchy is set to appropriate customer level.

Step 3 Navigate to **Dial Plan Management** > **Customer** > **Dial Plan**.

Step 4 Click **Add**.

Step 5 Click **Save**.

Note
- Customer ID is Unique, auto-generated, read-only number allocated to the customer
- If Site Location Code is not specified, by default Dial Plan Type will set to Type_4

Add Site Dial Plan

Before you begin

Ensure Customer Dial Plan is created, see Add Customer Dial Plan, on page 180.

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer.

Step 2 Ensure that hierarchy is set to appropriate site.

Step 3 Navigate to **Dial Plan Management** > **Site** > **Management**.

Step 4 Click **Add**.

Step 5 Enter **Extension Length** value, it ranges from 1 - 11.

Step 6 Click **Save**.

Site information is loaded in to Cisco Unified Communication Manager, it can be identified using Customer ID and Site ID in its prefix.

Note This step takes few minutes to provision the site dial plan.

ASA Integration

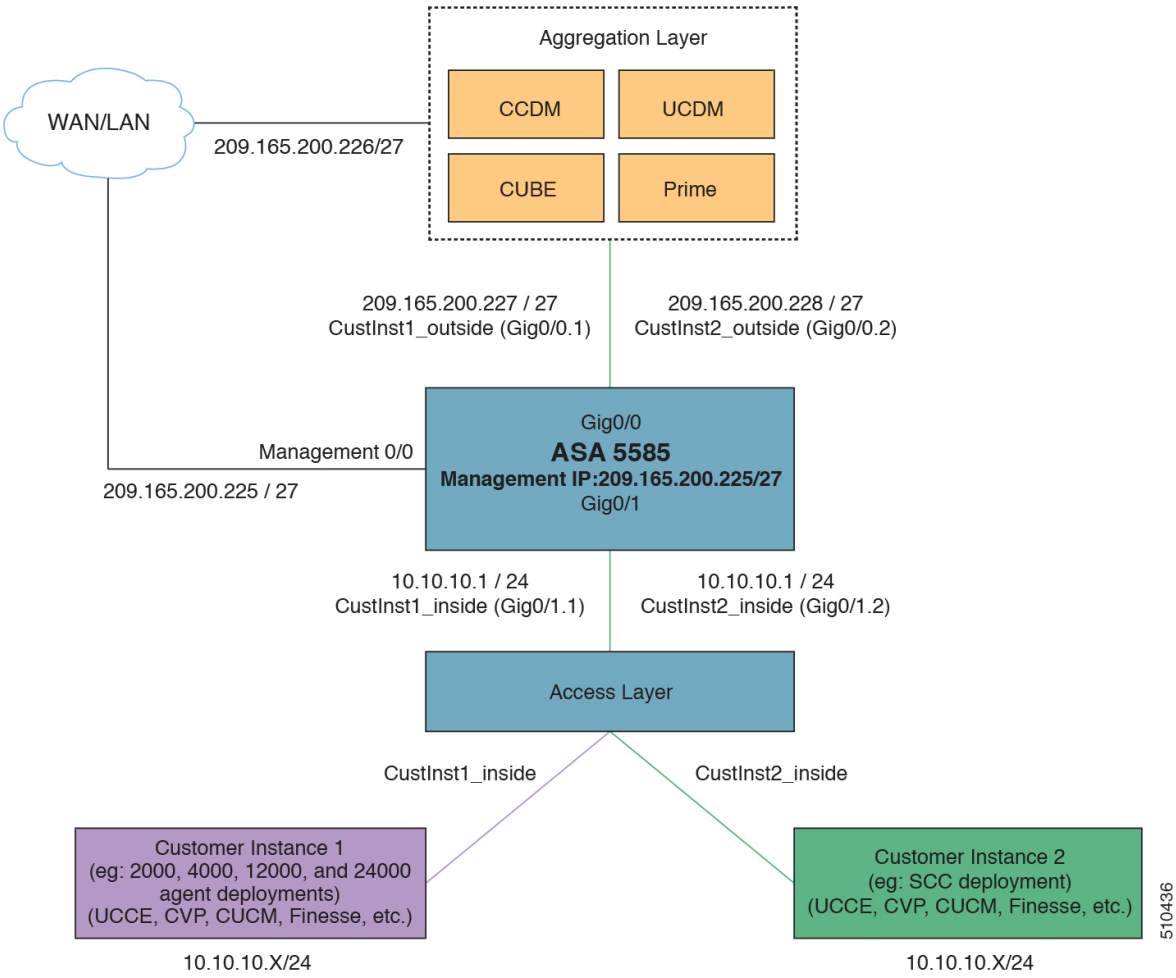
This section covers the configuration procedures required in Cisco ASA to integrate the customer instances for all types of HCS for CC deployment.

- Integration of ASA for HCS for CC Deployment model, on page 181
- Integration of ASA for Small Contact Center Deployment Model, on page 185

Integration of ASA for HCS for CC Deployment model

For the 2000, 4000, 12000, and 24000 agent deployment models the following configuration in Cisco ASA is required to integrate the customer instance components with the shared components. The following figure illustrates the deployment of different types with a Single ASA.

Figure 4: Customer Instances of Two Different Deployment Types Integrated with Shared Components



Repeat the Below procedures to integrate ASA for each customer instance. Required VLAN ID's and sub-interface ID for each customer instances will be different. Hence, IP addresses can be reused for these deployments:

- Configure Interfaces in the System Execution Space, on page 182
- Configure Security Contexts, on page 183
- Configure Interfaces in the Customer Instance Context, on page 184
- Configure Access-list in the Customer Instance Context, on page 185

Configure Interfaces in the System Execution Space

Procedure

Step 1 Navigate to global configuration mode:

```
hostname/context_name#changeto system
hostname#configure terminal
hostname(config)#
```

Step 2 Navigate to the interface Gigabit Ethernet 0/1 and enter the following command:

```
hostname(config)#interface gigabitethernet 0/1
hostname(config-if)#no shut
```

Step 3 Navigate to the sub-interface and enter the following commands, to assign the sub-interface to the customer_instance context and vlan ID inside the customer_instance:

```
hostname(config-if)#interface GigabitEthernet0/1.X
hostname(config-if)#vlan x
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.X
hostname(config-if)#vlan x
hostname(config-if)#no shut
```

Step 4 Repeat the above steps to assign a sub interface for each Customer instance.

Example:

For 2000 agent customer instance:

```
hostname(config)#interface  Gigabit Ethernet 0/1
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/1.1
hostname(config-if)#vlan 2
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.1
hostname(config-if)#vlan 340
hostname(config-if)#no shut
```

For 4000 agent customer instance:

```
hostname(config-if)#interface GigabitEthernet0/1.2
hostname(config-if)#vlan 4
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.2
hostname(config-if)#vlan 341
hostname(config-if)#no shut
```

Configure Security Contexts

Procedure

Step 1 Create customer_instance context in System Execution Space:

```
hostname(config)#context customer_instance
```

Step 2 Configure the customer_instance context definitions:

```
hostname(config-ctx)#description customer_instance context (optional)
hostname(config-ctx)#allocate-interface GigabitEthernet0/1.1 cust_inside invisible
```

```
hostname(config-ctx)#allocate-interface GigabitEthernet0/0.1 cust_outside invisible
hostname(config-ctx)#config-url disk0:/ customer_instance.cfg
```

Configure Interfaces in the Customer Instance Context

Procedure

Step 1 Navigate to customer_instance context configure mode:

```
hostname#changeto context customer_instance
hostname/customer_instance#configure  terminal
hostname/customer_instance(config)#
```

Step 2 Configure the interfaces for customer instances:

a) Navigate to the interface cust_inside:

```
hostname/customer_instance(config)#interface gigabitethernet0/1.1
```

b) Specify the name to inside interface of the customer_instance context:

```
hostname/customer_instance(config-if)#nameif inside_if_name
```

c) Enter the IP address of customer_instance of inside interface

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

d) Navigate to the interface cust_outside:

```
hostname/customer_instance(config-if)#interface gigabitethernet0/0.1
```

e) Specify the name to outside interface of the customer_instance context:

```
hostname/customer_instance(config-if)#nameif outside_if_name
```

f) Enter the IP address of customer_instance of outside interface:

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

Example:

```
hostname#changeto context 2000deployment
hostname/2000deployment#configure terminal
hostname/2000deployment(config)#interface gigabitethernet0/1.1
hostname/2000deployment(config-if)#nameif inside
hostname/2000deployment(config-if)#ip address 10.10.10.1 255.255.255.0
hostname/2000deployment(config-if)#interface gigabitethernet0/0.1
hostname/2000deployment(config-if)#nameif outside
hostname/2000deployment(config-if)#ip address 209.165.200.227 255.255.255.224
hostname/2000deployment(config-if)#exit
hostname/2000deployment(config)#exit
hostname/2000deployment#changeto context 4000deployment
hostname/4000deployment#configure terminal
hostname/4000deployment(config)#interface gigabitethernet0/1.2
hostname/4000deployment(config-if)#nameif inside
hostname/4000deployment(config-if)#ip address 10.10.10.1 255.255.255.0
hostname/4000deployment(config-if)#interface gigabitethernet0/0.2
hostname/4000deployment(config-if)#nameif outside
hostname/4000deployment(config-if)#ip address 209.165.200.228 255.255.255.224
```

Configure Access-list in the Customer Instance Context

Configure the access-list to allow IP traffic. The access-list is applied to both outside and inside interfaces:

Procedure

Step 1 Create the access-list for both outside and inside IP traffic:

```
hostname/customer_instance(config)#access-list access_list_name_outside extended permit ip
 any any
hostname/customer_instance(config)#access-list access_list_name_inside extended permit ip
any any
```

Step 2 Apply the access-list for both outside and inside IP traffic:

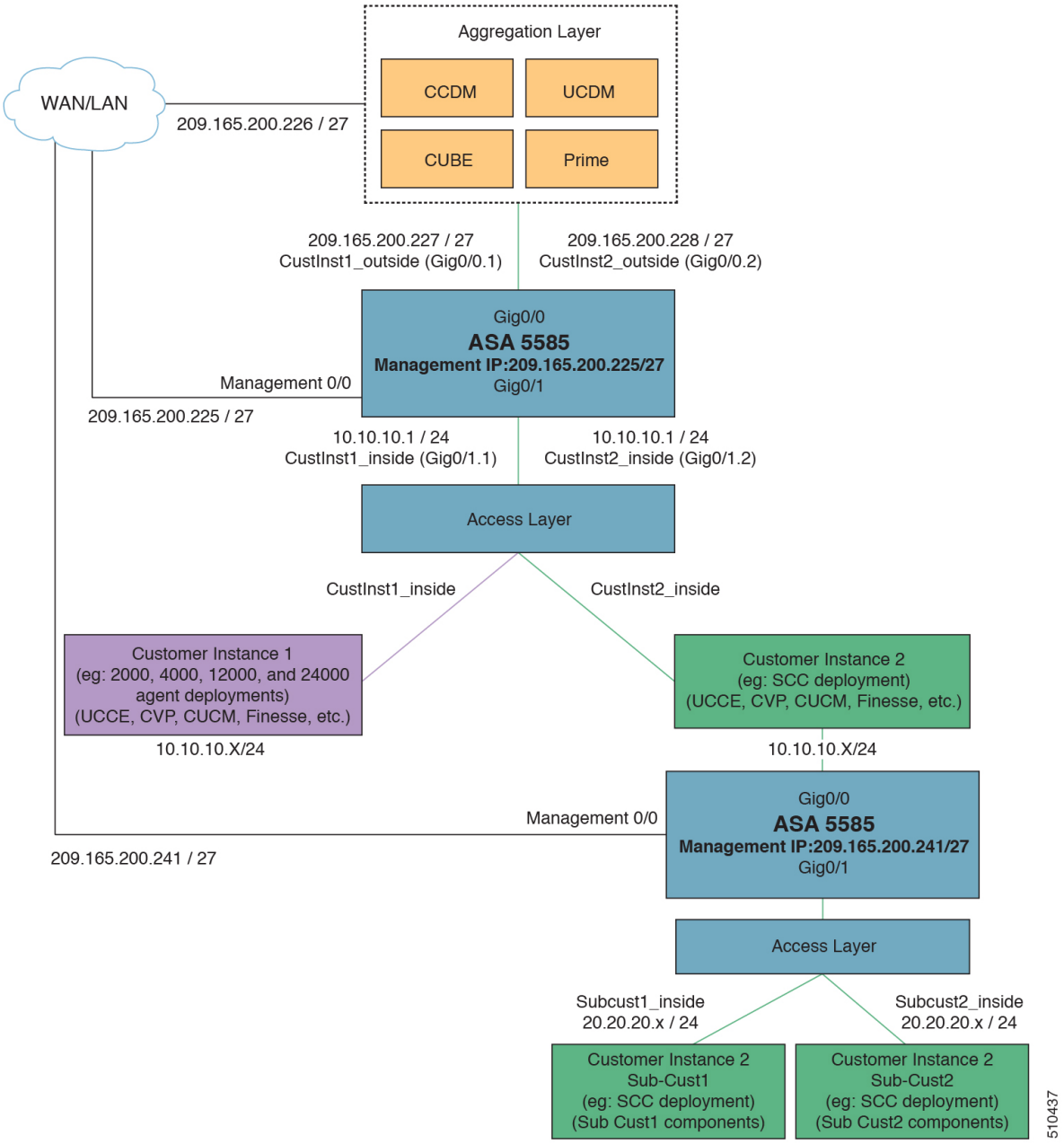
```
hostname/customer_instance(config)#access-group access_list_name_outside in interface
outside_if_name
hostname/customer_instance(config)#access-group access_list_name_inside in interface
inside_if_name
```

Note Allow or deny IP address in access-list as per the requirement of the network.

Integration of ASA for Small Contact Center Deployment Model

Small contact center deployment model requires two Cisco ASAs, one is to integrate the Small Contact Center customer instance with the shared components and another one is to integrate sub customer instances with the small contact center customer instance.

The following figure illustrates the deployments of 2000,4000, 12000, 24000 agents, and small contact center instances with two Cisco ASAs.



Integrate ASA for Small contact center with shared components, then Integrate ASA for Small contact center customer instance with sub-customer instance. For more information on installing and configuring ASA, for more information see *Install and Configure ASA Firewall and NAT* section of *Installing and upgrading guide for Cisco Hosted Collaboration Solution for Contact Center* http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

After Installing the ASA, repeat the below procedures for each sub-customer instance. Required VLAN ID's and sub-interface ID for sub-customer instances will be different. Hence, IP addresses can be reused for these deployments.

- Configure Interfaces in the System Execution Space, on page 187

- Configure Security Contexts for each Sub-customer Context, on page 188
- Configure Interfaces in each Sub-Customer Instance Context, on page 188
- Configure Access-list in the Sub-customer Instance Context, on page 189

Configure Interfaces in the System Execution Space

Procedure

Step 1 Navigate to global configuration mode:

```
hostname/context_name# changeto system
hostname# configure terminal
hostname(config)#
```

Step 2 Navigate to the interface Gigabit Ethernet 0/1 and enter the following command:

```
hostname(config)#interface gigabitethernet 0/1
hostname(config-if)#no shut
```

Step 3 Navigate to the sub-interface and enter the following commands, to assign the sub-interface to the sub-customer_instance context and vlan ID inside the sub-customer_instance:

```
hostname(config-if)#interface GigabitEthernet0/1.X
hostname(config-if)#vlan x
hostname(config-if)#no shut
```

```
hostname(config-if)#interface GigabitEthernet0/0.X
hostname(config-if)#vlan x
hostname(config-if)#no shut
```

Step 4 Repeat the above steps to assign a sub interface for each sub-customer instance.

Example:

For sub-cust1

```
hostname(config)#interface  gigabitethernet0/1
hostname(config-if)#No shut
```

```
hostname(config-if)#interface gigabitethernet0/1.1
hostname(config-if)#vlan 10
hostname(config-if)#no shut
```

```
hostname(config-if)#interface GigabitEthernet0/0.1
hostname(config-if)#vlan 11
hostname(config-if)#no shut
```

For sub-cust2

```
hostname(config-if)#interface gigabitethernet0/1.2
hostname(config-if)#vlan 20
hostname(config-if)#no shut
```

```
hostname(config-if)#interface gigabitethernet0/0.2
hostname(config-if)#vlan 21
hostname(config-if)#no shut
```

Configure Security Contexts for each Sub-customer Context

Procedure

Step 1 Create sub-customer_instance context in System Execution Space:

```
hostname(config)#context sub-customer_instance
```

Step 2 Configure the customer_instance context definitions:

```
hostname(config-ctx)#description sub-customer_instance context (optional)
hostname(config-ctx)#allocate-interface GigabitEthernet0/1.1 subcustX_inside invisible
hostname(config-ctx)#allocate-interface GigabitEthernet0/0.1 subcustX_outside invisible
hostname(config-ctx)#config-url disk0:/ sub-customer_instance.cfg
```

Example:

```
hostname/admin#changeto system
hostname#configure terminal
hostname(config)#context sub-cust1
hostname(config-ctx)#description sub-customer_1 context
hostname(config-ctx)#allocate-interface gigabitethernet0/1.1 sub-cust1_inside invisible
hostname(config-ctx)#allocate-interface gigabitethernet0/0.1 sub-cust1_outside invisible
hostname(config-ctx)#config-url disk0:/ sub-cust1.cfg
hostname(config-ctx)#context sub-cust2
hostname(config-ctx)#description sub-customer_2 context
hostname(config-ctx)#allocate-interface gigabitethernet0/1.2 sub-cust2_inside invisible
hostname(config-ctx)#allocate-interface gigabitethernet0/0.2 sub-cust2_outside invisible
hostname(config-ctx)#config-url disk0:/ sub-cust2.cfg
```

Configure Interfaces in each Sub-Customer Instance Context

Procedure

Step 1 Navigate to sub-customer_instance context configure mode:

```
hostname#changeto context sub_customer_instance_name
hostname/sub_customer_instance#configure  terminal
hostname/sub_customer_instance (config)#
```

Step 2 Configure the interfaces for sub-customer instances:

a) Navigate to the interface sub-cust_inside:

```
hostname/sub_customer_instance (config)#interface gigabitethernet0/1.1
```

b) Specify the name to inside interface of the sub-customer_instance context:

```
hostname/sub_customer_instance (config-if)#nameif inside_if_name
```

c) Enter the IP address of sub-customer_instance of inside interface

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

d) Navigate to the interface sub-cust_outside:

```
hostname/sub_customer_instance (config-if)#interface gigabitethernet0/0.1
```

e) Specify the name to outside interface of the sub-customer_instance context:

```
hostname/sub_customer_instance (config-if)#nameif outside_if_name
```

f) Enter the IP address of sub-customer_instance of outside interface:

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

Example:

```
hostname#changeto context sub-cust1
hostname/sub-cust1#configure terminal
hostname/sub_cust1(config)#interface sub-cust1_inside
hostname/sub_cust1(config-if)#nameif inside
hostname/sub_cust1(config-if)#ip address 20.20.20.1 255.255.255.0
hostname/sub_cust1(config-if)#interface sub-cust1_outside
hostname/sub_cust1(config-if)#nameif outside
hostname/sub_cust1(config-if)#ip address 10.10.10.254 255.255.255.0
hostname/sub_cust1(config)#interface sub-cust2_inside
hostname/sub_cust1(config-if)#nameif inside
hostname/sub_cust1(config-if)#ip address 20.20.20.1 255.255.255.0
hostname/sub_cust1(config-if)#interface sub-cust2_outside
hostname/sub_cust1(config-if)#nameif outside
hostname/sub_cust1(config-if)#ip address 10.10.10.254 255.255.255.0
```

Configure Access-list in the Sub-customer Instance Context

Configure the access-list to allow IP traffic. The access-list is applied to both outside and inside interfaces:

Procedure

Step 1 Create the access-list for both outside and inside IP traffic.

```
hostname/sub_customer_instance(config)#access-list access_list_name_outside extended permit
 ip any any
hostname/sub_customer_instance(config)#access-list access_list_name_inside extended permit
 ip any any
```

Step 2 Apply the access-list for both outside and inside IP traffic.

```
hostname/sub_customer_instance(config)#access-group access_list_name_outside in interface
outside_if_name
hostname/sub_customer_instance(config)#access-group access_list_name_inside in interface
inside_if_name
```

Note Allow or deny IP address in access-list as per the requirement of the network.

Session Border Controller Integration

For information on integrating CUBE Enterprise as the SBC in the aggregation layer, see Cisco Hosted Collaboration Solution - Deploying Multiple Virtual Forwarding (mVRF) using the Cisco Unified Border Element Enterprise Edition.

For information on integrating third-party Session Border Controller in the aggregation layer, see http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

Cisco Prime Collaboration Assurance Integration for Small Contact Center Deployment Model

Customer Management for Prime Collaboration Assurance

Procedure

Step 1 Login to Prime using the URL *https://<IP_address_of_Prime_Collaboration_application/* .
Step 2 Go to **Administration** > **Customer Management**.
Step 3 Click **Add**.
Step 4 In **General Info** tab, enter the **Customer Name**.
Step 5 Click **Next** and then **Save**.

Add Cluster

Procedure

Step 1 Log into HCM-F using administrator credentials.
Step 2 Choose **Cluster Management** > **Cluster**, and click **Add New**.
Step 3 Enter the cluster name.
Step 4 Choose the customer from the drop-down list.
Step 5 Choose **CC** for the cluster type from the drop-down list.
Step 6 Choose the cluster application version from the drop-down list.
Step 7 Choose PCA as the host name from the Application Monitoring the Cluster drop-down list.
Step 8 Click **Save**.

Add Contact Center Components

Customer Contact components includes Rogger, AW-HDS, Agent Peripheral Gateway, VRU Peripheral Gateway, CVP, CVP OAMP, and CVP RSA.

Procedure

Step 1 Log in to HCM-F using administrator credentials.

Step 2 Choose **Application Management** > **Cluster Application**.

Step 3 In the **General Information** section, configure the following.

a) Click **Add New**.
b) Choose **UCCE** from the **Application Type** drop-down list.

Choose **CVP** for CVP, CVP OAMP, CVP RSA , choose **UCCE** for Rogger, AW-HDS, Agent Peripheral Gateway, or VRU Peripheral Gateway.

c) Enter the host name of the CC component.
d) Choose a cluster from the drop-down list.
e) Click **Save**.

Step 4 In the **Credentials** section, configure the following.

a) Click **Add New**.
b) Choose **SNMP _V2** from the **Credential Type** drop-down list.
c) Enter the **Community Srting** configured on CC Component.
d) Choose **Read Only** option for the access type.
e) Click **Save**.
f) Click **Add New**.
g) Choose **ADMIN** from the **Credential Type** drop-down list.
h) Enter the administrator credentials.

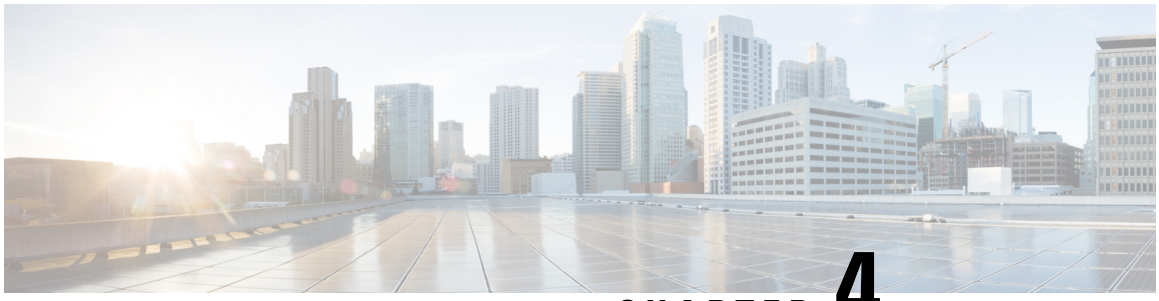
For CVP, CVP OAMP, CVP RSA use User ID as **`wsmadmin`** and password configured for OAMP web UI

i) Choose **Read Only** option for the Access Type .
j) Click **Save**.

Step 5 In **Network Addresses** section, configure the following.

a) Click **Add New**.
b) Choose **Application Space** from the **Network Space** drop-down list.
c) Enter the IPV4 Address and the hostname.
d) Click **Save**.
e) Click **Add New**.
f) Choose **Service Provider Space** from **Network Space** drop-down list.
g) Enter the NAT IPV4 Address and Hostname.
h) Click **Save**.

Note Follow the same procedure to add AW-HDS, Agent Peripheral Gateway,VRU Peripheral Gateway, CVP, CVP OAMP, and CVP RSA. Cisco Unified IC is not supported.



CHAPTER 4

Administration

Unified CCE Administration

Smart Licensing

Cisco Smart Software Licensing is a flexible software licensing model that streamlines the way you activate and manage Cisco software licenses across your organization. Smart Licenses provide greater insight into software license ownership and consumption, so that you know what you own and how the licenses are being used. The solution allows you to easily track the status of your license and software usage trends. It pools the license entitlements in a single account and allows you to move licenses freely across virtual accounts. Smart Licensing is enabled across most of the Cisco products and managed by a direct cloud-based or mediated deployment model.

Smart Licensing registers the Product Instance, reports license usage, and obtains the necessary authorization from **Cisco Smart Software Manager (Cisco SSM)** or **Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem)**.

You can use Smart Licensing to:

- View license usage and count.
- View the status of each license type and the product instance.
- View the product licenses available on Cisco SSM or Cisco SSM On-Prem.
- Register or deregister the Product Instance, renew license authorization and license registration.
- Sign in additional agents to Unified CCX up to the maximum limit that is configured in your OVA.

Smart Licensing Capabilities

Smart Licensing works in conjunction with Cisco Smart Software Manager (Cisco SSM) to intelligently manage product licenses by providing real-time visibility of license status and usage. You can use this data to make better purchase decisions, based on your consumption. Smart Licensing establishes a pool of software licenses or entitlements in Cisco Smart Account.

The Smart Account provides a central location where you can view, store, and manage your licenses, across the organization. You can get access to your software licenses, hardware, and subscriptions through your Smart Account. Smart Accounts are required to access and manage Smart License-enabled products.

Creating a Smart Account is easy and takes less than five minutes. Create a Smart Account on software.cisco.com.

Documentation Resources

Table 20: Documentation Resources

For	Go to...
Smart Licensing Prerequisites	Prerequisites for Smart Licensing, on page 194
Understanding the License consumption Calculation	License Consumption Calculation, on page 204
Migration to Smart Licensing	Migrate to Smart Licensing, on page 205
Best Practices	Best Practices, on page 209

Prerequisites for Smart Licensing

The following are the prerequisites for configuring Smart Licensing:

- **Smart Licensing Enrollment**

  Set up Smart and Virtual accounts. For more information, see https://software.cisco.com/#module/SmartLicensing.

- **Adoption of License Integration Strategy**

  Decide how you want to connect your product instance to Smart Licensing servers:

  - **On-Cloud:** Configure to connect to Cisco SSM On-Prem
  - **On-Premise:**

    1. Deploy the Cisco SSM On-Prem. For instructions on how to do this, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html.
    2. Configure to connect to Cisco SSM On-Prem.

  For more information, see Smart License Deployments, on page 195.

- **Import the Rogger A certificate into the AW machines**

  1. Export Logger/Rogger A certificate and save it by using the url `https:<Logger/Roggerhostname>:443`

2. Import the certificate in AW by using the following command:

   - `cd %CCE_JAVA_HOME%\bin`

```
C:\Program Files (x86)\Java\jre1.8.0_221\bin>keytool.exe -keystore
Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"
-import -alias <alias name> -file <certicate with fully qualified path>
```

3. Enter the truststore password when prompted.
4. Enter 'Yes' when prompted to trust the certificate.
5. Restart the Tomcat service.

Smart License Deployments

There are two software deployment options for Smart Licensing:

- Direct - Cisco Smart Software Manager (Cisco SSM)
- Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem)

Direct - Cisco Smart Software Manager (Cisco SSM)

The Cisco SSM is a cloud-based service that handles your system licensing. The Product Instance can connect either directly to Cisco SSM or through a proxy server.

Cisco SSM allows you to:

- Create, manage, or view virtual accounts.
- Manage and track the licenses.
- Move licenses across the virtual accounts.
- Create and manage Product Instance Registration Tokens.

For more information about Cisco SSM, go to https://software.cisco.com.

Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem)

Cisco SSM On-Prem is an on-premises component that can handle your licensing needs. When you choose this option, registers and reports license consumption to the Cisco SSM On-Prem, which synchronizes its database regularly with Cisco SSM that is hosted on cisco.com.

You can use the Cisco SSM On-Prem in either Connected or Disconnected mode, depending on whether the Cisco SSM On-Prem can connect directly to cisco.com.

Configure Transport URL for Cisco SSM On-Prem with Smart Call-Home URL:
https://<OnpremCSSM>/Transportgateway/services/DeviceRequestHandler

Note The <OnpremCSSM> value must match with the SSM Tomcat Certificate Common Name or Subject Alternative Name. In the above URL, replace <OnpremCSSM> with FQDN or IP, based on the SSM Tomcat Certificate.

- **Connected**—Use when there is connectivity to cisco.com directly from the Cisco SSM On-Prem. Smart account synchronization occurs automatically.
- **Disconnected**—Use when there is no connectivity to cisco.com from the Cisco SSM On-Prem. Cisco SSM On-Prem must synchronize with Cisco SSM manually to reflect the latest license entitlements.

  For more information on Cisco SSM On-Prem, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html.

Smart Licensing Task Flow

Complete these tasks to set up smart licensing for HCS for CC.

Steps	Action	Description
Step 1	Create your Smart Account	Use the Smart Account to organize licenses according to your needs. To create a Smart Account, go to http://software.cisco.com After the Smart Account is created, Cisco SSM creates a default Virtual Account for this Smart Account. You can use the default account or create other Virtual Accounts.
Step 2	Obtain the Product Instance Registration Token	Generate a product instance registration token for your virtual account. For more information, see Obtain the Product Instance Registration Token.
Step 3	Configure Transport Settings for Smart Licensing	Configure the transport settings through which HCS for CC connects to the Cisco SSM or Cisco SSM On-Prem. For more information, see Configure Transport Settings for Smart Licensing.
Step 4	Select the License Type	Select the License Type before registering the product instance. For more information, see Select License Type.
Step 5	Register with Cisco SSM	You can register HCS for CC with Cisco SSM or Cisco SSM On-Prem. For more information, see Register with Cisco Smart Software Manager.

Note After performing the above steps, wait for 10-15 minutes for the correct status to get reflected in the UI. There is no need to restart the services.

Obtain the Product Instance Registration Token

Obtain the product instance registration token from Cisco SSM or Cisco SSM On-Prem to register the product instance. Generate the registration token with or without enabling the Export-Controlled functionality.

Note The **Allow export-controlled functionality on the products that are registered with this token** check box does not appear for Smart Accounts that are not permitted to use the Export-Controlled functionality.

Procedure

Step 1 Log in to your smart account in either Cisco SSM or Cisco SSM On-Prem.

Step 2 Navigate to the virtual account with which you want to associate the product instance.

Step 3 Generate the Product Instance Registration Token.

Note
- Select the **Allow export-controlled functionality on the products registered with this token** check box to turn on the Export-Controlled functionality for a product instance you want in this smart account. When you select this check box and accept the terms, you enable higher levels of encryption for products that are registered with this registration token. By default, this check box is selected.
- Use this option only if you are compliant with the Export-Controlled functionality.

Step 4 Copy the generated token. This token is required when registering Smart Licensing with Cisco SSM.

Configure Transport Settings for Smart Licensing

Configure the connection mode between HCS for CC and Cisco SSM.

Procedure

Step 1 From Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management**.

Step 2 Click **Transport Settings** to set the connection method.

Step 3 Select the connection method to Cisco SSM:

- **Direct**—HCS for CC connects directly to Cisco SSM on cisco.com. This is the default option.
- **Transport Gateway**—HCS for CC connects to Cisco SSM On-Prem for smart licensing. Enter the Cisco SSM On-Prem URL.
- **HTTP/HTTPS Proxy**—HCS for CC connects to a proxy server, which connects to Cisco SSM. Enter the Fully Qualified Domain Name (FQDN) of the proxy server along with the port.

Step 4 Click **Save** to save the settings.

Select License Type

Smart Licensing offers two types of license—Flex and Perpetual

- **Flex**—Flex license is a recurring subscription of Standard and Premium license. These subscriptions are renewed periodically, for example 1, 3, or 5 years.
- **Perpetual**—Perpetual license is a permanent and one-time payment license that offers Premium license.

Note If you select incorrect License Type, the product instance is placed in the Out-of-Compliance state. If this issue is unresolved, the product instance is placed in the Enforcement state where the system operations are impacted.

Note If you select the Deployment Type as *HCS-CC*, the system automatically updates to **Flex** even when the License Type is configured as **Perpetual**.

Procedure

Step 1 From Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management**.

Step 2 Click **License Type**.
The **Select License Type** page is displayed.

Step 3 Select the License Type corresponding to what you have purchased before registering the product instance.

Step 4 Select the License Type and the Usage Mode corresponding to what you have purchased before registering the product instance.

Step 5 Click **Save**.

Register with Cisco Smart Software Manager

The product instance has 90 days of evaluation period, within which, the registration must be completed. Else, the product instance gets into the enforcement state.

Register your product instance with Cisco SSM or Cisco SSM On-Prem to exit the Evaluation or Enforcement state.

Note After you register the product instance, you cannot change the license type. To change the license type, deregister the product instance.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management.**

Step 2 Click **Register**.

Note
- Before you register the product instance, ensure to select the **License Type** and the communication mechanism in **Transport Settings**.

Step 3 In the **Smart Software Licensing Product Registration** dialog box, paste the product instance registration token that you generated from Cisco SSM or Cisco SSM On-Prem.

For information on generating the Registration Token, see the *Obtain the Product Instance Registration Token* section in Cisco Unified Contact Center Express Features Guide.

Step 4 Click **Register** to complete the registration process.

After registration, the **Smart Licensing Status** displays the following details.

Table 21: Smart Licensing Status

Smart License Status	Description
On Unsuccessful Registration	
Registration Status	Unregistered
License Authorization Status	Evaluation
Export-Controlled Functionality	Not Allowed
On Successful Registration	
Registration Status	Registered (Date and time of registration)
License Authorization Status	Authorized (Date and time of authorization)
Export-Controlled Functionality	Not Allowed
Smart Account	The name of the smart account
Virtual Account	The name of the virtual account
Product Instance Name	The name of the product instance
Serial Number	The serial number of the product instance

Entitlements are a set of privileges customers and partners receive when purchasing a Cisco service agreement. Using Smart Licensing, you can view the License consumption summary for the entitlements of different license types. The License consumption summary displays the License Name, Usage Count, and Status against each entitlement name.

You can update or purchase entitlements on the Cisco Commerce website. For more information, see https://apps.cisco.com/Commerce/.

Registration, Authorization, and Entitlement Status

Registration Status

This table explains the various product registration status for Smart Licensing in the Unified CCE Administration portal:

Table 22: Registration Status

Status	Description
Unregistered	Product is unregistered.
Registered	Product is registered. Registration is automatically renewed every six months.
Registration Expired	Product registration has expired because the ID Certificate issued by Cisco SSM is not renewed for more than 12 months.

Authorization Status

This table describes the possible product authorization status for Smart Licensing in the Unified CCE Administration portal:

Table 23: Authorization Status

Status	Description
Evaluation state	Product is not registered with Cisco.
Evaluation Expired	Product evaluation period has expired.
Authorized	Product is in authorized or in compliance state. Authorization is renewed every 30 days.
Authorization Expired	Product authorization has expired. This usually happens when the product has not communicated with Cisco for 90 days. It is in an overage period for 90 days before enforcing restrictions.
Out-of-Compliance	Product is in out-of-compliance state because of insufficient licenses. It is in an overage period for 90 days before enforcing restrictions.
Unauthorized	Product is unauthorized.
No License in Use	No Licenses are in use.

License Entitlement Status

This table describes the possible product instance license entitlement status for Smart Licensing in the Unified CCE Administration portal:

Table 24: License Entitlement Status

Status	Status Description
Authorization Expired	Product authorization has expired, when the product has not communicated with Cisco for 90 days.
Not Authorized	Product instance is not authorized.
Evaluation state	Product is not registered with Cisco.
Evaluation Expired	Product evaluation period has expired.
In Compliance	Product is in authorized or in compliance state. Authorization is renewed every 30 days.
ReservedInCompliance	Entitlement is in compliance with the installed reservation authorization code.
Out-of-Compliance	Product is in out-of-compliance state because of insufficient licenses. It is in an overage period for 90 days before enforcing restrictions.
Not Applicable	Entitlement is not applicable.
Invalid	Error condition state.
Invalid Tag	Entitlement tag is invalid.
No License in Use	Entitlement is not in use.
Waiting	Waiting for an entitlement request's response from Cisco SSM or Cisco SSM On-Prem.
Disabled	Product instance is deactivated or disabled.

Out-Of-Compliance and Enforcement Rules

Out-of-Compliance

The Product Instance reports license usage to Cisco SSM every 15 minutes. If your license consumption is more than the entitlements for four consecutive reporting intervals, the Product Instance is pushed to the Out-of-Compliance state. The Out-of-Compliance period is for 90 days, within which you need to purchase the additional licenses. If you fail to take corrective action within the 90 days period, the Product Instance is pushed to the Enforcement state.

All CVPs in a virtual account share the licenses from a pool. If the license consumption exceeds than those available in the pool, all CVPs in the virtual account follow the Out-of-Compliance and Enforcement rules.

Enforcement

The Product Instance is in the Enforcement state in the following scenarios:

- **Out-of-Compliance expiry**: When the Out-of-Compliance period of 90 days has expired.

  Purchase new licenses to exit the Enforcement state.

- **Authorization expiry**: When the Product Instance has not communicated with Cisco SSM or Cisco SSM On-Prem for 90 days and has not automatically renewed the entitlement authorizations.

  Renew the license authorizations to exit the authorization expiry state.

- **Evaluation expiry**: When the license evaluation period of 90 days has expired and the Product Instance is not registered with Cisco SSM.

  Register the Product Instance with Cisco SSM to exit the Evaluation expiry state.

Note In the Enforcement state, addition of new agents is blocked in HCS for CC.

License States

Smart Licensing has the following states:

- **Registration State**
  - **Unregistered**—Product Instance is unregistered.
  - **Registered**—After you purchase the license, you need to register the Product Instance with Cisco SSM. To register with Cisco SSM, generate a registration token from the Cisco SSM portal. Use the registration token to register your Product Instance.
  - **Registration Expired**—Product Instance registration has expired because the ID Certificate issued by Cisco SSM is not renewed for more than 12 months. Reregister the Product Instance.

- **Authorization State**
  - **No licenses in use**
  - **Evaluation Mode**—The Product Instance license has an Evaluation period of 90 days. In the Evaluation period you have unlimited access to the product with highest set of product capabilities and unlimited number of licenses. You must register the system with Cisco SSM or Cisco SSM On-Prem within 90 days. If the system is not registered before the end of the evaluation period, it will be moved to the Enforcement state where certain system functions are restricted.
  - **In Compliance**—When the license consumption is as per the purchased quantity, the product is compliant.
  - **Evaluation expired**—Product Instance evaluation period has expired.
  - **Authorized**—Product Instance is in authorized or in compliance state. Authorization is renewed every 30 days.
  - **Out of Compliance**—Product Instance reports license usage to Cisco SSM every 15 minutes. If your license consumption is more than the entitlements for five consecutive reporting intervals, the Product Instance is transitioned to the Out of Compliance state.

    The out-of-compliance period is for 90 days, within which you need to purchase the additional licenses. If you fail to take corrective action within the 90 days period, the Product Instance is transitioned to the Enforcement state.

- **Authorization Expired**—Product Instance authorization has expired. This usually happens when the product has not communicated with Cisco SSM for more than 90 days. It is in an overage period for 90 days before restrictions are enforced.

- **Enforcement State**

  When the 90 day period of Out-of-Compliance, Evaluation Period or Authorization period has expired, the Product Instance is moved to the Enforcement state in which system operations are impacted for Contact Center components. The Product Instance is in the Enforcement state in the following scenarios:

  - **Out-of-Compliance expiry**—When the out-of-compliance period of 90 days has expired.

    Purchase new licenses to exit the Enforcement state.

  - **Authorization expiry**—When the Product Instance has not communicated with Cisco SSM or Cisco SSM On-Prem for 90 days and has not automatically renewed the entitlement authorizations.

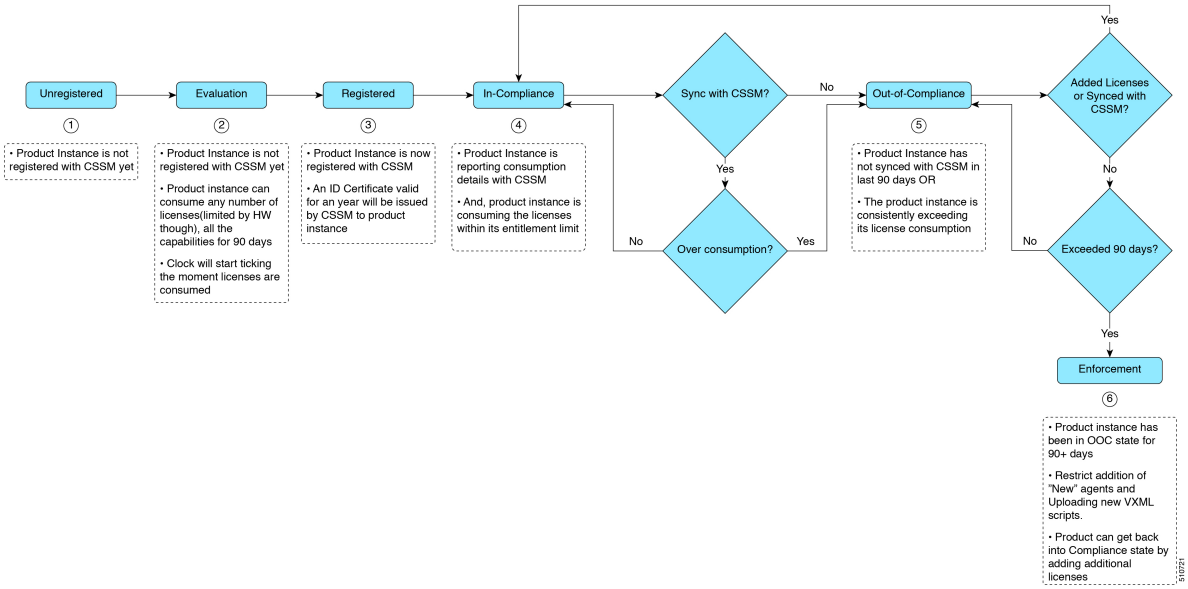
    Renew the license authorizations to exit the Authorization expiry state.

  - **Evaluation expiry**—When the license evaluation period of 90 days has expired and the Product Instance is not registered with Cisco SSM.

    Register the Product Instance with Cisco SSM to exit the evaluation expiry state.

A pictorial representation of different license states is as follows:

Figure 5: License States



Notifications and Alerts

The system maintains real-time status of license usage after Product Instances are registered and activated. Administrators are notified through alerts, event logs, and emails on the status of licenses in the Smart and Virtual Accounts. Pay attention to system alerts and banners to get regular information on compliance status and take necessary action.

Following are some of the notification methods:

- Banner Notifications
- System Alerts

Banner Notifications

- The banner displays the aggregate license compliance status on the Unified CCE Administration portal. The banner is displayed only when any of the product instances in the deployment is in the Evaluation, Out-of-Compliance, or Enforcement state.

  The **License Compliance report** displays the license status of product instances in the deployment. The reporting hierarchy is Enforcement, Out-of-Compliance, and Evaluation. This means that if any of the product instances in the deployment is in the Enforcement state, the banner displays Enforcement state as the overall status. Click the **Learn More** option to view the consolidated **License Compliance report**.

- When licenses are consumed in a Non-Production System, a banner message, "You are using a Non-Production System", is displayed.

System Alerts

Smart Licensing related system alerts, which get auto-corrected, are displayed in Unified CCE Administration portal when:

- Smart License state is not initialized
- Smart Agent is not enabled
- Serial number is not generated

In the above conditions, a red system alert is displayed in the **Alerts** button on the Unified CCE Administration portal. The red circle against the name of the machine in the inventory indicates the identified issue and the immediate action needed. After the issue is resolved, a green circle against the name of the machine indicates the system is running fine, for example, when the Smart Agent is enabled or Smart License state is initialized.

License Consumption Calculation

The system reports peak license usage to Cisco SSM every 15 minutes. If in five consecutive reports you are seen to have consumed more licenses than you are authorized to, the Product Instance is pushed to the Out-of-Compliance state. The Out-of-Compliance period is for 90 days, within which you need to purchase additional licenses. If you do not take corrective action within the 90 days period, the Product Instance is pushed to the Enforcement state in which, some of the operations are impacted.

Log in to Cisco SSM to view the detailed license consumption. Cisco SSM reports purchased quantity, in-use quantity, and balance licenses. At a quick glance, you can decide if the consumption of your licenses are in deficit or surplus, based on which you can make the right decision on the number of licenses that are required.

License Computation Scenario 1

License purchased: 100 licenses

Figure 6: License Computation

If Cisco SSM registers consecutive five instances of license over usage, the Product Instance transitions to Out-of-Compliance. Thereafter, the Product Instance reports Locked usage quantity (130 in the above scenario)

until the deficit licenses (130-100=30) are purchased. The Locked usage is the highest number of license usage (130) in the Out-of-Compliance state. The Product Instance will not report the actual license usage when the Product Instance is in the Out-of-Compliance state.

Purchase additional licenses from the Cisco Commerce website (CCW) to exit the Out-of-Compliance state.

Reported Usage column in the **License Management** page displays the locked usage quantity. However, the actual license usage is available in the **License Consumption** report of CUIC.

For more information, see *Cisco Unified Contact Center Express Reporting User Guide*.

License Computation Scenario 2

If Cisco SSM reports only two consecutive instances of license over usage within a one-hour window, the Product Instance will not transition to Out-of-Compliance. For example:

License Purchased: 100 licenses

Figure 7: License Computation

In the example, the Product Instance is back to In-compliance state after two instances of overage. The next time the Product Instance goes Out-of-Compliance, the count will be 1 of 5. So, you get 45 min (after the first Out-of-Compliance notification from Cisco SSM) to bring back the consumption within the acceptable range to stay in the In-compliance state.

Note To know about the agent license that is consumed by the Standard and Premium licenses, see the *Cisco Collaboration Flex Plan Contact Center Data Sheet* at https://www.cisco.com/c/en/us/products/collateral/unified-communications/cisco-collaboration-flex-plan/datasheet-c78-741220.html

New Deployments

For new deployments, buy the licenses on Cisco Commerce website at https://apps.cisco.com. Begin to use the product by using the licenses from your Smart Account.

Migrate to Smart Licensing

PAK-Based Migration

Migrate to Smart Licensing for fulfilled, partially fulfilled, and unfulfilled PAKs.

1. Log in to the Traditional Licensing Portal at https://tools.cisco.com/SWIFT/LicensingUI/Home.
2. Locate the PAKs that are to be migrated.
3. Right click and select **Assign to Smart Account and Virtual Account**.
4. Select the Smart Account and Virtual Account to which the PAK will be assigned.

   Once done, the classic PAKs will show assigned Smart Account.

Using LRP

1. Select the PAK that needs to be converted to smart entitlement.
2. From the PAK context option, select **Convert to Smart Licensing.**
3. Select the **SKUs**, **Quantity to Convert** and click on **Submit**.

Note Classic Licenses that are partially converted will need new Classic License file for managing the remaining Classic Licenses.

After the licenses are converted to smart entitlements, successful conversion message is shown. The entitlements will be available on Cisco SSM under selected Smart and Virtual Account.

Using Cisco SSM

Convert PAKs to equivalent Smart Licenses.

1. Go to the **Convert PAKs** tab.

   Assigned PAKs are listed on the Cisco SSM portal.
2. Click **Convert to Smart License** in the **Actions** column.
3. Select **SKUs** and **Quantity to Convert** and click **Next**.

   Classic Licenses which are partially converted will need new Classic License file for managing the remaining Classic Licenses.
4. Review and to confirm click **Convert License**.

   Once converted to Smart Entitlement, the old classic licenses will be invalidated. Converted Smart Licenses are added into the Smart Account and the Virtual Account.

Device-Based Conversion

Use the device-based Smart Licensing to convert the Classic licenses to smart entitlements.

Using LRP

1. Login to the Traditional Licensing Portal at https://tools.cisco.com/SWIFT/LicensingUI/Home
2. Go to **Devices** tab and then **Add Device**.
3. Locate the device to be migrated (filter using the device UUID). Once added, the added device shows up under **Devices** tab.
4. Select the device and right click **Assign to Smart Account** to Smart Account and Virtual Account.
5. Select the Smart Account and the Virtual Account.

   Once done, the table is updated with the Smart Account assigned to the device.
6. For Classic licenses to be converted to smart entitlements, select the device and select **Convert licenses to Smart Licensing** option.

7. Select the SKUs and **Quantity to Convert**.

   Classic Licenses which are partially converted will need new Classic License file for managing the remaining Classic Licenses.

8. Confirm and click **Submit**.

   Once the licenses are fully converted, the device UUID will be removed from the LRP. Once done, the successful conversion message is shown. The entitlements will now be available on Cisco SSM under selected Smart and Virtual Account.

Using Cisco SSM

Assigned Devices show up on the Cisco SSM Portal. The Cisco SSM portal is refreshed every hour. If the assigned device is not visible in Cisco SSM, please recheck after an hour.

1. Go to **Convert Licenses** tab and click the **License Conversion wizard.**
2. Select the **Product family** and provide the device UUID.
3. Select the **SKU** and **Quantity to Convert**.

   Classic Licenses which are partially converted will need new License file for managing the remaining Classic Licenses.

4. Review, Confirm and click **Submit.**

   When the conversion is complete and smart licenses are active, the classic licenses are invalidated.

License Management

Smart Licensing can be managed by using Cisco SSM and .

- **Cisco SSM—**Cisco SSM enables you to manage all your Cisco smart software licenses from a centralized website. With Cisco SSM, you organize and view your licenses in groups called virtual accounts (collections of licenses and product instances).

  You can access Cisco SSM from https://software.cisco.com, by clicking the Smart Software Licensing link under the License menu.

- **License Management in Unified CCE Administration portal—**Using the License Management option in the Unified CCE Administration portal, you can register or deregister the product instance, select your License Type, set transport settings or view the licensing consumption summary.

Smart Licensing Tasks

After you successfully register Smart Licensing, you can perform the following tasks as per the requirement:

- **Renew Authorization**—The license authorization is renewed automatically every 30 days. Use this option to manually renew the authorization.
- **Renew Registration**—The initial registration is valid for one year. Registration is automatically renewed every six months. Use this option to manually renew the registration.
- **Reregister**—Use this option to forcefully register the product instance again.

- **Deregister**—Use this option to release all the licenses from the current virtual account.

Renew Authorization and Renew Registration are automated tasks that take place at regular intervals. If there is a failure in the automated process, you can manually renew authorization and registration.

For more information, see *Smart License Management* section in *Cisco Unified Contact Center Express Admin and Operations Guide*.

Note You have to Deregister and Reregister manually.

Renew Authorization

The license authorization is renewed automatically every 30 days. The authorization status expires after 90 days if the product is not connected to Cisco SSM or Cisco SSM On-Prem.

Use this procedure to manually renew the License Authorization Status for all the licenses listed in the License Type.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management.**

Step 2 Click **Action** > **Renew Authorization**.

This process takes a few seconds to renew the authorization and close the window.

Renew Registration

Use this procedure to manually renew your certificates.

The initial registration is valid for one year. Renewal of registration is automatically done every six months, provided the product is connected to Cisco SSM or Cisco SSM On-Prem.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management** .

Step 2 Click **Action** > **Renew Registration**.

This process takes a few seconds to renew the authorization and close the window.

Reregister License

Use this procedure to reregister HCS for CC with Cisco SSM or Cisco SSM On-Prem.

Note Product can migrate to a different virtual account when reregistering with the token from a new virtual account.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management.**

Step 2 Click **Action** > **Reregister**.

Step 3 In the **Smart Software Licensing Product Registration** dialog box, paste the copied or saved Registration Token Key that you generated using the Cisco SSM or Cisco SSM On-Prem in the Product Instance Registration Token text box.

Step 4 Click **Reregister** to complete the reregistration process.

Step 5 Close the window.

Deregister License

Use this procedure to deregister HCS for CC from Cisco SSM or Cisco SSM On-Prem and release all the licenses from the current virtual account. All license entitlements that are used for the product are released to the virtual account and is available for other product instances to use.

Note If HCS for CC is unable to connect to Cisco SSM or Cisco SSM On-Prem, and the product is deregistered, then a confirmation message notifies you to remove the product manually from Cisco SSM or Cisco SSM On-Prem to free up licenses.

Note After deregistering, the product reverts to the Evaluation state if the evaluation period is not expired. All the license entitlements that are used for the product are immediately released to the virtual account and are available for other product instances to use them.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management** .

Step 2 Click **Action** > **Deregister**.

Step 3 On the **Confirm Deregistration** dialog box, click **Yes** to deregister.

Best Practices

Some of the best practices for Smart Licensing are:

- Before purchasing your licenses, run the License Consumption report on the existing system to understand the consumption pattern to make the right purchase decisions on the license requirement.
- Configure Admin email address in Cisco SSM to receive notifications and alerts from Cisco SSM.

Provision Unified CCE Using Unified CCDM

Complete the following procedures to provision the Unified CCE using Unified Contact Center Domain Manager (Unified CCDM).

- Manage Roles , on page 263
- Configure Gadgets, on page 270

CRUD Operations for Unified CCDM Objects

The following table mentions the Create, Read, Update, and Delete (CRUD) operations for Unified CCDM objects.

Note Bulk upload supports only the create operation. See Bulk Operations Using Unified CCDM, on page 248.

You cannot edit any default resources in CCDM portal.

Object	Create	Read	Update	Delete	Bulk Upload
Bucket Interval, see Configure Call Type, on page 221.		x			
ECC Variables, see Configure Expanded Call Variable, on page 231.	x	x	x	x	
Network VRU Script, see Configure Network VRU Scripts, on page 227.	x	x	x	x	x
Call Type, see Create a Call Type, on page 221.	x	x	x	x	x
Dialed Number, see Configure Dialed Number, on page 229.	x	x	x	x	x
Skill Group, see Configure Skill Group, on page 242.	x	x	x	x	x
Folder, see Configure Folder, on page 234.	x	x	x	x	x
Group, see Configure Group, on page 235.	x	x	x	x	
Agent, see Configure Agents, on page 216.	x	x	x	x	x
Agent Desktop, see Configure Agent Desktop, on page 219.	x	x	x	x	x
Agent Team, see Configure Agent Team, on page 220.	x	x	x	x	x

Object	Create	Read	Update	Delete	Bulk Upload
Person, see Configure Person, on page 238.	x	x	x	x	x
User, see Configure User, on page 212.	x	x	x	x	x
User Variable, see Configure User Variable, on page 247.	x	x	x	x	x
Enterprise Skill Group, see Configure Enterprise Skill Group, on page 230.	x	x	x	x	x
Label, see Configure Label, on page 237.	x	x	x	x	x
Attribute, see Configure Precision Attribute, on page 223.	x	x	x	x	x
Precision Queue, see Configure Precision Queue, on page 225.	x	x	x	x	x
Service, see Configure Service, on page 241	x	x	x	x	

Configure User

Complete the following procedures to configure a user:

- Create Users in Active Directory, on page 161
- Create User, on page 212
- Assign Roles to Users, on page 214
- Assign Permission to Sub-customer Tenant and User, on page 214
- Edit User, on page 215
- Delete User, on page 215

Create User

Note Login as administrator to create tenant/sub customer user.

Procedure

Step 1 In Unified CCDM portal, click burger icon in the top-left corner and select **Security** > **Users**.

Step 2 Select the tenant in which you have to create user and click **New**.

Step 3 Enter **Login Name**.

Step 4 Enter **First Name**, **Last Name** and **Description**.

Step 5 From **Culture** drop-down list, select **English (United States)** option.

Step 6 Check the following check boxes:

Advanced Mode

- **Account Enabled**
- **Password Never Expires**
- **User Cannot Change Password**
- **Internet Script Editor Enabled** (applicable for ISE user)

Step 7 In **User Home Folder** field, ensure that selected path is correct.

Ensure that **Create a new folder for this user** check box is unchecked.

Step 8 Enter **Password** and **Confirm** the password.

Step 9 Click **Save**.

Configure an Imported Unified CCE User

After integration of Unified CCE with Unified CCDM, Unified CCDM import existing Unified CCE users. All imported users are located in default import location, move the imported users to appropriate tenants/folders.

Follow the below steps to configure imported users.

Procedure

Step 1 In Unified CCDM, locate the imported Unified CCE user. Edit the username of Unified CCDM as follows:

<*username*>@<*domainname*>, where *username* is a windows username and *domainname* is a fully qualified windows domain name.

Example:

iseuser1@testdomain.local

Step 2 Select the user to view the details.

Step 3 Select **Details** tab and check the following check boxes:

- **Account Enabled**
- **Advanced Mode**
- **Internet Script Editor** (applicable for ISE user)

Step 4 Click **Save** to update the user details for the linked Unified CCDM user.

Note Before you login ISE, if SSO is disabled, you must log in to Unified CCDM portal as imported Unified CCE user. Enter corresponding windows active directory user password in **Password** field.

Assign Roles to Users

Follow the below procedure to assign corresponding roles to the user:

Procedure

Step 1 In Unified CCDM portal, click burger icon in the top-left corner and select **Security** > **Users**.

Step 2 Select newly created user from the list.

Step 3 Select **Group** tab, click **Add to Group**.

Step 4 Select the tenant/folder that has a user you want to assign roles.

Step 5 Check **Basic Users** check box to provide basic permission for the tenant.

Step 6 Check **Advanced Users** check-box for a tenant/ISE user and click **OK**.

Default, advanced users will have **Browse Dimension** permission.

Step 7 Check **Supervisors** check-box for a supervisor user and click **OK**.

Step 8 Click **Save**.

Assign Permission to Sub-customer Tenant and User

Procedure

Step 1 Log in to CCDM Web portal.

Step 2 Click burger icon.

Step 3 Select **Security** > **Permissions**.

Step 4 Select the sub-customer tenant and click **Permission** tab, uncheck **Inherit Permissions from /Root** and click **OK**.

Repeat this step for **Unallocated** > **SCCTenant Folder**.

Step 5 Select newly added user and click **Group** tab.

Step 6 Click **Add to Groups**.

Step 7 Click **Unallocated** > **SCCTenant Folder** and enable **Basic Users** permissions.

Step 8 Click the sub-customer tenant and assign **Advanced Users** permissions and click **OK**.

Default, **Advanced User** will have **Browse Dimension** permission.

Step 9 Click **Save**.

Edit User

Follow the below procedure to edit user:

Procedure

1. In Unified CCDM portal, click burger icon in the top-left corner and select **Security** > **Users**.
2. From the folder tree, select the folder containing the user that you want to edit.
3. Select the user you want to edit.
4. Click **Details** tab.
5. Edit the required details.
6. Click **Groups** tab, to add or remove the groups.
7. Click **Save**.

Delete User

Follow the below procedures to delete users:

Procedure

1. In Unified CCDM portal, click burger icon in the top-left corner and select **Security** > **Users**.
2. From folder tree on left, select the folder containing the user that you want to delete.
3. Select the user that you want to delete.
4. Click **Delete** and click **Yes**.

Configure Departments

To configure a department perform the following instructions.

- Create a Department, on page 215
- Edit a Department, on page 216
- Move a Department, on page 216
- Delete a Department, on page 216

Create a Department

Procedure

1. Log in to CCDM portal as Tenant Administrator.
2. Click the burger icon and select **Provisioning** > **Resource Manager**
3. Select the required Folder from the Tenant. Click **Resource** and select **Department**.
4. Enter the name of the department and complete the mandatory fields.

Step 5 Click **Save**.

Edit a Department

Procedure

Step 1 Log in to CCDM portal as Tenant Administrator.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**
Step 3 Expand the required Folder from the Tenant. Click **Department**.
Step 4 Select the department that you want to edit and modify the required fields.
Step 5 Click **Save**.

Move a Department

Procedure

Step 1 Log in to CCDM portal as Tenant Administrator.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**
Step 3 Expand the required Folder from the Tenant. Click **Department**.
Step 4 In **Department** tab, check the department you want to move and click **Move**.
Step 5 Browse to the destination folder you want the department to be moved and click **Save** and click **Ok**.

Delete a Department

Procedure

Step 1 Log in to CCDM portal as Tenant Administrator.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**
Step 3 Expand the required Folder from the Tenant. Click **Department**.
Step 4 In the **Department** tab, Select the department that you want to delete.
Step 5 Click **Delete** and click **Ok**.

Configure Agents

Complete the following procedures for agent configuration:

- Create an Agent, on page 217
- Edit an Agent, on page 218

- Delete an Agent, on page 218

Create an Agent

Complete the following procedure to create an agent:

Procedure

Step 1 Log in to CCDM portal as tenant or sub customer user or Supervisor user.

Step 2 Click the burger icon and select **Provisioning**.

Step 3 Create an agent.

- For Tenant or Sub customer user, select **Resource Manger**, select the folder that you want to create the agent. Select **Resource** > **Agent**.
- For Supervisor user, select **Agent Team Manager** and click **New Agent**.

Step 4 Click the **Details** tab and configure as follows:

a) Enter the Agent's Name.
b) Enter a Description of the agent.
c) Select a Peripheral to create the agent.
d) Associate the person with the agent.

You can choose an existing person, or you can create a new person and associate with the agent.

- **Select Existing Person**: Select an existing person from the drop-down list, . You can search for a specific person by typing a part of their name in the search box. The new agent uses the details specified in that person's Peripheral Login box to log in to their Agent Desk Setting.
- **Create New Person**: Enter the first name and last (or family) name for the person, and fill in the details they will use to log in to the peripheral. The person is automatically created and associated with the agent.

e) If Unified CCE is in hybrid mode , check the **SSO** checkbox to make the agent a SSO agent.

Step 5 To make agent a supervisor, click **Supervisor** tab and check the **Supervisor** checkbox. If supervisor is a non-SSO agent, do the following:

a) Associate the agent with a Domain Account (the account the agent uses to log into a computer on the contact center network).

Note You cannot set up a domain account from Unified CCDM because security rules typically prevent this. Contact your administrator if you are uncertain of the domain account to use.

b) Enter part of the account name, click **Find** and then select the correct account.

Step 6 Click the **Agent Teams** tab and configure the following:

a) Select an agent team to which the agent belongs to. Agents may only be a member of a single team, but a supervisor can supervise multiple teams. Use the Selected Path drop-down list to see agent teams in other folders.
b) Click **Add** to associate the team with this agent.
c) Check the **Member** check box to make the agent a member of the team.

Supervisors can supervise a team without being a member.

d) If the agent is a supervisor, select a primary or secondary supervisory role for any team they supervise..

They may or may not also be a member of this team.

Step 7 Click the **Skill Groups** tab and configure the following:

a) Select skill groups for the agent to belong to. Use the Selected Path drop-down to change folders.
b) Click **Add** to add the agent to the selected skill groups.

Step 8 Click **Save**.

Edit an Agent

Complete the following procedure to view or edit agents.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 In **Resource Manager**, in the folder tree panel, select the folder where you want to edit the agent.

Step 4 In **Items** panel, select the agent from the list.

Step 5 Edit the agent details.

Clicking a different tab (such as Supervisor or Agent Teams) shows a different set of fields. You can return to previous tabs if necessary.

Step 6 Click **Save**.

Delete an Agent

Complete the following procedure to delete an agent.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 In **Resource Manager**, navigate to the folder containing the Agent you want to delete, and view the agents in that folder using the Items panel list view.

Step 4 In the Items panel, check the required agent check boxes that you want to delete.

Step 5 Click **Delete**.

Step 6 Click **Yes** to delete the agent.

Configure Agent Desktop

Complete the following procedures to configure an agent desktop:

- Create an Agent Desktop, on page 219
- Edit an Agent Desktop, on page 219
- Delete an Agent Desktop, on page 219

Create an Agent Desktop

Complete the following procedure to create an agent desktop.

Procedure

Step 1 Login to Unified CCDM Portal as Tenant or Sub customer user and select **Resource Manager**.

Step 2 In **Resource Manager**, in the Folder Tree panel, select the folder where you want to create the agent desktop.

Step 3 Click **Resource**, and click **Agent Desktop**.

Step 4 Complete the required fields.

Step 5 Click **Save**.

Edit an Agent Desktop

Complete the following procedure to edit an agent desktop.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder that contains the agent desktop you want to edit, and view the agent desktops in that folder using the Items panel list view.

Step 4 In the **Items** panel, click the agent desktop you want to edit.

The details of this agent desktop appears in the Details panel.

Step 5 In the **Details** tab, click the appropriate tab and make the required changes.

Step 6 Click **Save**.

Delete an Agent Desktop

Complete the following procedure to delete the agent desktop.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder that contain the agent desktop you want to delete, and view the agent desktops in that folder using the Items panel list view.

Step 4 In the Items panel, check the check box or check boxes of the agent desktops you want to delete.

Step 5 Click **Delete** and Click **Yes**.

Note Deletion of agent desktop will remove the associated agent desktops automatically.

Configure Agent Team

Complete the following procedures to configure an agent team:

- Create an Agent Team, on page 220
- Edit an Agent Team, on page 220
- Delete an Agent Team, on page 221

Create an Agent Team

Complete the following procedure to create an agent team:

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 In the folder tree panel, select the folder where you want to create the agent team.

Step 4 Click **Resource**, and then click **Agent Team**.

Step 5 Enter a unique name for the team.

Step 6 Enter all the required fields to create the agent team.

Step 7 To assign agents to the team, check the check boxes of one or more agents in the Agents tab, and click **Add**.

Step 8 When you add an agent to the team, you must also check their Member check box to make them a member of the team.

This is because it is possible to be involved with a team without being a member, by supervising it.

If an agent is a supervisor, a drop-down list appears in the right-hand column.

Step 9 Specify whether the agent has a supervisory role for this particular team.

Step 10 Click **Save**.

Edit an Agent Team

Complete the following procedure to edit an agent team.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder that contain the agent team you want to edit, and view the agent teams in that folder using the Items panel list view.

Step 4 In the **Items** panel, click the agent team you want to edit.

The details of this agent team appear in the Details panel.

Step 5 Click through the tabs and edit the fields you want to change.

Step 6 To remove agents from a team, click the **Agents** tab and check the check boxes of the agents you wish to remove from the team and click **Remove**.

Step 7 Click **Save.**

Delete an Agent Team

Complete the following procedure to delete an agent team

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder that contains the agent teams you want to delete, and view the agent teams in that folder using the Items panel list view.

Step 4 In **Items** panel, check the check box or check boxes of the agent teams you want to delete.

Step 5 Click **Delete.**

Delete Agent Teams confirmation dialog box appears.

Step 6 Click **Yes** to delete the agent teams.

Configure Call Type

Create a Call Type

Complete the following procedure to create a call type.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 In folder tree panel, select a folder where you want to create the call type.

Step 4 Click **Resource**, and then click **Call Type**.

Step 5 Enter the following details:

a) In **Name** field, enter the unique name.

b) Select **Bucket Interval** from the drop-down list.

Note The bucket interval is the count of answered or abandoned calls that are used as intervals for the Call Type. The default value is system default.

c) Select **Service Level Threshold** from the drop-down list.

d) Select **Service Level Type** from the drop-down list.

Step 6 Click **Save**.

Edit a Call Type

Complete the following procedure to edit a call type.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder that contain call types that you want to delete, and view the call types in that folder using the Items panel list view.

Step 4 In **Items** panel, select the call types you want to edit.

Step 5 Click through the tabs and edit the fields you want to change.

Step 6 Click **Save**.

Delete a Call Type

Complete the following procedure to delete a call type.

Note You cannot delete the default call type.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder containing the call types you want to delete and under Summary in Items panel list view click **Call Type** .

Step 4 In **Items** panel, select the call types you want to delete.

Step 5 Click **Delete** and click **Yes**.

Configure Precision Routing

Complete the following procedures to configure precision routing.

- Configure Precision Attribute, on page 223
- Assign Precision Attribute to an Agent, on page 224
- Configure Precision Queue, on page 225
- Create Routing Scripts, on page 226

Configure Precision Attribute

Complete the following procedures to configure precision attribute.

- Create Precision Attribute, on page 223
- Edit Precision Attribute, on page 223
- Delete Precision Attribute, on page 224

Create Precision Attribute

Complete the following procedure to create a precision attribute.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the required tenant to create precision attribute.

Step 4 Click **Resource**, and click **Precision Attribute**.

Step 5 Provide a Name for the precision attribute. For example, **ENGLISH**.

Step 6 Enter the Description for the precision attribute.

Step 7 Select the Data Type for the precision attribute. For example, **Proficiency**.

Step 8 Select the **Default Value** from the drop-down list.

Step 9 Click **Save**.

Edit Precision Attribute

Complete the following procedure to edit a precision attribute.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 In **Resource Manager**, select the folder containing the precision attribute you want to edit, and view the precision attributes in that folder using the Items panel list view.

Step 4 In the Items panel, click the precision attribute you want to edit.

The details of this precision attribute appears in the Details panel.

Step 5 In the Details panel, click the appropriate tab and make the desired changes.

Step 6 Click **Save**.

Note The precision attribute of a data type cannot be modified once it is assigned. However, the default value of the data type can be modified.

Delete Precision Attribute

Complete the following procedure to delete a precision attribute.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 In **Resource Manager**, select the folder containing the precision attribute you want to delete, and view the precision attributes in that folder using the Items panel list view.

Step 4 In **Items** panel, check the check boxes of the precision attributes that you want to delete.

Step 5 Click **Delete**.

Note You cannot delete the precision attribute if it is referenced by a precision queue, remove the reference to delete the precision attribute.

Step 6 Click **Yes**.

Assign Precision Attribute to an Agent

Complete the following procedure to assign the precision attribute to an agent.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 In **Resource Manager**, navigate to the folder containing the agent to which you want to assign the precision attribute and view the agent in that folder using the **Items panel** list view.

Step 4 In the Items panel, click the agent to which you want to assign the precision attribute.

The details of this agent appear in the Details panel.

Step 5 In the Details panel, click **Precision Attribute**. Check the check box against the precision attribute tab and click **Add**.

Step 6 Click **Save**.

Note The supervisor agent must be associated with a domain account before they can have precision attributes assigned to them.

Configure Precision Queue

Complete the following procedures to configure precision queue.

- Create Precision Queue , on page 225
- Edit Precision Queue, on page 225
- Delete Precision Queue, on page 226

Create Precision Queue

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the required tenant to create the precision queue.

Step 4 Click **Resource**, and click **Precision Queue**.

A new page appears.

Step 5 Complete the required fields

Step 6 Select the **Steps** tab and click **Step1**. A new page appears.

Step 7 In the Expression1 field, provide the attribute name and select the operation from the drop-down list and also select Proficiency level from the drop-down list. For example, Attribute = **ENGLISH**, Operation is >, and Proficiency level is **6**.

Note Based on the requirement, we can add the attribute, expression and steps.

Step 8 Click **OK**.

Step 9 Click **Save**.

Edit Precision Queue

Complete the following procedure to edit a Precision Queue.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 In **Resource Manager**, select the folder containing the Precision Queue you want to edit, and view the Precision Queue in that folder using the **Items panel** list view.

Step 4 In the Items panel, click the Precision Queue that you want to edit.

The details of this Precision Queue appears in the Details panel.

Step 5 In the Details panel, click the appropriate tab and make the desired changes.

Step 6 Click **Save**.

Delete Precision Queue

Complete the following procedure to delete the Precision Queue.

Note You cannot delete a precision queue that is referenced in a routing script, remove the reference to delete the precision queue.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 In **Resource Manager**, navigate to the folder containing the Precision Queue you want to delete and view the Precision Queue in that folder using the **Items panel** list view.

Step 4 In the Items panel, check the check boxes of the Precision Queue that you want to delete.

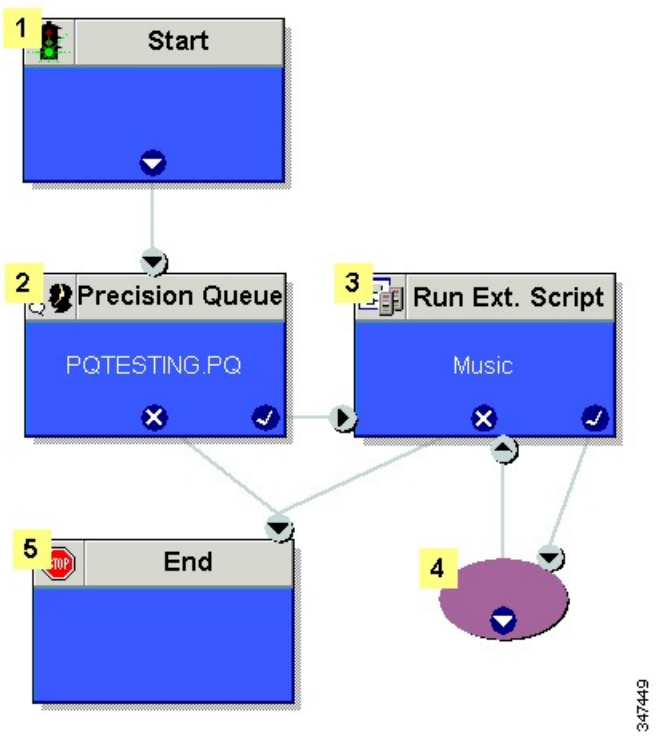
Step 5 Click **Delete**.

Step 6 Click **Yes**.

Create Routing Scripts

See the following illustration to create routing scripts:

Figure 8: Create Routing scripts



Configure Network VRU Scripts

Create Network VRU Script

Complete the following procedure to set up the network VRU script.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder where you want to create the network VRU Script.

Step 4 Select **Resource**, and click **Network Vru Script**.

Step 5 Complete fields as follows:

a) Name* (Required)- Enter a unique name that will identify the script.

Example:

Play_Welcome

b) Network VRU* (Required) - Select the Network VRU from the drop-down list.

c) VRU Script Name* (Required)- Enter the name of the script as it is known on the Unified CVP.

d) Configuration Parameter (Optional)- A string used by Unified CVP to pass additional parameters to the IVR Service. The content of string depends on the micro-application to be accessed.
e) Timeout* (Required)- Enter a number to indicate the number of seconds for the system to wait for a response from the routing client after directing it to run the script.
f) Interruptible (Optional)- This check box indicates whether or not the script can be interrupted; for example, when an agent becomes available to handle the call.

Note
- System generates a default Enterprise Name in **Advance** tab.
- You cannot upload an audio file, when you first create the network VRU script.

Step 6 Click **Save**.

Edit Network VRU Scripts

Complete the following procedure to edit Network VRU details and associate an audio file with a VRU script:

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select the folder containing the **Network VRU script** you want to edit.
Step 4 In the **Items panel**, click the **Network VRU script** you want to edit.
Step 5 Click the **Audio** tab.
Step 6 Click **Browse** and select the audio file from your hard drive.
Step 7 Click **Upload**.
Step 8 After the file has uploaded, click **Save**.

Delete Network VRU Scripts

Note You cannot delete the dialed number that is referenced in a script. This reference should be removed to delete the dialed number.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select the folder containing the **Network VRU script** you want to delete.
Step 4 In the **Items panel**, click the **Network VRU script** you want to delete.
Step 5 Select the **Delete** option.

Step 6 Click **Yes**, to delete the Network VRU script.

Configure Dialed Number

Complete the following procedures for dialed number configuration:

- Create a Dialed Number, on page 229
- Edit a Dialed Number, on page 229
- Delete a Dialed Number, on page 230

Create a Dialed Number

Complete the following procedure to create one or more dialed numbers.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder where you want to create the dialed number.

Step 4 Click **Resource**, and then click **Dialed Number**.

Step 5 Enter unique name of up to 32 characters for the dialed number.

This should consist alphanumeric characters, periods, and underscores only.

For wild card dialed number follow the pattern below:

Example:

7*xx*

Step 6 Complete fields as for the dialed number Fields.

Step 7 Click **Add** to specify the call types and other dialing information to be associated with this dialed number.

Step 8 Click **Save**.

Edit a Dialed Number

Complete the following procedure to edit the dialed numbers.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder where you want to edit, and view the dialed number in that folder using the **Items panel** list view.

Step 4 In the **Items panel**, select the dialed numbers that you want to edit.

Step 5 After modification, click **Save**.

Delete a Dialed Number

Complete the following procedure to delete one or more dialed numbers.

Note You cannot delete the dialed number that is referenced in a script, remove the reference to delete the dialed number.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select the folder containing the dialed numbers that you want to delete, and view the dialed numbers in that folder using the Items panel list view.
Step 4 In **Items** panel, select the dialed numbers to be deleted.
Step 5 Click **Delete**.
Step 6 Click **Yes**.

Configure Enterprise Skill Group

Complete the following procedures for enterprise skill group configuration:

- Create an Enterprise Skill Group, on page 230
- Edit an Enterprise Skill Group Configuration, on page 231
- Delete an Enterprise Skill Group, on page 231

Create an Enterprise Skill Group

Complete the following procedure to create an enterprise skill group.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select the folder where you want to create the enterprise skill group.
Step 4 Click **Resource**, and then click **Enterprise Skill Group**.
Step 5 Enter a unique name for the group.
Step 6 Enter all the required fields to create an enterprise skill group.
Step 7 To assign skill groups to the group, click **Add** and select one or more skill groups.

Step 8 Click **Save**.

Edit an Enterprise Skill Group Configuration

Complete the following procedure to edit an enterprise skill group.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 In the folder tree panel, select the folder where you want to edit, and view the enterprise skill groups in that folder using the **Items panel** list view.
Step 4 In the **Items panel**, select the enterprise skill groups that you want to edit.
Step 5 After modification, click **Save**.

Delete an Enterprise Skill Group

Complete the following procedure to delete an enterprise skill group.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select the folder containing the enterprise skill groups you want to delete, and view the enterprise skill groups in that folder using the Items panel list view.
Step 4 In the **Items** panel, check the check box or check boxes of the enterprise skill groups you want to delete.
Step 5 Click **Delete**.
Step 6 Click **Yes**.

Configure Expanded Call Variable

Complete the following procedures to configure an expanded call variable.

- Create an Expanded Call Variable, on page 231
- Edit an Expanded Call Variable, on page 232
- Delete an Expanded Call Variable, on page 232

Create an Expanded Call Variable

Complete the following procedure to create an expanded call variable.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder where you want to create the expanded call variable.

Step 4 Click **Resource**, and then click **Expanded Call Variable**.

Step 5 Enter the required information in the following fields:

a) In **Name** field, enter the unique name.
b) In **Description** field, enter the description.
c) In **Maximum Length** field, enter the maximum length of call variable.
d) Optional, check **Persistent** check-box.
e) Optional, check **Enabled** check-box.
f) Optional, check **ECC Array** check-box.

Step 6 In **Advanced** tab, set the end date for the call variable.

Note Uncheck **Forever** check-box to set the end date.

Step 7 Click **Save**.

Edit an Expanded Call Variable

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder where you want to modify the expanded call variable.

Step 4 Click **Expanded Call Variable** in the items panel.

Step 5 Select the Expanded Call Variable to modify.

Step 6 Modify the fields in Details tab as required.

Step 7 Click **Save**.

Delete an Expanded Call Variable

Complete the following procedure to delete expanded call variable.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder containing the expanded call variables you want to delete, and view the expanded call variables.

Step 4 In **Items** panel, select the expanded call variables that you want to delete.

Step 5 Click **Delete**.

Step 6 Click **Yes**.

Configure ECC Payload

Complete the following procedures to configure an expanded call variable.

- Create an ECC Payload, on page 233
- Edit an ECC Payload, on page 233
- Delete an ECC Payload, on page 234

Create an ECC Payload

Complete the following procedure to create an ECC Payload.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the Cisco icon and select **Gadget** > **Open App**. Create an App if it is not already created. For more information, see Configure Gadgets, on page 270.

Step 3 Select an **ECC payload** resource from the search bar list.

Step 4 Click the **New** icon.

Step 5 On the **Details** tab, enter the required information:

a) In the **Name** field, provide a name for the ECC Payload.

b) In the **Description** field, provide a suitable description for the ECC Payload.

Step 6 To add the Expanded Call Variable to the ECC Payload, on the **Expanded Call Variable** tab, click **Show Available**. Select the available call variable and add it to the ECC payload.

Step 7 On the**Advanced** tab, enter the Enterprise name and set the end date for the ECC payload.

Step 8 Click **Save**.

Edit an ECC Payload

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the Cisco icon and select **Gadget** > **Open App**.

Step 3 Select an **ECC payload** resource from the search bar list.

Step 4 Select the **ECC payload** to be modified.

Step 5 Modify the fields in the **Details** tab as required.

Step 6 Add or remove the ECC variable as required.

Step 7 Click **Save**.

Delete an ECC Payload

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the Cisco icon and select **Gadget** > **Open App**.
Step 3 Select the **ECC payload** resource from the search bar list.
Step 4 Select the **ECC payload** to be deleted and click **Delete**.
Step 5 Click **OK** to confirm the changes.

Configure Folder

Complete the following procedures for folder configuration:

- Create Folders, on page 234
- Rename a Folder, on page 235
- Move Folder, on page 235
- Delete Folder, on page 235

Create Folders

Complete the following procedures to create folders:

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select the folder/tenant where you want to create the new folder.
Step 4 Click **System**, and then click **Folder**.
Step 5 In the Name field enter a name for the new folder.
Step 6 In the Description field enter any explanatory text for the folder, this is optional.
Step 7 If required, uncheck the **Inherit Permissions** check box to make this folder a policy root that does not inherit security permissions from its parent folder.
Step 8 Check the **Create Another** check box if you want to create more folders at the same point in the tree structure.
Step 9 Click **Save** to save the new folder in the tree.

Rename a Folder

Procedure

In **Resource Manager**, right-click the folder in the Folder Tree panel and select **Rename Folder** and enter the required name.

Move Folder

Complete the following procedure to move a folder:

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 In the Items panel, click **Folders**.
Step 4 Check the folder(s) check box that you want to move.
Step 5 Click **Move**.
Step 6 In the folder tree, select the location that you want to move the folders.
Step 7 Click **Save**.

You can also use drag and drop option to move folders.

Delete Folder

Complete the following procedures to delete a folder:

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 In the Items panel, click **Folders**.
Step 4 Check the folder(s) check boxes that you want to delete.
Step 5 Click **Delete**.
Step 6 In the Delete folder dialog, select **Yes**.

Configure Group

Complete the following procedure for group configuration:

- Create a Group, on page 236

- Edit a Group, on page 236
- Move a Group, on page 237
- Delete a Group, on page 237

Create a Group

Complete the following procedure to create a group.

Procedure

Step 1 Log in to Unified CCDM Portal as Administrator/Tenant /Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager** .

Step 3 Select the folder or the tenant where you want to create the new group.

Step 4 Click **System** , and then click **Group**

Step 5 Enter the following details:

a) In the Name field enter the name for the new group.

Groups in different folders may have the same name.

b) In the Description field enter a description for the group, such as a summary of its permissions or the categories of users it is intended for.

c) If you want to create more than one group, check the **Create Another** check box (to remain on the Create a new group page after you have created this group).

d) Click **Save**.

Edit a Group

Complete the following procedure to edit or view group details.

Procedure

Step 1 Log in to Unified CCDM Portal as Administrator/Tenant /Sub Customer user.

Step 2 Click the burger icon and select **Provisioing** > **Resource Manager** .

Step 3 Select the folder that contain groups that you want to modify, and view the group in that folder using the Items panel list view.

Step 4 In the **Items panel** , select the group that you want to edit.

Step 5 Edit the group details as required.

Step 6 Click the **Members** tab to add or remove the members of the group.

Step 7 Click the **Groups** tab to add or remove the group from other groups.

Step 8 Click **Save**.

Move a Group

Complete the following procedure to move a group.

Procedure

Step 1 Log in to Unified CCDM Portal as Administrator/Tenant /Sub Customer user.

Step 2 Click the burger icon and select **Provisioing** > **Resource Manager**.

Step 3 Select the folder that contain groups that you want to move, and view the group in that folder using the Items panel list view.

Step 4 In the **Items panel** , select the group to be moved.

Step 5 Click **Move.**

Step 6 Navigate to the tenant or the folder you want to move the group to.

Step 7 Click **Save.**

Delete a Group

Complete the following procedure to delete a group.

Procedure

Step 1 Log in to Unified CCDM Portal as Administrator/Tenant /Sub Customer user.

Step 2 Click the burger icon and select **Provisioing** > **Resource Manager** .

Step 3 Select the folder that contain groups that you want to delete, and view the group in that folder using the Items panel list view.

Step 4 In the **Items panel** , select the group that you want to deleted.

Step 5 Click **Delete** and confirm the deletion when prompted.

Configure Label

Complete the following procedures for label configuration:

- Create a Label, on page 237
- Edit a Label, on page 238
- Delete a Label, on page 238

Create a Label

Complete the following procedure to create a label.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select the folder where you want to create the label.
Step 4 Click **Resource**, and click **Label**.
Step 5 Complete all fields for the label.
Step 6 Click **Save**.

Edit a Label

Complete the following procedure to edit a label.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select the folder containing the labels that you want to edit, and view the labels in that folder using the **Items panel** list view.
Step 4 In the **Items panel**, select the labels that you want to edit.
Step 5 After modification, Click **Save**.

Delete a Label

Complete the following procedure to delete a label.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select the folder containing the labels you want to delete, and view the labels in that folder using the Items panel list view.
Step 4 In the Items panel, check the check box or check boxes of the labels you want to delete.
Step 5 Click **Delete**.
Step 6 In the Delete Labels dialog box, click **Yes**.

Configure Person

Complete the following procedures to configure a person:

- Create a Person, on page 239

- Edit a Person, on page 239
- Delete a Person, on page 240

Create a Person

Complete the following procedure to create a person.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user or Supervisor user.

Step 2 Click the burger icon and select **Provisioning**.

Step 3 Create a person.

- For Tenant or Sub customer user, select **Resource Manger**, select the folder that you want to create the agent. Select **Resource** > **Person**.
- For Supervisor user, select **Agent Team Manager** and click **New Person**.

Step 4 Complete the required fields for person.

Step 5 Select **Equipment** tab, select the Unified Contact Center Enterprise.

Step 6 Set Active from and to dates in the **Advanced** tab.

Step 7 Click **Save**.

Note After you create a person, you cannot edit the Unified CCDM account details for a person through another person. You must edit the Unified CCDM account details directly.

You cannot link a person with an existing Unified CCDM user account.

Edit a Person

Complete the following procedure to edit a person.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub-Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder containing the persons that you want to edit, and view the person in that folder using the **Items panel** list view.

Step 4 In the **Items panel**, select the persons that you want to edit.

Step 5 Optional, reset the password as follows:

a) Select **Details** tab.
b) Check **Reset Password** check box.
c) Enter new password and confirm.

Step 6 After modification, Click **Save**.

Delete a Person

Complete the following procedure to delete a person.

Note Deletes all the agents associated with the person.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select folder containing the person or persons you want to delete the persons in that folder using the Items panel list view.
Step 4 In the Items panel check the check box or check boxes of the person or persons you want to delete.
Step 5 Click **Delete**.
Step 6 Click **Yes** to delete the person.

Configure Supervisors

Complete the following procedure to configure a supervisor.

Before you begin

This is applicable for Sub-customer users of Small Contact Center Deployment that requires Supervisor to associate with Domain account.

1. Select **Security** > **Sub-customer Tenant**.
2. Select **User Tab** > **User** and click **Change Permission**.
3. Check **Full Permission** check-box for the Sub customer tenant and click **OK**.
4. Add this sub-customer tenant to **Advanced Group**.

Procedure

Step 1 Log in to the CCDM portal as Tenant/Sub Customer User and select **Resource Manager**.
Step 2 In **Resource Manager**, select the folder that contains the agent that you want as a supervisor or create a new agent to configure supervisor, see Create an Agent, on page 217.
Step 3 Click **Supervisor** tab and and check the **Supervisor** checkbox. This does not require that they supervise a team. If supervisor is a non-SSO agent, the **Supervisor** tab only displays the **Supervisor** checkbox. All other fields and checkboxes are not available when a default domain has been configured for Unified CCE 11.5 or later versions.

Note You cannot set up a domain account from Unified CCDM because security rules typically prevent this. Contact your administrator if you are uncertain of which domain account to use.

Step 4 Click **Save**.

Configure Service

Note Complete the following procedures to configure service:

- Create Service, on page 241
- Edit Service, on page 241
- Delete Service, on page 242

Create Service

Complete the following procedure to create service:

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select the folder that you want to create service from the left-hand side panel.
Step 4 In **Resource** drop-down list, select **Service** option.
Step 5 Complete the required fields.
Step 6 Goto **Advanced** tab, choose **Cisco_Voice** from **Media Routing Domain** drop-down list.
Step 7 Goto **Skillgroups** tab, check the skill group that you want to add and click **Add**.
Step 8 Click **Save**.

Edit Service

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Navigate to the folder that you want to edit or view service from the left-hand side panel.
Displays the list of all the services in items panel.
Step 4 Click on the service that you want to edit.
Step 5 After editing click **Save**.

Delete Service

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select the folder that you want to delete service from the left-hand side panel.
Step 4 Check the service from the list that you want to delete.
Step 5 Click **Delete** and click **Yes**.

Configure Skill Group

Complete the following procedures to configure skill group:

- Create a Skill Group, on page 242
- Edit a Skill Group, on page 242
- Delete a Skill Group, on page 243

Create a Skill Group

Complete the following procedure to create a skill group.

Note When you create a skill group, a default route is created.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 In the folder tree panel, select the folder where you want to create the skill group.
Step 4 Click **Resource**, and click **Skill Group**.
Step 5 Enter a unique name for the group.
Step 6 Select **Agents** tab, check the agent(s) check box and click **Add**.
Step 7 Click **Save**.

Edit a Skill Group

Complete the following procedure to edit a skill group.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder containing the skill group that you want to edit, and view the skill groups in that folder using the Items panel list view.

Step 4 In the Items panel, click the skill group you want to edit.

The details of this skill group display in the Details panel.

Step 5 Click the tabs and edit the fields you want to change.

Step 6 Optional, to remove agents from a skill group, select **Agents** tab and select the agents you want to remove from the team.

Step 7 Click **Remove**.

Step 8 Optional, to remove the route association from a skill group, select **Route** tab and click **Delete** for which route you want to delete.

Step 9 Optional, to edit the details of an existing route associated with the skill group, select **Route** tab and click **Edit** for which route you want to delete. Click **Update**.

Step 10 Click **Save**.

Delete a Skill Group

Complete the following procedure to delete a skill group.

Note You cannot delete the skill group that is referenced in a script, remove the reference to delete the skill group.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder containing the skill groups you want to delete, and view the skill groups in that folder using the Items panel list view.

Step 4 In the Items panel, select the skill groups you want to delete.

Note Ensure that skillgroup is not mapped to any services.

Step 5 Click **Delete**.

Delete Skill Groups page appears.

Step 6 Click **Yes**.

The skill groups are deleted.

Configure Route

Complete the following procedure to configure a route.

Procedure

Step 1	Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2	Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3	In the folder tree panel, select the folder where you want to create the route.
Step 4	In the Folder Tree panel, click **Skill Group**.
Step 5	Choose the skill group for which you are creating a route.
Step 6	Select **Routes** tab.
Step 7	In **Route Name** field, enter a unique name that will identify the script.
Step 8	Click **Add**.
Step 9	Click **Save**.

Agent Re-skilling and Agent Team Manager

You can login as user with supervisor role to perform agent re-skilling and agent team manager.

Before performing these tasks ensure that the user is created. To create user, see Create User, on page 212 and to assign supervisor role, see Assign Roles to Users, on page 214.

Configure Supervisor for Agent Re-skill and Agent Team Manager in CCDM

Procedure

Step 1	Log in to the Unified CCDM Portal as administrator.
Step 2	Click the burger icon and select **Provisioning** > **Resource Manager** .
Step 3	Click on resource and select **Agent** resource.
Step 4	Select an agent for the supervisor.
Step 5	In **Supervisor** tab, check the checkbox for supervisor and click **Save**.
Step 6	In **Person** tab, select the **goto person** icon.
Step 7	In **Portal** tab, click the portal account and click the existing user.
Step 8	Select the tenant and select supervisor user from the list of users.
Step 9	Click next icon. Displays **User's Group** dialog box.
Step 10	Make sure supervisor group is added to the user and click **Save**.
Step 11	Click **Save**.

Associating Supervisor Agent to Agent Team

Procedure

Step 1 Log in to Unified CCDM Portal as administrator.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Click resource and select **Agent** resource.
Step 4 Select the Supervisor agent.
Step 5 In the Agent Team tab, select agent teams that you want to add and click **Add**.
Step 6 In **Supervisory Role** column, Select **Primary** from the drop-down list and click **Save**.

View Skill Group

Complete the following procedure to view a skill group.

Procedure

Step 1 Log in to Unified CCDM portal as supervisor.
Step 2 Click the burger icon and select **Provisioning** > **Agent Re-Skilling**.
Step 3 From the **Skill Group** drop-down list, select the skill group you want to view.
Displays a list of agents for the selected skill group.
Step 4 Click the **Goto Agent** icon to modify the agent details

Add an Agent to Skill Group

Complete the following procedure to add an agent to a skill group.

Procedure

Step 1 Log in to Unified CCDM portal as supervisor.
Step 2 Click the burger icon and select **Provisioning** > **Agent Re-Skilling** .
Step 3 Select **Skill Group** from the drop-down list.
Displays a list of agents for the selected skill group.
Step 4 In **My Agents on Peripheral** list, select the agents you want to add to the skill group, then click **Add**.

Note You can search agents using a search bar with a part of agent's name.

Step 5 Click **Save**.

Remove an Agent from Skill Group

Complete the following procedure to remove an agent from a skill group.

Procedure

Step 1 Log in to Unified CCDM portal as supervisor.

Step 2 Click the burger icon and select **Provisioning** > **Agent Re-Skilling** .

Step 3 Select a skill group to remove an agent or agents.

Step 4 In the top list, select the agents to remove from the skill group using the check boxes.

Step 5 You enter part of an agent's name into the search box, and then click **Search** to filter the list of agents by the specified search string.

Step 6 Click **Remove** to remove the agents from this skill group.

Step 7 Click **Save** to save your changes, or **Cancel** to leave the details as they were before you started.

View Agent Team

Login as a supervisor user and complete the following procedure to view Agent team

Procedure

Step 1 Log in to Unified CCDM portal as supervisor.

Step 2 Click the burger icon and select **Provisioning** > **Agent Team manager** .

Step 3 Select the **Agent team** drop-down list and select the agent team you want to view.
Displays the list of agents for the selected agent team.

Modify Agent Team

Complete the following procedure to modify an agent's team:

Procedure

Step 1 Log in to Unified CCDM portal as supervisor.

Step 2 Click the burger icon and select **Provisioning** > **Agent Team Manager**.

Step 3 From the **My Agent Team** drop-down list, select the agent team to which agent belongs.

Step 4 Click the **Goto Agent** icon to modify the agent details.

Step 5 Select **Agent Team** tab.
Displays the current membership of agent with the agent team.

Step 6 Optional, check the agent team check box that you want to remove and click **Remove**.

Step 7 Optional, select the agent team from the list that you want to add and click **Add**.

Note You can add an agent as a member of that team, check the **Member** check box. Otherwise, you can also add an agent as primary or secondary supervisor, if they are supervisor agent.

Step 8 Click **Save**.

Configure User Variable

Complete the following procedure for user variable configuration:

- Create a User Variable, on page 247
- Edit a User Variable, on page 247
- Delete a User Variable, on page 247

Create a User Variable

Complete the following procedure to create a user variable.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 In folder tree panel, select the folder where you want to create the user variable.
Step 4 Click **Resource** and click **User Variable**
Step 5 Complete the required fields for user variable.
Step 6 Set Active from and to dates in **Advanced** tab.
Step 7 Click **Save**.

Edit a User Variable

Complete the following procedure to edit a user variable.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.
Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.
Step 3 Select the folder containing the user variables that you want to edit, and view the user variables in that folder using the **Items panel** list view.
Step 4 In the **Items panel**, select the user variables that you want to edit.
Step 5 After modification, Click **Save**.

Delete a User Variable

Complete the following procedure to delete a user variable.

Procedure

Step 1 Log in to Unified CCDM Portal as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**.

Step 3 Select the folder containing the user variables you want to delete, and view the user variables in that folder using the Items panel list view.

Step 4 In Items panel, check the check box or check boxes of the user variables you want to delete.

Step 5 Click **Delete**.

Step 6 In the Delete User Variables dialog box, click **Yes**.

The user variables are deleted.

View the Unified CCDM Version

Complete the following procedure to view the Unified CCDM version.

Procedure

Step 1 In the Settings page, click **Settings**.

Step 2 Click **About**.

View the Unified CCDM version installed on your system.

Bulk Operations Using Unified CCDM

The bulk upload tool is used for importing large numbers of resource items into Unified CCDM. It is used to generate resources such as Agents or Skill Groups by filling in resource attributes using the standard CSV format. All CSV files require headers that dictate where each value goes. These headers are provided by templates that can be downloaded from the appropriate Bulk Upload page in Unified CCDM. You can bulk upload the following resources:

- Agents
- Agent desktop
- Agent team
- Call Type
- Department
- Dialed Number
- Enterprise Skill Group
- Skill Group
- User Variable
- Folder
- Network VRU Script
- Label
- Person
- User
- Precision Attribute
- Precision Queue

Bulk Upload for Unified CCDM

Complete the following procedure to bulk upload Unified CCDM:

Procedure

Step 1 Log in to Unified CCDM portal as Tenant or Sub-Customer.

Step 2 Click the burger icon and select **Provisioing** > **Resource Manager**.

Step 3 Click the required folder.

Step 4 Click **Upload** in the Folder Tree panel and then select the item type you want to bulk upload from the drop-down list.

The Bulk Upload Control page appears.

Step 5 Select a template for your chosen resource. The template link is present in the horizontal toolbar near the top of the page. Once selected, a download box is presented allowing you to save this CSV file onto your machine.
.

Step 6 Open the template in the editor you require (such as Notepad) and begin to enter your data or paste it from another source.

For detailed information on Bulk Upload templates, please refer to User Guide for Cisco Unified Contact Center Domain Manager

Step 7 Return to the Bulk Upload Control page and make sure the path is set correctly.

Note This path is only used if you removed the Path column in the CSV file. This option is not available for folders, dashboard layouts or dashboard styles.

Step 8 Browse to the CSV file into which you just entered the data.

Step 9 Click **Upload**.

A progress bar at the bottom of the screen displays the upload progress.

Note *Do not upload more than 500 items per CSV file.*

Templates for Creating CSV Files

Data types

The following data types are used for creating CSV files:

- Standard Naming Convention (SNC). This is alphanumeric data with no exclamation marks or hyphens, although underscores are permitted.
- BOOLEAN values can be one of the following:
  - TRUE.
  - FALSE.
  - Empty field. Leaving these fields empty defaults the field to FALSE.
- Y/N is similar to BOOLEAN however it can only contain the values Y or N.

- Date format is the universal date format <Year>-<Month>-<Day> for example 2006-08-30.
- Any Data Type marked with a hyphen (-) implies that there are no constraints on what you can put in the field (except for the constraints imposed by the built-in CSV format).
- When a column supports a list of values (for example, an agent may belong to multiple skill groups) separate each skill group with a semi-colon, for example Skillgroup1; Skillgroup2; Skillgroup3.

Global Template Columns

These columns are common to every template file except where stated. The **Required?** column indicates whether the column can be removed entirely.

Column Name	Data Type	Required?	Description
Path	Path	No	Describes where in the tree the resource will be created. If you wish to supply the path in the bulk upload screen, you must remove this column. **Note** If you leave the column present and do not set a value, it attempts to upload into the Root directory, which is valid for items such as folders, but not for resources such as agent or skill group. If you remove the column completely, the resources upload into the folder you were working in when you initiated the bulk upload.
Name	SNC	Yes	The name of the resource in the Unified CCDM system. This must be a unique name. In most cases, this is not provisioned.
Description	—	Yes	Describes the dimension being created. This is never provisioned.
EnterpriseName	SNC	No	The name for the resource being created. This field is provisioned. If you leave it blank an Enterprise name is generated for you.
EffectiveFrom	Date	No	The date from which the resource is active. The default is the current date. **Note** This date is not localized, and is treated as a UTC date.
EffectiveTo	Date	No	The date on which the resource becomes inactive. The default is forever. **Note** This date is not localized, and is treated as a UTC date.

Department Template

Column Name	Data Type	Required?	Description
EnterpriseName	SNC	No	The name for the Department being created. This field is provisioned. If you leave it blank an Enterprise name is generated for you.
Name	SNC	Yes	The name of the Department in the Unified CCDM system. This must be a unique name. In most cases, this is not provisioned.
EffectiveFrom	Date	No	The date from which the resource is active. The default is the current date. Note This date is not localized, and is treated as a UTC date.
EffectiveTo	Date	No	The date on which the resource becomes inactive. The default is forever. Note. This date is not localized, and is treated as a UTC date.

Person Template

Column Name	Data Type	Required?	Description
EquipmentName	SNC	No	The instance name of the Unified CCE or Unified CM you want this person added to. This name corresponds directly with the equipment instance name that was specified when configured through the Unified CCDM Cluster Configuration utility.
FirstName	SNC	Yes	The first name of the person.
LastName	SNC	Yes	The last name of the person.
LoginName	SNC	Yes	The peripheral login name for the person.
PassPhrase	Password	Yes	The peripheral login password for the person.
DepartmentMember	Enterprise Name	No	The department that this person represents.

Agent Template

Column Name	Data Type	Required?	Description
PeripheralNumber	Numeric	No	The service number as known at the peripheral.
PeripheralName	SNC	No	The name identifying the agent on the associated peripheral.
Supervisor	Boolean	No	Indicates whether the agent is a supervisor. The Supervisor column name does not create a Unified CCDM system user but it allows you to bind this agent to a domain login name.
AgentStateTrace	Y/N	No	Indicates whether the software collects agent state trace data for the agent.
DomainLogin	NETBIOS Login Name	If Agent is a supervisor	The login name for the domain user this agent is associated with. The login name often uses the form <domain>\<username>
DomainUserName	NETBIOS Username	If Agent is a supervisor	The username of the domain user this agent is associated with.
PeripheralMember	Enterprise Name-PG name	Yes	The peripheral to assign this agent to.
AgentDesktopMember	Enterprise Name	No	The desktop this agent will use.
PersonMember	Enterprise Name	Yes	The person that this agent represents.

Column Name	Data Type	Required?	Description
AgentTeamMember	Enterprise Name	No	The team this agent belongs to. The team must be on the same peripheral otherwise provisioning will fail. This column may also be subject to capacity limitations. For example, there may only be so many agents allowed in a team and that team has already reached its capacity.
SkillGroupMember	Enterprise Name	No	The skill group or skill groups this agent belongs to. The skill groups must be on the same peripheral otherwise provisioning fails. To specify multiple skill groups, separate each skill group with a semi-colon (;) character.
DepartmentMember	Enterprise Name	No	The department that this agent represents.
PrecisionAttributeMember	Enterprise Name and Values	No	The attributes that agent has and the values of each. Assign values using '=' and separate each attributes with a semicolon(;). Example: Spanish=5, MortgageTraining=True
DefaultSkillGroup	Enterprise Name	No	

Agent Desktop Template

Column Name	Data Type	Required?	Description

WrapupDataIncomingMode	Numeric	No	Indicates whether the agent is allowed or required to enter wrap-up data after an inbound call. **0**: Required **1**: Optional **2**: Not allowed **3** : Required with Wrap up Data. If value is blank, it assigns default value to 1
WrapupDataOutgoingMode	Numeric	No	Indicates whether the agent is allowed or required to enter wrap-up data after an outbound call. **0**: Required **1**: Optional **2**: Not allowed **3** : Required with Wrap up Data. If value is blank, it assigns default value to 1
WorkModeTimer	Numeric	No	The amount of time in seconds (1-7200) allocated to an agent to wrap up the call. Default value will be 7200.
RemoteAgentType	Numeric	No	Indicates how mobile agents are handled. **0** : No remote access **1** : Use call by call routing **2** : Use nailed connection **3** : Agent chooses routing at login **4** : Required with Wrap up Data If value is blank, it assigns default value to 1
DepartmentMember	Alpha Numeric	No	The department that this agent desktop represents

Agent Team Template

Column Name	Data Type	Required?	Description
PeripheralMember	Enterprise Name- PG name	Yes	The peripheral to assign this agent team to.

DialedNumberMember	Enterprise Name	No	The dialed number to use for this agent team.
DepartmentMember	Enterprise Name	No	The department that this agent team represents.

Call Type Template

Column Name	Data Type	Required?	Description
ServiceLevelType	Numeric	No	Indicates how the system software calculates the service level for the skill group. If this field is 0, Unified CCE uses the default for the associated Peripheral/MRD pair. Valid numbers are as follows: 0 or blank: Use Default 1: Ignore Abandoned Calls 2: Abandoned Call Has Negative Impact 3:Abandoned Call Has Positive Impact.
ServiceLevelThreshold	Numeric	No	The service level threshold, in seconds, for the service level. If this field is negative, the value of the Service Level Threshold field in the Peripheral table is used.
DepartmentMember	Enterprise Name	No	The department that agent team represents.

Dialed Number Template

Column Name	Data Type	Required?	Description
Dialed Number	SNC	Yes	The string value by which the Agent/IVR Controller identifies the dialed number.
RoutingClient Member	SNC	Yes	The name of the routing client (such as NIC or PG) that this number should use to submit routing requests to the Unified CCE.

Column Name	Data Type	Required?	Description
MediaRouting DomainMember	SNC	Yes	The name of the media routing domain.
DepartmentMember	Enterprise Name	No	The department that agent team represents.

Skill Group Template

Column Name	Data Type	Required?	Description
PeripheralNumber	Numeric	No	The service number as known at the peripheral.
PeripheralName	SNC	No	The name of the peripheral as it is known on the site.
AvailableHoldoffDelay	Numeric	No	The value for this skill group instead of using the one associated with this peripheral.
Priority	Numeric	No	The routing priority for the skill. This should be set to 0.
Extension	Numeric	No	The extension number for the service.
IPTA	Y/N	No	Indicates whether the Unified CCE picks the agent.
ServiceLevelThreshold	Numeric	No	The service level threshold, in seconds, for the service level. If this field is negative, it uses the value of the Service Level Threshold field in the peripheral table.
ServiceLevelType	Numeric	No	Indicates how the system software calculates the service level for the skill group. If this field is 0, Unified CCE uses the default for the associated peripheral/MRD pair. Possible values are: 0 = Use Default 1 = Ignore Abandoned Calls 2 = Abandoned Call Has Negative Impact 3 = Abandoned Call Has Positive Impact
DefaultEntry	Numeric	No	Typical entries are 0 (zero). Any records with a value greater than 0 are considered a default skill group for configuration purposes. Unified CCE uses records with the value of 1 as the default target skill group.
PeripheralMember	Enterprise Name	Yes	The peripheral to assign this skill group to.
MediaRoutingDomainMember	Numeric	Yes	You cannot change this column name after skill group upload.

DepartmentMember	Enterprise Name	Yes	The department that this skill group represents.
RouteMember	SNC	No	The Routes associated with this skill group. To supply a list of routes, separate the routes in the list with a semi-colon (;). **Note** The specified route or routes must not already exist. They will be created as part of the bulk upload of the skill group.

Enterprise Skill Group Template

Column Name	Data Type	Required?	Description
DepartmentMember	Enterprise Name	No	The department that this item belongs to. This field is only valid if the tenant is associated with a Unified CCE instance running Unified CCE version 10.0 or later. Otherwise, an error will be reported if this field is present.
SkillGroupMember	Enterprise Name	No	The skill group or skill groups associated with this enterprise skill group. The skill groups must be on the same Peripheral otherwise provisioning will fail. To specify multiple skill groups, separate each skill group with a semi-colon (;) character.

User Variable Template

Column Name	Data Type	Required?	Description
ObjectType	Numeric	Yes	A number indicating the type of object with which to associate the variable. Select 31 (User Variable) if you choose to not associate the user variable with an object. The valid numbers are: **1:** Service **2:** Skill Group **7:** Call Type **8:** Enterprise Service **9:** Enterprise Skill Group **11:** Dialed Number **14:** Peripheral **16:** Trunk Group **17:** Route **20:** Master Script **21:** Script Table **29:** Application Gateway **31:** User Variable

Label Template

Column Name	Data Type	Required?	Description
RoutingClientMember	SNC	Yes	The name of the routing client (NIC or PG), this number is used to submit the routing request to Unified CCE.
LableType	Numeric	False	The type of label: • 0: Normal • 1: DNIS Overide • 2: Busy • 3: Ring • 4: Post-Query • 5: Resource

Column Name	Data Type	Required?	Description
Label	SNC	False	The string value used to identify the label by the routing client.

Network VRU Script Template

Column Name	Data Type	Required?	Description
NetworkVruMember	SNC	Yes	The network VRU to associate with this Network VRU Script.
VruScriptName	SNC	Yes	Represent the VRU Script Name
DepartmentMember	Enterprise	No	The department that is Network VRU represent .
Timeout	Numeric	Yes	The number of seconds to wait for a response after the script starts executing.

Folder Template

Note Folders do not use the Enterprise Name, Effective To or Effective From global columns.

Column Name	Data Type	Required?	Description
Security	CSS Styled List	No	Allows you to set security on the folder you upload. See section *Security Field Example* for an example of the syntax for this field.

User Template

Note Users use only the 'Path' and 'Description' global columns from the Global Template

Column Name	Data Type	Required?	Description
LoginName	SNC	Yes	Login name of the user that will be used for application logon
Password	Password	Yes	Password for the new user account
AdvancedMode	Boolean	No	Determines if the user is advanced or not
FirstName	SNC	No	The first name of the user

Column Name	Data Type	Required?	Description
LastName	SNC	No	The last name of the user
ChangePasswordOn NextLogon	Boolean	No	Determines if after the initial logon the user should be prompted to reset their password
PasswordNeverExpires	Boolean	No	Determines if the password for this user will ever expire
HomeFolder	Path	No	The folder path to the folder which will be used as the users home folder
CreateNewUserFolder	Boolean	No	Determines whether a new folder should be created for the user home folder in the HomeFolder location
Groups	Group Name(s)	No	A semi colon separated list of Group names (including their path) to which the user will be added. Since group names are not unique the path must also be specified for example, /Folder1/Admins;/Folder2/Admins
InternetScriptEditorEnabled	Boolean	No	Whether the user is linked to a Unified CCE user that can access Cisco's Internet Script Editor. If true, the following apply: • The login name must correspond to an existing Windows active directory use • If the installation does not use single sign on, the specified password must match the password for the corresponding active directory user

Precision Attribute Template

The following table includes the columns that are required for loading bulk precision attributes.

Column Name	Data Type	Required?	Description
AttributeDataType	Numeric	Yes	Type of data to associate with one of the following attributes: 3: Boolean (true or false only) 4: Proficiency (a numeric range)
DefaultValue	Boolean or Numeric, according to Attribute Data Type	Yes	Default value to be used when an attribute is assigned to an agent if no explicit value is specified.

Column Name	Data Type	Required?	Description
DepartmentMember	Enterprise Name	No	The department that this attribute represents.

Precision Queue Template

The following table includes the columns that are required for loading bulk precision queues.

Column Name	Data Type	Required?	Description
Steps	—	Yes	Specification of the steps in this precision queue. See Syntax for Precision Queue Steps, on page 262
AgentOrdering	Numeric	Yes	If more than one agent satisfies the precision queue criteria agents are chosen in the following order to handle the call: 1: Agent that has been available the longest. 2: Most skilled agent. 3: Least skilled agent.
ServiceLevelThreshold	Numeric	No	The service level threshold in seconds for allocating the call to a suitable agent using the rules in the precision queue from 0 to 2147483647.
ServiceLevelType	Numeric	No	Abandoned calls in service level calculations, calls are handled in the following order: 1: Ignore abandoned calls. 2: Abandoned calls have negative impact (that is, exceed the service level threshold). 3: Abandoned calls have positive impact (that is, meet the service level threshold).

Column Name	Data Type	Required?	Description
DepartmentMember	Enterprise Name	No	The department that this precision queue represents.

Syntax for Precision Queue Steps

The Precision Queue Steps field consists of one or more steps. Each step is divided into the following parts:

- **Consider If** condition (optional, but not valid if there is only one step, and not valid for the last step if there is more than one step). If it is present, this condition specifies the circumstances to which the step applies. For example, a step might apply only if there has been a higher than usual number of unanswered calls for the day.
- **Condition Expressions** (always required for each step). This condition specifies the attributes that an agent must have to receive the call. It may be a simple comparison, or it may involve multiple comparisons linked by *and* or *or*. For example, the condition expressions might specify an agent who can speak Spanish and is trained to sell mortgages and is based in London.
- **Wait Time** (always required, except for the last step) this condition specifies the amount of time in seconds to wait before moving on to the next step if the conditions in this step cannot be satisfied. For example, a wait time value of 20 means that if no agent that matches the conditions for that step is available at the end of 20 seconds, the next step is considered.

Note To build the Steps field from these components, separate each step with a semicolon (;) and separate the parts of each step with a colon (:) as example shown below:

Example: ENGLISH1==5:WaitTime=22;ENGLISH1==5:WaitTime=20;ENGLISH==5

"English1" and "English" indicates the Enterprise Name of Precision Attribute.

The following example shows a Steps field with three steps. The first step has a **Wait Time** expression and the condition expression. The second has a **Consider If** expression and a **Wait Time** expression as well as the condition expression. The third step is the last step, so it has only a condition expression.

First Step:

Specify the time in seconds to wait for the conditions in the step to be satisfied. This syntax is a part of the step, so it ends with a colon.

```
WaitTime=10:
```

Specify the condition expression to be used. This syntax is the end of the step, so it ends with a semicolon.

```
Spanish >= 5 && MortgageTrained == True && Location == London;
```

Second Step:

Specify the circumstances to consider this step. This syntax is part of the step, so it ends with a colon. See the note below for the syntax for the Consider If statement.

```
ConsiderIf=TestforSituation:
```

Specify the time in seconds to wait for the conditions in the step to be satisfied. This syntax is a part of the step, so ends with a colon.

```
WaitTime=20:
```

Specify the condition expression to be used. This syntax is the end of the step, so it ends with a semicolon.

```
Spanish >= 5 && MortgageTrained == True;
```

Third Step:

Specify the condition expression to be used if all previous steps fail.

```
(Spanish >= 5) || (Spanish >=3 && MortgageTrained == True),
```

Manage Roles

Roles are collections of tasks that can be grouped together and applied to users or groups. Like tasks, roles can be folder-based, containing a collection of folder-based tasks, or global, containing a collection of global tasks. Folder roles always apply to folders. A user that has a particular folder role can perform all the tasks in that role on the items in that folder. A user with a global role can perform all the tasks for that global role.

Default Roles

Following default roles are provided in the system:

- **Default global roles**
  - **Global Basic** - Allows a user to perform basic provisioning and management functions.
  - **Global Advanced** - Allows a user to perform advanced provisioning and management functions, including all those allowed by the global basic role.
  - **Global Host** - Allows a user to perform all licensed functions.
- **Default folder roles**
  - **Supervisor** - Allows a user to manage users and most resources in the specified folder.
  - **Basic** - Allows a user to browse most resources and to manage reports and parameter sets in the specified folder.
  - **Advanced** - Allows a user to browse and access most resources in the specified folder, including all those allowed by the basic folder role and the supervisor folder role.
  - **Full Permissions** - Allows a user to perform all licensed functions in the specified folder.

Create a Global Role

Complete the following procedure to create a global role.

Procedure

Step 1 Log in to CCDM portal as administrator.

Step 2 Click the burger icon and select **Security** > **Roles** > **Global Roles**.

Step 3 Click **New**.

Step 4 In **Name** field, enter new role name that reflects the permissions or category of the user it is intended.

Step 5 Optional, in **Description** field, enter description. It can be summary of the permissions granted.

Step 6 Select the tasks you want to enable the role.

Step 7 Click **Save**.

Assign a Global Role

Complete the following procedure to assign users with global roles.

Procedure

Step 1 Login as administrator and configure the following, to grant or remove global permissions:

a) In **Global Roles** window, select the global role that you want to assign to users or groups.

b) Click **Members**.

c) Click **Add Members**.

d) In folder tree panel, select the folder that has users or groups you want to assign.

Note You can use the fields at the top to filter the view such as only users, only groups, or to search for specific names.

e) Check the check box for the newly added members.

Note You can select users and groups from multiple folders.

f) Click **OK**.

g) Click **Save**.

Step 2 Click delete icon and click **Confirm**, to remove a user or group from this global role.

Edit a Global Role

Complete the following procedure to edit a global role.

Procedure

Step 1 Login as administrator and select **Security** > **Roles** > **Global Roles**.

Step 2 Select the global role that you want to edit.

Step 3 Select **Details** tab and change the details if required.

Step 4 Check **Enabled** check box to ensure that global role is available to users.

Step 5 Check **Hidden** check box if you want to hide global roles from system users.

Step 6 Select **Tasks** tab and check the tasks that you want to add and uncheck the tasks that you want to remove from the global role.

Step 7 Click **Save**.

Delete a Global Role

Complete the following procedure to delete a global role.

Procedure

Step 1 Login as System Administrator and click **Global Roles** in Security.

Step 2 In **Global Roles** window, check the required global role check box you want to delete and click **Delete**.

Step 3 Click **OK** to confirm the deletion.

Create a Folder Role

Complete the following procedure to create a folder role.

Procedure

Step 1 Login the CCDM Portal as System Administrator.

Step 2 Click the burger icon and select **Security** > **Roles**.

Step 3 In **Roles** window, click **New**.

Step 4 In **Name** field, enter new role name that reflects the permissions or category of the user it is intended.

Step 5 Optional, in **Description** field, enter description. It can be summary of the permissions granted.

Step 6 Select the tasks you want to enable the role.

Step 7 Click **Save**.

Assign a Folder Role

Complete the following procedure to assign a folder role.

Procedure

Step 1 Login the CCDM Portal as Administrator and click **Security** > **Permissions**.

Step 2 In Security Manager, click the location in the folder tree that contains the users or groups you want to assign folder roles to. Then, do one of the following:

- Click the **Users** tab to see the users in that folder. (or)
- Click the **Groups** tab to see the users in that folder.

Step 3 Check the check boxes beside the users or groups that you want to edit the permissions for.

Step 4 Click **Change Permissions** to change the folder roles for the selected users or groups.

Step 5 If you see a message that states that the current folder is inheriting permissions, and you want to stop this process and set different permissions for this folder, click **Edit Item Security**, and then click **OK** to confirm the action. Click **Cancel** if you do not want to set different permissions for the folder.

Step 6 If you are continuing to set folder roles, in the Folder Permissions dialog box, select a folder location from the folder tree on the left side of the screen, and one or more folder roles from the right side of the screen.

Step 7 Check the **Change Permissions for Subfolders** check box if you want to copy the changed permissions to the subfolders of the selected folder also.

Step 8 Click **Save** to see a summary of the folder roles that you changed.

Step 9 Click **Confirm** to apply the new folder roles.

Edit a Folder Role

Complete the following procedure to edit a folder role.

Procedure

Step 1 Login the CCDM Portal as Administrator and click **Roles** under **Security**.

Step 2 In Role Manager, click the name of the folder role you want to edit.

Step 3 Check the tasks you want to add to the folder role, and uncheck the tasks you want to remove from the folder role.

Step 4 Click **Save** to save your changes.

Delete a Folder Role

Complete the following procedure to delete a folder role:

Procedure

Step 1 To delete a folder role, in Role Manager, check the check box beside the folder role you want to delete.

Step 2 Click **Delete**, and then click **OK**.

You cannot delete a folder role that is still being used.

Global Role Tasks

Global roles such as Basic, Advanced, Host and System Administrator are applied to users or groups of users, enabling them to access the same set of functions on all the folders to which they have access. The following table displays a list of all available tasks configurable for a global role, accessed through Security > Global.

Global Task Name	Comments	Basic	Advanced
Security Manager	Displays Security Manager and Security Manager options on the user's tools page.		x
Service Manager	Displays Service Manager on the tools page.		x
System Manager	Displays System Manager on the tools page.		x

Global Task Name	Comments	Basic	Advanced
Advanced User	Displays a check box on the user settings page, enabling access to Advanced User mode, which displays the tools page on startup.		x
Manage site	Allows the user to save system settings, security settings, reporting settings, and provisioning settings on the Settings page.		
Self skill	Allows the user to save system settings, security settings, reporting settings, and provisioning settings on the Settings page.		
Browse Roles	Allows the user to view folder-based roles within Role Manager and Security Manager.		x
Manage Roles	Allows the user to create, modify, and delete folder-based roles within Security Manager > Role Manager.		
Browse Global Roles	Allows the user to view global roles in Global Security Manager.		x
Manage Global Roles	Allows the user to add, modify, and delete global roles using Global Security Manager.		
Browse Global Security	Enables Global Security Manager within the Security Manager tool on the home page. Access is view-only. Roles are unable to be edited.		x
Manage Global Security	Displays the Global Security Manager option within Security Manager tool on the tools page enabling the user to view and edit global security roles.		
Browse Dimension type	Allows the user to select dimension types (such as Agent or Call Type) from an Item Type drop-down when creating a Parameter Set in Reports.	x	x
Bulk Import Dimensions	Allows the user to select dimension types (such as Agent or Call Type) from an Item Type drop-down when creating a Parameter Set in Reports.		x
Provision Agent	Allows the user to create and manage an Agent using System Manager, or Agent Team Manager, provided the user also has granted permission to Manage Dimensions on the specified folder, and Browse Connected Systems is enabled.	x	x

Global Task Name	Comments	Basic	Advanced
Provision Agent Desktop	Allows the user to add an Agent Desktop, through the New > Resource Items menu within System Manager, provided the user also has granted permission to Manage Dimensions on the specified folder, and Browse Connected Systems is enabled.		x
Provision Agent Team	Allows the user to add an Agent Team item to a folder, through the New > Resource Items menu within System Manager.	x	x
Provision Call Type	Allows the user to add a new Call Type to a folder using the System Manager, New > Resource Items menu.		x
Provision Dialed Number	Allows the user to provision new dialed Numbers.		x
Provision Directory Number	Allows the user to provision new directory numbers.		x
Provision Enterprise Skill Group	Allows the user to provision new Enterprise skill groups.		x
Provision Expanded Call Variable	Allows the user to create an Expanded Call Variable and manage its settings and active dates through System Manager > New Resource.		x
Provision Label	Allows the user to create labels through System Manager > Resource Folder > Resource Item.		x
Provision Person	Allows the user to provision a person using System Manager or Service Manager, provided the user also has granted permission to Manage Dimensions on the specified folder, and Browse Connected Systems is enabled.		x
Provision Service	Allows the user to provision and manage a service, including setting Service Level Type, associated Skill Groups, and peripherals, using System Manager.		x
Provision Skill Group	Allows the user to manage skill groups using System Manager, Skill Group Manager (within Service Manager) provided the user also has given permission to Manage Dimensions on the folder where the skill group is located.		x
Provision User Variable	Allows the user to provision a user-defined variable using System Manager.		x

Folder-Based Roles

You can apply roles to a specific folder, so that users that are assigned the folder-based role have access to the task-based permissions specified only for that folder. The following table lists the tasks available to create a folder-based role, using Security Manager > Role Manager. The Basic, Supervisor, and Advanced columns indicate whether the task is enabled by default for these preconfigured roles in Unified CCDM.

Name	Comments	Basic	Supervisor	Advanced
Folder Settings				
Browse Folders	Allows the user to see a folder in the folder tree.	x		x
Manage Folders	Allows the user to edit, create, and remove folders in the specified folder.			x
Users and Security				
Browse Users	Allows the user to view the details of all users in the specified folder.	x		x
Manage Users	Allows the user to modify settings of users within the specified folder.		x	x
Reset passwords	Allows the user to reset the password of other users within the specified folder.			x
Manage Tenants	Allows the user to manage the tenant items within the specified folder.			
Manage Security	Allows the user to modify security permissions on the selected folder. Access to the Security Manager tool is required.			x
Dimensions and Prefixes				
Browse Dimensions	Allows the user to list system resources in the specified folder.	x		x
Manage Dimension	Allows the user to edit, move, and delete dimensions such as agents, agent teams, or skill groups in the specified folder using System Manager.		x	x
Manage Dimension Memberships	Allows the user to add, modify, and delete dimension memberships.			
Clone Dimensions	Allows user to copy agents.		x	
Browse Prefixes	Allows the user to browse automatic resource movement prefixes in the specified folder on the prefix details tab of a tenant item in the System Manager.			x

Manage Prefixes	Allows the user to add and remove automatic resource movement prefixes in the specified folder on the prefix details tab of a tenant item in the System Manager.			

Configure Gadgets

You can perform the following operations to configure gadgets:

- Create Gadget, on page 270
- Edit Gadget, on page 270
- Delete Gadget, on page 271

Create Gadget

Procedure

Step 1 Login to the CCDM portal as tenant or sub-customer user.

Step 2 Click **Gadget**.

Step 3 Select **Add Gadget** from the drop-down list.

Step 4 Click **Resource Manager**.

Step 5 Click the burger icon and select a tenant.

Step 6 Select a resource from the search bar list.

The list includes Agent, Agent Desktop, Agent Team, Call Type, Department, Dialed number, Enterprise Skill Group, Expanded Call Variable, Label, Network Vru Script, Person, Precision Attribute, Precision Queue, Service, Service, Skill Group, and User Variable.

Step 7 Click **Gadget** > **Save App**, enter a name for the gadget and browse a folder to save the gadget.

Edit Gadget

Procedure

Step 1 Login to the CCDM portal as tenant or sub-customer user.

Step 2 Click **Gadget** and select **Open App**, choose the app that you have created.

Step 3 Select the gadget you want to modify.

Step 4 Select the required tenant and required resource to modify the gadget.

Step 5 Click **App Name** > **Save App**, click **Yes** to save the modified fields.

Delete Gadget

Procedure

Step 1 Login to the CCDM portal as tenant or sub-customer user.

Step 2 Click **Gadget** > **Open App** and select an app.

Step 3 Select the gadget that you want delete from the app and click **Delete**.

Step 4 Click **Save** to save the app.

Note To delete an app, click **Gadget** > **Delete App** and click **OK**.

Provision Unified CCE Using Administration Workstation

Complete the following procedures to provision Unified CCE using Administration Workstation.

Note
- The base configuration that you upload using the ICMdba tool will automatically provision other required elements of Unified CCE.
- Administration Workstations can support remote desktop access. But, only one user can access workstation at a time. Unified CCE does not support simultaneous access by several users on the same workstation.

Set up Agent Targeting Rules

Complete the following procedure to configure individual agent targeting rules.

Procedure

Step 1 In the Configuration Manager, navigate to Configure **ICM** > **Targets** > **Device target** > **Agent Targeting Rule** or navigate to **Tools** > **List Tools** > **Agent Targeting Rule**.

Step 2 In the ICM Agent Targeting Rules dialog box, click **Retrieve**.

Step 3 Click **Add**.

Step 4 Enter a name for the rule.

Step 5 Choose a peripheral where the rule will be associated.

Step 6 Choose **Agent Extension** from the Rule Type drop-down list.

Step 7 Choose one or more routing clients that can initiate the route request.

Step 8 Enter the agent extension range.

Step 9 Click **Save**.

Provision Unified CCE Using Web Administration

Set Up Reason Code

Complete the following procedure to set up the reason code.

Procedure

Step 1 Login to the **CCE Web Administration** page, click **Manage** and select **Reason Codes**.

Step 2 Click **New** on the List of Reason Codes page to open the New Reason Code page.

Step 3 Complete fields as follows:

a) In **Text** field, enter the relevant text for the reason code.
b) In **Code** field, enter a unique positive number.
c) Optional, in **Description** field, enter the description for the reason code.

Step 4 Save the reason code to return to the List page, where a message confirms the successful creation.

Provision Routing Script Using Internet Script Editor

Complete the following procedure to log in to ISE:

Procedure

Step 1 Launch Internet Script Editor `iscriptEditor.exe`.

Step 2 Enter your Username, Password and Domain.

Example:

If ISE user is in format iseuser1@domain.com then username will be iseuser1 and domain will be domain.com

Step 3 Click **Connection**.

Step 4 Enter the AW Server Address, Port, and ICM Instance Name.

Step 5 Click **OK**.

Step 6 Click **OK**.

Upgrade Internet Script Editor, if necessary.

Note After login, you will see only the script items that the linked Unified CCDM user has access to view.

Business Hours

Business hours are the working hours during which you conduct business. You can create and modify business hours and set weekly and daily schedules for each business hour. You can create different business hour schedules for regular working days and holidays. You can also open or close the business hours if there is an emergency.

You can define the status reasons for business hours and assign codes for each status reason. Status reason is required when you force open or force close a business hour, and when you add special hours and holidays.

Add and Maintain Business Hours

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization** > **Business Hours**.

Step 2 On the **Business Hours** page, click **New** to open the **New Business Hours** page.

Step 3 Complete the following information on the **General** tab and click **Save**.

Field	Required?	Description
Status	-	Select one of the following statuses for the business hour: • **Open/Closed as per Business Calendar** • **Force Open** • **Force Close**
Status Reason	Yes, if the status is Force Open or Force Close.	This field is enabled only if the status is Force Open or Force Close. Search and select a status reason for the business hour.
Name	Yes	Enter a unique name for the business hour. Maximum length is 32 characters. Valid characters are alphanumeric, period (.), and underscore (_). The first character must be alphanumeric.
Description	No	Enter a description of the business hour.
Time Zone	Yes	Select a time zone of the business hour from the drop-down list.
Department	-	Search and select a department to associate with the business hour. Default is Global. **Note** This is applicable for Packaged CCE deployment only.

Step 4 Click the **Regular Hours** tab and complete the following information:

• Select one of the following **Business Hour Type**:

- **24x7**: Always open. You cannot customize the working hours.
- **Custom**: You can customize the working hours.

- If you select **Custom**, enable at least one business day and select the **Start Time** and **End Time**.

Step 5 Click the **Special Hours & Holiday** tab. You can either add or import special hours and holidays.

Step 6 Click **Add** to open the **Add Special Hours & Holiday** popup window. Complete the following information:

Field	Required?	Description
Date	Yes	Select a date from the calendar.
Description	No	Enter a description for the special hour.
Status	-	Select a status. If the status is **Open**, the **Start Time** and **End Time** fields are enabled.
Start Time	Yes, if status is Open.	Select a start time for the special hour.
End Time	Yes, if status is Open.	Select an end time for the special hour.
Duration	-	Displays the duration of the special hour.
Status Reason	Yes	Search and select a status reason.

Step 7 Click **Save** to add the special hours and holidays.

Step 8 To import special hours and holidays, follow these steps.

a) Click **Import** to open the **Import Special Hours and Holidays** pop-up window.

b) Click the download icon to download the Special Hours & Holidays template. Use this template to enter the special hours and holidays.

c) Click **Choose File** and browse to the special hours and holidays file. Click**Import** to upload the file.

Note The file must contain at least one special hour and holiday.

The file must be in CSV format with a file extension as .txt or .csv.

Step 9 Click **Export** to download the special hours and holidays in .csv format.

Step 10 Click **Save**.

Note The imported business hours overwrites the existing ones.

Add Business Hours by Copying an Existing Business Hour Record

You can create a new Business Hour record by copying an existing Business Hour record.

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization** > **Business Hours**.

Step 2 Click the Business Hour you want to copy, and then click the **Copy** button in the Edit <Business Hour> page. The **New Business Hour** page opens.

Step 3 Enter **Name** and **Description** for the Business Hour.

Step 4 Review the rest of the fields on the **General**, **Regular Hours**, and **Special Hours & Holiday** tabs that were copied from the original Business Hour record, and make any necessary changes.

Step 5 Click **Save** to return to the List window.

Add Status Reasons

This procedure explains how to add and maintain status reasons for business hours.

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization** > **Business Hours** > **Status Reasons**.

Step 2 Click **Add** to open the **Add Status Reason** popup window.

Step 3 Enter the Status Reason. Maximum length is 255 characters.

Step 4 Enter a unique Reason Code. Range is 1001 to 65535. Codes 1 to 1000 are reserved as system-defined reason codes.

Step 5 Click **Save**.

To add more status reasons, repeat steps from 2 to 5.

Step 6 Click **Done** to return to the List window.

Edit Status for Multiple Business Hours

Perform the following steps to edit the status of multiple business hours at once.

Procedure

Step 1 On the **Business Hours** page, select two or more business hours to edit.

Step 2 Choose **Edit** > **Status** to open the **Edit Business Hours** page.

Step 3 Check the **Status** check box and select the required status.

Step 4 If you select the status as **Force Open** or **Force Close**, search and select a **Status Reason**.

Step 5 Click **Save**.

Edit Schedule for Multiple Business Hours

Perform the following steps to edit schedules of multiple business hours at once.

Procedure

Step 1 On the **Business Hours** page, select two or more business hours to edit.
Step 2 Choose **Edit** > **Schedule** to open the **Edit Business Hours** page.
Step 3 Check the **Time Zone** check box and the select the required time zone from the drop-down list.
Step 4 Check the **Type** check box and select the required business hour type.
Step 5 If you select **Custom**, enable atleast one business day and select the **Start Time** and **End Time**.
Step 6 Click **Save**.

Configure Yearly Schedules

You can configure and maintain Business Hour schedules for the whole year.

Procedure

Step 1 Configure the regular working hours for weekdays.
Step 2 Configure **Special Hours & Holidays** schedules for whole year by doing the following:

a) Add the **Special Hours & Holidays** details for all the special hours and holidays for the whole year into the CSV template file.
b) On the **Import Special Hours & Holidays** page, click **Choose File** and browse to the special hours and holidays file.
c) Click**Import** to upload the file.

After you import the configuration file, the BH configurations are loaded on the Business Hours page. Validate the configurations.

d) Click **Save**.

Note When you update the configured Business Hours, remove any elapsed schedules and then update the new schedules for any new special hours or holidays in a Business Hour configuration.

Unified CVP Administration

• Provisioning Unified CVP Using Unified CCDM, on page 277

Provisioning Unified CVP Using Unified CCDM

Uploading the Media File

Procedure

Step 1 Log into CCDM Portal.
Step 2 In **Resource Manager**, navigate to the CVP assigned default import tenant.
Step 3 Click **Resource** and select **Mediafile**.
Step 4 Select the media server on which the file has to be uploaded.
Step 5 Click **Add file(s)** to add media files.
Step 6 Click **Save**.

Uploading the IVR Script

Procedure

Step 1 Log into the CCDM Portal
Step 2 In **Resource Manager**, select the CVP assigned default import tenant.
Step 3 Click **Resource** and select **IVR app**.
Step 4 Select the VXML servers on which the IVR script has to be uploaded.
Step 5 Click **Add file(s)** to add IVR files (.zip files).
Step 6 Click **Save**.

Unified Communication Manager Administration

Provision Unified Communications Manager Using UCDM

- Configure Route Patterns, on page 287
- Configure Directory Number Inventory and Lines, on page 290
- Configure Phones, on page 291
- Configure Regions, on page 293
- Configure Class of Service, on page 294
- Configure Cisco Unified CM Group, on page 288
- Configure Device Pool, on page 289
- Associate Phone to Application User, on page 296
- Disassociate Unified Communication Manager from UCDM, on page 296
- Built-in-Bridge, on page 297
- Bulk Operations Using UCDM, on page 298
- Increase the SW MTP and SW Conference Resources, on page 299

CRUD Operations for UCDM Objects

Following table provides an information of create, update or delete operations for UCDM objects.

Note Bulk upload is supported only for create operations. See, CRUD Operations for UCDM Objects, on page 278

Object	Create	Read	Update	Delete	Bulk Upload
Contact Center Servers See, Configure Contact Center Servers, on page 280	x	x	x	x	x
Contact Center Services See, Configure Contact Center Services, on page 281	x	x	x	x	x
SIP Trunks See, Configure SIP Trunks, on page 282	x	x	x	x	x

Object	Create	Read	Update	Delete	Bulk Upload
Route Group See, Configure Route Groups, on page 284	x	x	x	x	x
Route List See, Configure Route List, on page 285	x	x	x	x	x
Route Patterns See, Configure Route Patterns, on page 287	x	x	x	x	x
Directory Number and Lines See, Configure Directory Number Inventory and Lines, on page 290	x	x	x	x	x
Phones See, Configure Phones, on page 291	x	x	x	x	x
Regions See, Configure Regions, on page 293	x	x	x	x	x
Class of Service See, Configure Class of Service, on page 294	x	x	x	x	x
Device Pools See, Configure Device Pool, on page 289	x	x	x	x	x

Provisioning Contact Center Server and Contact Center Services

This section describes the procedure to configure contact center servers and services. Configuring server enables CUCM to communicate with Contact Center during call transfer from agent to agent and routing a

call back to the customer voice portal (CVP). Configuring services enables internal service calls to be routed to CUBE for contact center process.

Configure Contact Center Servers

A Contact Center Server can be configured only for the customer assigned to a specific Cisco Unified Communications Manager.

- Add Contact Center Servers, on page 280
- Edit Contact Center Servers, on page 280
- Delete Contact Center Servers, on page 281

Add Contact Center Servers

Procedure

Step 1 Login to the UCDM server using provider or reseller admin credentials.

Step 2 Set the hierarchy according to the customer level.

Step 3 Select **Services** > **Contact Center** > **Servers**.

Step 4 Click **Add**.

Step 5 Enter the contact center server name.

Step 6 Select the appropriate CUCM from the **CUCM** drop-down list.

Step 7 Enter the transfer conference pattern number.
This creates a CTI Route Point and associates with the default application user (pguser).

Step 8 Enter the network VRU pattern.
This creates route pattern associated with CVP trunk and CUBE trunk.

Step 9 Expand SIP trunk section and configure the CVP trunk.

a) Select **CVP** trunk from **Trunk Destination Type** drop-down list.
b) Expand **Destination Addresses** and enter the trunk destination address and trunk destination port.
c) Select the appropriate trunk security profile from the drop-down list.

Step 10 Expand SIP trunk section and configure the CUBEE trunk.

a) Select **CUBEE** trunk from **Trunk Destination Type** drop-down list.
b) Expand **Destination Addresses** and enter the trunk destination address and trunk destination port.
c) Select the appropriate trunk security profile from the drop-down list.

Step 11 Click **Save**.

Edit Contact Center Servers

Procedure

Step 1 Login to the UCDM server using provider or reseller admin credentials.

Step 2 Set the hierarchy according to the customer level.

Step 3 Select **Services** > **Contact Center** > **Servers**.

Step 4 Click the contact center server that you want to edit and modify the required fields.

Note You cannot change contact center server name.

Step 5 Click **Save**.

Delete Contact Center Servers

Before you begin

Delete the contact center service and parameters associated with contact center server.

Procedure

Step 1 Login to the UCDM server using provider or reseller admin credentials.

Step 2 Set the hierarchy according to the customer level.

Step 3 Select **Services** > **Contact Center** > **Servers**.

Step 4 Click the contact server that you want delete.

Step 5 Click **Save**.

Configure Contact Center Services

- Add Contact Center Services, on page 281
- Edit Contact Center Services, on page 282
- Delete Contact Center Services, on page 282

Add Contact Center Services

Procedure

Step 1 Login to the UCDM server using provider or reseller admin credentials.

Step 2 Set the hierarchy to the customer or site level.

Step 3 Select **Services** > **Contact Center** > **Service**.

Step 4 Click **Add**.

Step 5 Enter the contact center service name

Step 6 Select the associated contact center server name from the drop-down list.

Step 7 Expand **Internal Service Numbers** section , enter the service number pattern (pattern that is used to route internal service calls to the CUBE) .

Step 8 Click **Save**.

Note Adding Contact center server and services in UCDM creates application user , Trunk , CTI route point , Route group , Route Pattern as default configuration.

For additional CTI Route Points, see Set Up CTI Route Point , on page 429

Edit Contact Center Services

Procedure

Step 1 Log in to the Unified CDM server using provider or reseller admin credentials.

Step 2 Set the hierarchy according to the customer level.

Step 3 Select **Services** > **Contact Center** > **Services**.

Step 4 Click the contact center service that you want to edit and modify the required fields.

Note You cannot change contact center service name.

Step 5 Click **Save**.

Delete Contact Center Services

Procedure

Step 1 Log in to the Unified CDM server using provider or reseller admin credentials.

Step 2 Set the hierarchy according to the customer level.

Step 3 Select **Services** > **Contact Center** > **Services**.

Step 4 Click the contact center service that you want to delete.

Step 5 Click **Delete**.

Configure SIP Trunks

Add SIP Trunks

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **SIP Trunks**:

- For provider or reseller administrator **Device Management** > **CUCM** > **SIP Trunks**
- For customer administrator **Device Management** > **Advanced** > **SIP Trunks**

Step 4 Click **Add** to create SIP trunk.

Step 5 Perform the following, In **Device Information** tab:

a) Choose required IP address from **CUCM** drop-down list that you want to add SIP trunk.
b) Enter a unique SIP trunk name in **Device Name** field.
c) Choose **Device Pool** from the drop-down list.
d) Check **Run On All Active Unified CM Nodes** check-box, if required.

Step 6 Goto **SIP Info** tab and perform the following:

a) Click **Add** icon in **Destination** panel.
b) Enter destination IP address in **Address IPv4** field.

Note To create the SIP trunk from CUCM to CVP, CUBE or any other destinations, enter IP addresses of respective devices.

c) Change **Port**, if required.
d) Enter **Sort Order** to prioritize multiple destinations.

Note Lower sort order indicates higher priority.

e) Choose an appropriate option from **SIP Trunk Security Profile** drop-down list.
f) Choose **sip profile** from the drop-down list.

Repeat this step to add another trunk.

Step 7 Click **Save**.

Edit SIP Trunks

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **SIP Trunks**:

- For provider or reseller administrator **Device Management** > **CUCM** > **SIP Trunks**
- For customer administrator **Device Management** > **Advanced** > **SIP Trunks**

Step 4 Click the SIP trunk that you want to edit and modify the required fields.

Step 5 Click **Save**.

Delete SIP Trunks

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **SIP Trunks**:

- For provider or reseller administrator **Device Management** > **CUCM** > **SIP Trunks**
- For customer administrator **Device Management** > **Advanced** > **SIP Trunks**

Step 4 Click the SIP trunk that you want to delete.

Step 5 Click **Delete**.

Configure Route Groups

Before you begin

Ensure SIP Trunks are configured. See, Configure SIP Trunks, on page 282.

Perform the following instruction to configure route groups.

- Add Route Group, on page 284
- Edit Route Group, on page 285
- Delete Route Group, on page 285

Add Route Group

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **Route Groups**:

- For provider or reseller administrator **Device Management** > **CUCM** > **Route Groups**
- For customer administrator **Device Management** > **Advanced** > **Route Groups**

Step 4 Click **Add** to create route group.

Step 5 Choose required IP address from **CUCM** drop-down list to add route group.

Step 6 Enter a unique name in **Route Group Name** field.

Step 7 Click **Add** icon in **Members** panel.

Step 8 Choose an appropriate SIP trunk from **Device Name** drop-down list.

Note When a SIP trunk is selected, it will select all the ports on the device.

Step 9 Click **Save**.

Edit Route Group

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.
Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.
Step 3 Navigate to **Route Groups**:

- For provider or reseller administrator **Device Management** > **CUCM** > **Route Groups**
- For customer administrator **Device Management** > **Advanced** > **Route Groups**

Step 4 Click the route group from the list that you want to edit and modify required fields.
Step 5 Click **Save**.

Delete Route Group

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.
Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.
Step 3 Navigate to **Route Groups**:

- For provider or reseller administrator **Device Management** > **CUCM** > **Route Groups**
- For customer administrator **Device Management** > **Advanced** > **Route Groups**

Step 4 Click the route group from the list that you want to delete.
Step 5 Click **Delete**.

Configure Route List

Before you begin

Ensure Route Groups are configured. See, Configure Route Groups, on page 284.

Perform the following instructions to configure route list:

- Add Route List, on page 286
- Edit Route List, on page 286
- Delete Route List, on page 286

Add Route List

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.
Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.
Step 3 Navigate to **Route List**:

- For provider or reseller administrator **Device Management** > **CUCM** > **Route List**
- For customer administrator **Device Management** > **Advanced** > **Route List**

Step 4 Click **Add** to create route list.
Step 5 Choose required IP address from **CUCM** drop-down list to add route list.
Step 6 Enter a unique route list name in **Name** field.
Step 7 Click **Add** icon in **Route Group Items** panel.
Step 8 Choose the route group from **Route Group Name** drop-down list.
Step 9 Click **Save**.

Edit Route List

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.
Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.
Step 3 Navigate to **Route List**:

- For provider or reseller administrator **Device Management** > **CUCM** > **Route List**
- For customer administrator **Device Management** > **Advanced** > **Route List**

Step 4 Click the route list from the list that you want to edit and modify the required fields.
Step 5 Click **Save**.

Delete Route List

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.
Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.
Step 3 Navigate to **Route List**:

- For provider or reseller administrator **Device Management** > **CUCM** > **Route List**

- For customer administrator **Device Management** > **Advanced** > **Route List**

Step 4 Click the route list from the list that you want to delete.

Step 5 Click **Delete**.

Configure Route Patterns

Before you begin

Ensure Route Lists are configured. See Configure Route List, on page 285.

Perform the following instructions to configure route patterns:

- Add Route Pattern, on page 287
- Edit Route Patterns, on page 287
- Delete Route Pattern, on page 288

Add Route Pattern

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **Route Patterns**:

- For provider or reseller administrator **Device Management** > **CUCM** > **Route Patterns**
- For customer administrator **Device Management** > **Advanced** > **Route Patterns**

Step 4 Click **Add** to create route pattern.

Step 5 Perform the following, In **Pattern Defination** tab:

a) Choose required IP address from **CUCM** drop-down list that you want to add route pattern.
b) Enter a unique name in **Route Pattern** field.
c) Choose either route list or trunk from respective drop-down list, in **Destination (Only Choose Route List or Gateway)** panel.

Step 6 Click **Save**.

Edit Route Patterns

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **Route Patterns**:

- For provider or reseller administrator **Device Management** > **CUCM** > **Route Patterns**
- For customer administrator **Device Management** > **Advanced** > **Route Patterns**

Step 4 Click the route pattern from the list that you want to edit and modify the required fields.

Step 5 Click **Save**.

Delete Route Pattern

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **Route Patterns**:

- For provider or reseller administrator **Device Management** > **CUCM** > **Route Patterns**
- For customer administrator **Device Management** > **Advanced** > **Route Patterns**

Step 4 Click the route pattern from the list that you want to delete.

Step 5 Click **Delete**.

Configure Cisco Unified CM Group

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **Unified CM Groups**.

- For provider or reseller administrator **Device Management** > **CUCM** > **Unified CM Groups**
- For customer administrator **Device Management** > **Advanced** > **Unified CM Groups**

Step 4 Enter unique Unified CM group name in **Name** field.

Step 5 Click **Add** icon in **Unified CM Group items** panel.

Step 6 Enter **Priority**.

Step 7 Choose appropriate CUCM from **Selected Cisco Unified Communications Manager** field.

Step 8 Click **Save**.

Configure Device Pool

Ensure that Cisco Unified CM Group is configured. See, Configure Cisco Unified CM Group, on page 288.

Add Device Pool

Procedure

Step 1 Login to Cisco Unified Communications Domain Manager as provider/reseller or customer admin.

Step 2 Ensure that hierarchy is set to node where CUCM is configured.

Step 3 Navigate to **Device pool**:

- For provider/reseller **Device Management** > **CUCM** > **Device Pools**
- For customer admin **Device Management** > **Advanced** > **Device Pools**

Step 4 Click **Add**.

Step 5 Choose **Network Device List** from the drop-down list.

Step 6 In **Device Pool Settings** tab:

a) Enter **Device Pool Name**.
b) Choose call manager group from **Cisco Unified Communication Manager** drop-down list.

Step 7 Goto **Roaming Sensitive Settings** tab:

a) Choose **Date/Time Group** from drop-down list.
b) Choose **Region** from drop-down list.
c) Choose **SRST Reference** from drop-down list

Step 8 Click **Save**.

Edit Device Pool

Procedure

Step 1 Login to Cisco Unified Communications Domain Manager as provider/reseller or customer admin.

Step 2 Navigate to **Device pool**:

- For provider/reseller **Device Management** > **CUCM** > **Device Pools**
- For customer admin **Device Management** > **Advanced** > **Device Pools**

Step 3 Click device pool from the list that you want to edit and modify the required fields.

Step 4 Click **Save**.

Delete Device Pool

Procedure

Step 1 Login to Cisco Unified Communications Domain Manager as provider/reseller or customer admin.

Step 2 Navigate to **Device pool**:

- For provider/reseller **Device Management** > **CUCM** > **Device Pools**
- For customer admin **Device Management** > **Advanced** > **Device Pools**

Step 3 Click device pool from the list that you want to delete.

Step 4 Click **Delete**.

Configure Directory Number Inventory and Lines

- Add Directory Number Inventory, on page 290
- Edit Lines, on page 291
- Delete Lines, on page 291

Add Directory Number Inventory

Before you begin

Ensure Site dial plan is created, see Add Site Dial Plan, on page 180.

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as a provider, reseller or customer.

Step 2 Ensure that hierarchy path is set to appropriate customer.

Step 3 Navigate to **Dial Plan Management** > **Customer** > **Number Management** > **Add Directory Number Inventory**.

Step 4 Choose **Site** from drop-down list that you want to add directory numbers.

Step 5 Enter **Starting Extension** value.

Step 6 If you want to set the range, enter **Ending Extension** value.

Step 7 Click **Save**.

Newly added directory number to inventory does not add directory number to Cisco Unified Communication Manager unless it is associated with a phone.

Edit Lines

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as a provider, reseller or customer.
Step 2 Ensure that hierarchy path is set to appropriate customer.
Step 3 Navigate to **Subscriber Managemet** > **Lines**.
Step 4 Click line from the list that you want to edit and modify the required fields.
Step 5 Click **Save**.

Delete Lines

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as a provider, reseller or customer.
Step 2 Ensure that hierarchy path is set to appropriate customer.
Step 3 Navigate to **Subscriber Managemet** > **Lines**.
Step 4 Click line from the list that you want to delete.
Step 5 Click **Delete**.

Configure Phones

Before you begin

Ensure Directory Number Inventory is created, see Add Directory Number Inventory, on page 290

Perform the following instructions to configure phones:

- Add Phones, on page 291
- Edit Phones, on page 293
- Delete Phones, on page 293

Add Phones

Perform the following to add phone for provider, reseller or customer.

- Add Phones as Provider or Reseller, on page 292
- Add Phones as Customer, on page 292

Add Phones as Provider or Reseller

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider or reseller .

Step 2 Ensure that hierarchy is set to appropriate site.

Step 3 Navigate to **Subscriber Management** > **Phones**.

Step 4 Click **Add**.

Step 5 Enter a unique **Device Name** with the prefix SEP.

Example:

SEPA1B2C3D4E5F6

Step 6 Choose **Product Type** from the drop-down list.

Step 7 Choose **Device Protocol** from the drop-down list.

Step 8 Choose **Calling Search Space** from drop-down list.

Step 9 Choose **Device Pool** from drop-down list.

Step 10 Choose **Location** from drop-down list.

Step 11 Goto **Lines** tab and perform the following:

a) Click **Add** icon in **Lines** panel to add line.
b) Choose directory number from **Pattern** drop-down list, in **Dirn** panel.
c) Choose **Route Partition Name** from drop-down list.

Step 12 Click **Save**.

Add Phones as Customer

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as customer.

Step 2 Ensure that hierarchy is set to appropriate site.

Step 3 Navigate to **Subscriber Management** > **Phones**.

Step 4 Click **Add**.

Step 5 Choose **Product Type** from the drop-down list.

Step 6 Choose **Protocol** from the drop-down list.

Step 7 Enter a unique **Device Name** with the prefix SEP.

Example:

SEPA1B2C3D4E5F6

Step 8 Choose **Calling Search Space** from drop-down list.

Step 9 Goto **Advanced Information** tab and perform the following:

a) Choose **Device Pool** from drop-down list.
b) Choose **Location** from drop-down list.

Step 10 Goto **Lines** tab and perform the following:

a) Click **Add** icon in **Lines** panel to add line.
b) Choose directory number from **Pattern** drop-down list, in **Dirn** panel.
c) Choose **Route Partition Name** from drop-down list.

Step 11 Click **Save**.

Edit Phones

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer.
Step 2 Ensure that hierarchy is set to appropriate site.
Step 3 Navigate to **Subscriber Management** > **Phones**.
Step 4 Click phone from the list that you want to edit and modify the required field.
Step 5 Click **Save**.

Delete Phones

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer.
Step 2 Ensure that hierarchy is set to appropriate site.
Step 3 Navigate to **Subscriber Management** > **Phones**.
Step 4 Click phone from the list that you want to delete.
Step 5 Click **Delete**.

Configure Regions

- Add Regions, on page 293
- Edit Regions, on page 294
- Delete Regions, on page 294

Add Regions

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.
Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **Device Management** > **CUCM** > **Regions**.
Step 4 Click **Add**.
Step 5 Choose **CUCM** from the drop-down list.
Step 6 Enter unique region name in **Name** field.
Step 7 Expand **Related Regions**.
Step 8 Choose **Use System Default** from **Immersive Video Bandwidth (Kbps)** drop-down list.
Step 9 Keep the default selection in **Audio Bandwidth (Kbps)** drop-down list.
Step 10 Choose **Use System Default** from **Video Bandwidth (Kbps)** drop-down list.
Step 11 Choose **Use System Default** from **Audio Codec Preferrence** drop-down list.
Default codec is G.711.
Step 12 Choose **Region Name** from drop-down list.
Step 13 Click **Save**.

Edit Regions

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.
Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.
Step 3 Navigate to **Device Management** > **CUCM** > **Regions**.
Step 4 Click the regions from the list that you want to edit and modify the required fields.
Step 5 Click **Save**.

Delete Regions

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.
Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.
Step 3 Navigate to **Device Management** > **CUCM** > **Regions**.
Step 4 Click the region that you want to delete.
Step 5 Click **Delete**.

Configure Class of Service

Use this procedure to create a new Calling Search Space (CSS) or edit an existing CSS that is tied to a site. The CSS can be used as a Class of Service (COS) for a device or line, or any of the other templates that rely on COS to filter different features.

Add Class of Service

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to valid site under customer.

Step 3 Navigate **Dial Plan Management** > **Site** > **Class of Service**

Step 4 Click **Add**.

Step 5 Enter unique **Class of Service Name**.

This name can use alphanumeric characters, periods, underscores, hyphens and spaces, it should not exceed 50 characters. You can also make use of macros that are available in the system to create a Class Of Service name. Macros allow you to dynamically add site IDs, customer IDs, and other types of information to the CSS.

Example:

Cu1-24HrsCLIP-PT-{{macro.HcsDpSiteName}}

Step 6 Expand **Member** panel to add partition.

Step 7 Choose partition from drop-down list under **Selected Partitions** column.

Note
- Click **Add** icon to add more partitions, repeat this step to add desired members to this Class of Service.
- Add **`Cu<CUSTOMER_ID>CC<CC_SERVER_ID>-Xfer4CCServer-PT`** to the Class of Service partition member list.

Step 8 Click **Save**.

Edit Class of Service

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to valid site under customer.

Step 3 Navigate **Dial Plan Management** > **Site** > **Class of Service**

Step 4 Click Class of Service from the list that you want to edit and modify the required fields.

Step 5 Click **Save**.

Delete Class of Service

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.
Step 2 Ensure that hierarchy is set to valid site under customer.
Step 3 Navigate **Dial Plan Management** > **Site** > **Class of Service**
Step 4 Click Class of Service from the list that you want to delete.
Step 5 Click **Delete**.

Associate Phone to Application User

Before you begin

Phones should be added, see Add Phones, on page 291

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer.
Step 2 Ensure that hierarchy is set to appropriate site.
Step 3 Navigate to **Subscriber Management** > **Agent Lines**.
Step 4 Click **Add** to add new agent line.
Step 5 Choose **Phones** from **Device Type** drop-down list.
Step 6 Choose device from **Device Name** drop-down list.
Step 7 Choose **Line** from drop-down list.
Step 8 Choose **Application User** from drop-down list.
Step 9 Click **Save**.

Disassociate Unified Communication Manager from UCDM

To retain Unified Communication Manager configurations, perform the following before deleting the customer:

Procedure

Step 1 Login to UCDM as provider or reseller.
Step 2 Choose the customer from hierarchy that you want to disassociate CUCM.
Step 3 Navigate to **Device Management** > **CUCM** > **Servers**.
Step 4 Click the CUCM that you want to disassociate.
Step 5 Click **Remove** icon in **Network Addresses** panel.

Step 6 Click **Save**.

Built-in-Bridge

Built-in-Bridge (BIB) is not enabled by default for the phones. It is disabled at the system level as it is not used by all the customer by default. It is used only by the customers having Contact Center.

The provider has to perform the following procedures to enable BIB for the customers having contact center.

Note Create a new Field Display Policies at the customer level and add Built-in Bridge to the list.

- Configure the Built-in-Bridge , on page 297
- Enable or Disable the Built-in-Bridge , on page 297

Configure the Built-in-Bridge

Procedure

Step 1 Login to **Cisco Unified Communication Domain Manager** as provider.
Step 2 Navigate **Role Management** > **Field Display Policies**.
Step 3 Ensure that hierarchy is set to the appropriate customer.
Step 4 Select the **SubscriberPhoneMenuItemProvider**.
Step 5 In the details page, go to **Action** menu and click **Clone**.
Step 6 Enter **SubscriberPhoneMenuItemProvider** as the name.
Step 7 Select **relation/SubscriberPhone** from the **Target Model Type** drop-down list.
Step 8 Expand **Groups** section and enter **Phone** for Title.
Step 9 Select **builtInBridgeStatus** from the **Available** list and click **Select**.
Step 10 Click **Save**.

Enable or Disable the Built-in-Bridge

Before you begin

Ensure that you configure Built-in-Bridge. See, Configure the Built-in-Bridge , on page 297.

Procedure

Step 1 Login to **Cisco Unified Communication Domain Manager** as a provider.
Step 2 Ensure that hierarchy is set to the appropriate customer.
Step 3 Navigate **Subscriber Management** > **Phones** and select the appropriate phone.
Step 4 In the **Phone** tab:

- To enable BIB choose **On** from the **Built in Bridge** drop-down list.
- To disable BIB choose **Off** from the **Built in Bridge** drop-down list.

Step 5 Click **Save**.

Bulk Operations Using UCDM

The bulk upload option is used for importing large numbers of resource items into Cisco Unified Communications Domain Manager (UCDM). It is used to generate resources for UCDM objects by filling in the resource attributes using the standard .xlsx format. All .xlsx files require headers that dictate where each value goes. These headers are provided by templates that can be downloaded from the appropriate Bulk Upload page in UCDM.

There are three ways to provision the bulk upload:

1. HCS Intelligent Loader (HIL)
2. Cisco Unified Communications Domain Manager Administrative tools/bulkloader
3. Cisco Unified Communications Domain Manager REST API

For more information on provisioning bulk upload, see *Cisco Unified Communications Domain Manager, Bulk Provisioning Guide*. You can find this guide on the **Component Documentation** tab here:http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-version-10-6-1/model.html#~tab-solution-documentation.

Cisco Unified Communications Domain Manager Administration Tools/Bulkloader

- Export Bulk Load, on page 298
- Bulk Load Sheets, on page 298
- Perform Bulk Upload, on page 299

Export Bulk Load

Procedure

Step 1 Login to Unified Communication Domain Manager as provider, reseller or customer.
Step 2 Ensure the hierarchy is set to appropriate level for required UCDM object.
Step 3 Goto the required form of any UCDM object that supports bulk load.
Step 4 Click **Action** and click **Export Bulk Load** Template in submenu.
Step 5 Save Bulk load Template in .xlsx format in your local drive.

Bulk Load Sheets

An exported bulk load template is a workbook containing a single sheet and serves as the basis for bulk loading. A workbook can also be created that contains more than one sheet as a tabbed workbook.

For tabbed workbooks, bulk load transactions are carried out from the leftmost sheet or tab to the rightmost. For example, if a site is to be added under a customer, the customer sheet tab should be to the left of the associated site.

The spreadsheet workbook is in Microsoft Excel .xlsx format. The maximum file upload size is 4GB. You can enter any name for the workbook or enter the same filename and load the file multiple times, although it is appropriate to use different names.

To bulk load data, preliminary steps need to be carried out. Verify existing information on the sheet and determine required information in order to complete the required data and prepare the spreadsheet.

Perform Bulk Upload

Procedure

Step 1 Login to Unified Communication Domain Manager as provider, reseller or customer.

Step 2 Ensure the hierarchy is set to appropriate level for required UCDM object.

Step 3 Navigate to **Administrative Tools** > **Bulk Load**.

Step 4 Click **Browse** to open file upload dialog box.

Step 5 Click **Bulk Load File**.

Note If you want to check the status of bulk load, navigate to **Administrative Tools** > **Transactions**.

Increase the SW MTP and SW Conference Resources

Procedure

Step 1 Login to the **CUCM Administration** web page.

Step 2 Under the **System** tab, select the **Service Parameter**.

Step 3 Select the CUCM server from the drop-down list.

Step 4 Select the **Cisco IP Voice Media Streaming App** service.

Step 5 Modify the Conference Bridge (CFB) parameters and the Media Termination Point (MTP) parameters field as following:

- SW CFB:

  Default total conference parties : 48 (16 CFB 3-party sessions)

  Maximum conference parties : 256 (85 CFB 3-party sessions)

- SW MTP:

  Default total MTP parties : 48 (24 MTP sessions with 2-parties per session)

  Maximum MTP parties : 512 (256 MTP sessions)

Single Sign-on Administration

Set up the System Inventory for Single Sign-On

Set up the System Inventory before configuring the Cisco Identity Service (Cisco IdS) and the components for single sign-on. By default, the System Inventory displays a list of all AWs, Routers, and Peripheral Gateways in the deployment.

The Principal AW (Admin Workstation) is responsible for managing background tasks that are run periodically to sync configuration with other solution components, such as SSO management, Smart Licensing, etc.

Select the Principal AW to manage to register the components with the Cisco IdS and enabling them for SSO. Add the remaining SSO-capable machines to the System Inventory, and select the default Cisco IdS for each of the SSO-capable machines.

Procedure

Step 1 In Unified CCE Administration, navigate to **Features** > **Single Sign-On**.

Step 2 Set the Principal AW:

a) Click the AW that you want to be the Principal AW.

Note If the AW is coresident with the Router, you can set the Principal AW on the Router.

The **Edit AW** popup window opens.

b) Check the **Principal AW** check box on the General tab.

c) Enter the Unified CCE Diagnostic Framework Service domain, username, and password.

These credentials must be for a domain user who is a member of the Config security group for the instance. These credentials must be valid on all CCE components in your deployment (Routers, PGs, AWs, and so on).

d) Click **Save**.

Step 3 Add the SSO-capable machines to the System Inventory:

a) Click **New**.
The **Add Machine** popup window opens.

b) From the **Type** drop-down, select one of the following types of machines:

- **Finesse Primary**
- **CUIC, LD, IdS Publisher**, if you're using coresident deployment applicable for 2000 agent reference design.
- **Unified Intelligence Center Publisher**, if you're using a standalone Unified Intelligence Center
- **Identity Service Primary**, if you're using a standalone Cisco IdS

c) In the **Hostname** field, enter the FQDN, IP address, or hostname of the machine.

Note If you don't enter the FQDN, the system converts the value you enter to FQDN.

d) Enter the machine's Administration credentials.
e) Click **Save**.
The machine and its related Subscriber or Secondary machine are added to the System Inventory.
f) Repeat this procedure to add all of the SSO-capable machines in the deployment.

Step 4 Select the default Identity Service for each of the following machines:

- All Unified CCE AW servers
- Finesse Primary and Secondary
- Unified Intelligence Center Publisher and Subscriber

Note If you're using a coresident CUIC, LD, Ids Publisher and Subscriber, you don't need to set the default Cisco IdS for those machines.

In a standalone deployment, select the Cisco IdS that's deployed on the same Data Center Side (A or B) as the machine that you're configuring. For example, in the Reference Deployment:

- Select the Identity Service Publisher (IdS A) for AW-HDS-DDS 1, AW-HDS 3, Finesse 1 Pub, Finesse 2 Pub, CUIC Pub, and CUIC Sub 1.
- Select the Identity Service Subscriber (Ids B) for AW-HDS-DDS 2, AW-HDS 4, Finesse 1 Sub, Finesse 2 Sub, CUIC Sub 2, and CUIC Sub 3.

For details on the Reference Deployment, see *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

a) Click a machine to open the **Edit Machine** popup window.
b) Click the Search icon next to **Default Identity Service** to open the **Select Identity Service** popup window.
c) Enter the machine name for the Cisco IdS in the Search field and choose the Cisco IdS from the list.
d) Click **Save**.

Configure the Cisco Identity Service

The Cisco Identity Service (Cisco IdS) provides authorization between the Identity Provider (IdP) and applications.

When you configure the Cisco IdS, you set up a metadata exchange between the Cisco IdS and the IdP. This exchange establishes a trust relationship that then allows applications to use the Cisco IdS for single sign-on. You establish the trust relationship by downloading a metadata file from the Cisco IdS and uploading it to the IdP. You can then select settings related to security, identify clients of the Cisco IdS service, and set log levels and, if desired, enable Syslog format.

Procedure

Step 1 In Administration, navigate to **Features** > **Single Sign-On**.

Note Use a log in name in the format *username@FQDN* to log in to the Administration.

Step 2 Click **Identity Service Management**.

Result:

The Cisco Identity Service Management window opens.

Step 3 Enter your user name, and then click **Next**.

Step 4 Enter your password, and then click **Sign In**.

The Cisco Identity Service Management page opens, showing the **Nodes**, **Settings**, and **Clients** icons in the left pane.

Step 5 Click **Nodes**.

The **Nodes** page opens to the overall Node level view and identifies which nodes are in service. The page also provides the **SAML Certificate Expiry** details for each node, indicating when the certificate is due to expire. The node **Status** options are **Not Configured**, **In Service**, **Partial Service**, and **Out of Service**. Click a status to see more information. The star to the right of one of the Node names identifies the node that is the primary publisher.

Step 6 Click **Settings**.

Step 7 Click **IdS Trust**.

Step 8 To begin the Cisco IdS trust relationship setup between the Cisco IdS and the IdP, click **Download Metadata File** to download the file from the Cisco IdS Server.

Step 9 Click **Next**.

Step 10 To upload the trusted metadata file from your IdP, browse to locate the file.

The **Upload IdP Metadata** page opens and includes the path to the IdP. When the file upload finishes, you receive a notification message. The metadata exchange is now complete, and the trust relationship is in place.

Step 11 Clear the browser cache.

Step 12 Enter the valid credentials, when page is redirected to IdP.

Step 13 Click **Next**.

The **Test SSO Setup** page opens.

Step 14 Click **Test SSO Setup**.

A message appears telling you that the Cisco IdS configuration has succeeded.

Step 15 Click **Settings**.

Step 16 Click **Security**.

Step 17 Click **Tokens**.

Enter the duration for the following settings:

- **Refresh Token Expiry** -- The default value is 10 hours. The minimum value is 2 hours. The maximum is 24 hours.
- **Authorization Code Expiry** -- The default value is 1 minute, which is also the minimum. The maximum is 10 minutes.
- **Access Token Expiry** -- The default value is 60 minutes. The minimum value is 5 minutes. The maximum is 120 minutes.

Step 18 Set the **Encrypt Token** (optional); the default setting is **On**.

Step 19 Click **Save**.

Step 20 Click **Keys and Certificates**.

The **Generate Keys and SAML Certificate** page opens and allows you to:

- Regenerate the **Encryption/Signature key** by clicking **Regenerate**. A message appears to say that the Token Registration is successful and advises you to restart the system to complete the configuration.
- Regenerate the **SAML Certificate** by clicking **Regenerate**. A message appears to say that the SAML certificate regeneration is successful.

Step 21 Click **Save**.

Step 22 Click **Clients**.
The **Clients** page identifies the existing Cisco IdS clients, providing the client name, the client ID, and a redirect URL. To search for a particular client, click the Search icon above the list of names and type the client's name.

Step 23 To add a client:

a) Click **Add Client**.
b) Enter the client's name.
c) Enter the Redirect URL. To add more than one URL, click the plus icon.
d) Click **Add** (or click **Clear** and then click the X to close the page without adding the client).

Step 24 To edit or delete a client, highlight the client row and click the ellipses under **Actions**. Then:

- Click **Edit** to edit the client's name, ID, or redirect URL. On the **Edit Client** page, make changes and click **Save** (or click **Clear** and then click the X to close the page without saving edits).
- Click **Delete** to delete the client.

Step 25 Click **Settings**.

Step 26 From the **Settings** page, click **Troubleshooting** to perform some optional troubleshooting.

Step 27 Set the local log level by choosing from **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.

Step 28 To receive errors in Syslog format, enter the name of the Remote Syslog Server in the Host (Optional) field.

Step 29 Click **Save**.

You can now:

- Register components with the Cisco IdS.
- Enable (or disable) SSO for the entire deployment.

Register Components and Set Single Sign-On Mode

If you add any SSO-compatible machines to the System Inventory after you register components with the Cisco IdS, those machines are registered automatically.

Before you begin

- Configure the Cisco Identity Service (Cisco IdS).
- Disable popup blockers. It enables viewing all test results correctly.
- If you are using Internet Explorer, verify that:
  - It is not in the Compatibility Mode.

- You are using the fully qualified domain name of AW to access the CCE Administration (for example, **https://<FQDN>/cceadmin**).

Procedure

Step 1 In the Unified CCE Administration, navigate to **Features** > **Single Sign-On**.

Step 2 Click the **Register** button to register all SSO-compatible components with the Cisco IdS.

The component status table displays the registration status of each component.

If a component fails to register, correct the error and click **Retry**.

Step 3 Click the **Test** button. When the new browser tab opens, you may be prompted to accept a certificate. In order for the page to load, accept any certificates. Then, when presented with a log in dialog, log in as a user with SSO credentials.

The test process verifies that each component has been configured correctly to reach the Identity Provider, and that the Cisco IdS successfully generates access tokens. Each component that you are setting up for SSO is tested.

The component status table displays the status of testing each component.

If a test is unsuccessful, correct the error, and then click **Test** again.

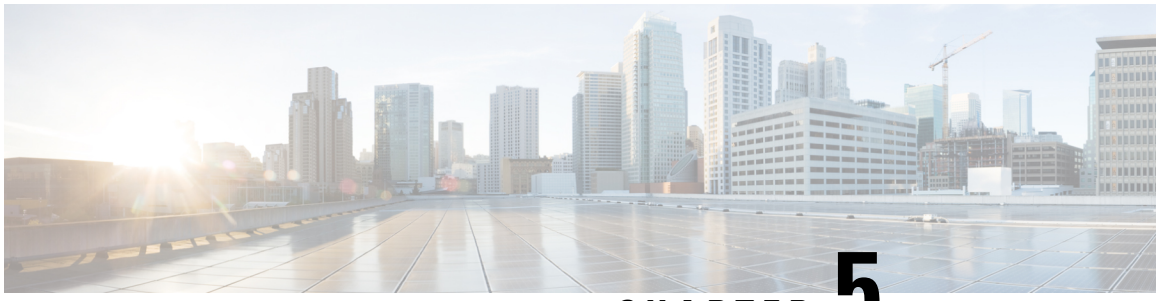
Test results are not saved. If you refresh the page, run the test again before enabling SSO.

Step 4 Select the SSO mode for the system from the **Set Mode** drop-down menu:

- Non-SSO: This mode disables SSO for all agents and supervisors. Users log in using existing Active Directory-based local authentication.
- Hybrid: This mode allows you to enable agents and supervisors selectively for SSO.
- SSO: This mode enables SSO for all agents and supervisors.

The component status table displays the status of setting the SSO mode on each component.

If the SSO mode fails to be set on a component, correct the error, and then select the mode again.



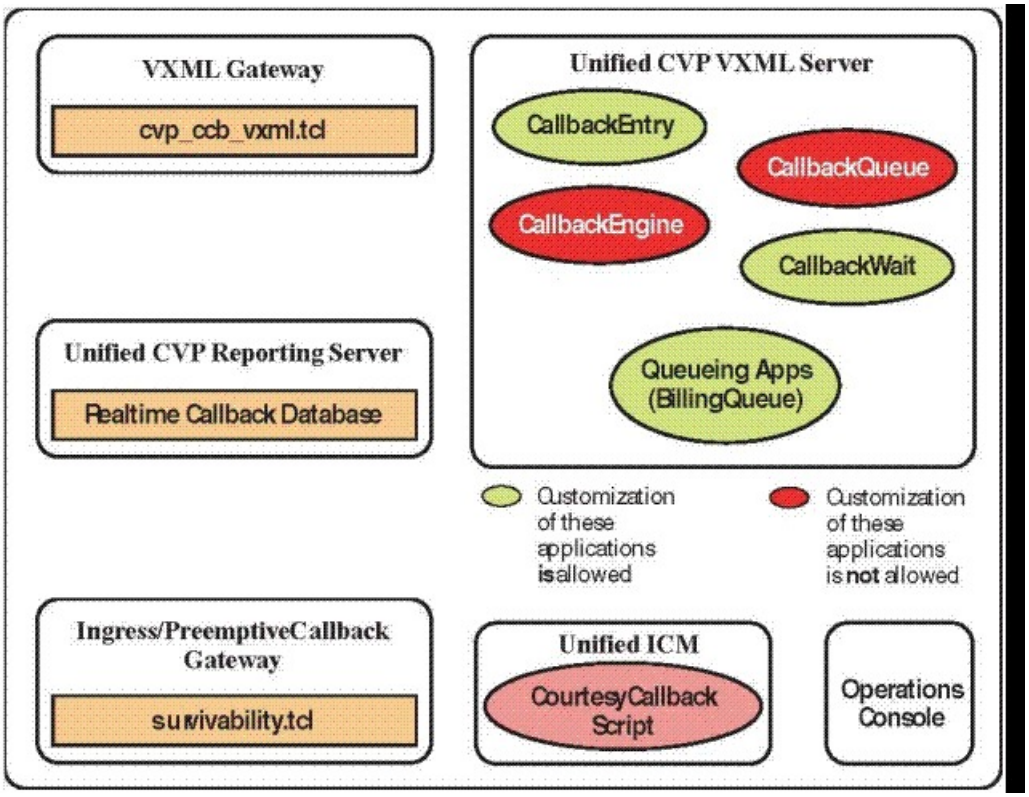
CHAPTER 5

Configure Core Component Integrated Options

Configure Courtesy Callback

The following diagram shows the components that you must configure for Courtesy Callback.

Figure 9: Courtesy Callback components



Complete the following procedures for Courtesy Callback configurations:

- Configure Gateway, on page 306
- Configure Unified CVP, on page 309
- Configure Unified CCE, on page 313

Configure Gateway

Configure the VXML Gateway for Courtesy Callback

Complete the following procedure to configure the VXML gateway for Courtesy Callback:

Procedure

Step 1 Copy **cvp_ccb_vxml.tcl** from the CVP Operations Console to the flash memory of the gateway, as follows:

a) Select **Bulk Administration** > **File Transfer** > **Scripts and Media**.
b) In Device Association, select **Gateway** for Device Type.
c) Select the required gateway from the Available list.
d) Click the right arrow icon to move the available gateway to the Selected list.
e) From the default gateway files, highlight **cvp_ccb_vxml.tcl**.

f) Click **Transfer**.

Step 2 Log on to VXML gateway.

Step 3 Add the cvp_cc service to the configuration **service cvp_cc flash:cvp_ccb_vxml.tcl**.

This service does not require any parameters.

Step 4 Enter the following command to load the application:

call application voice load cvp_cc

Step 5 On the VoIP dial-peer that defines the VRU from Unified CCE, verify that the codec can be used for recording.

Example:

The following example verifies that g711ulaw can be used for recording in Courtesy Callback:

```
dial-peer voice 123 voip
 service bootstrap
 incoming called-number 123T
 dtmf-relay rte-nte
 h245-signal
 h245-alphanumeric
 codec g711ulaw
 no vad!
```

Step 6 Configure the following to ensure that SIP is setup to forward SIP INFO messaging:

```
voice service voip
 signaling forward unconditional
```

Step 7 To play the beep to prompt the caller to record their name in the BillingQueue example script add the following text to the configuration:

vxml version 2.0

Note Whenever you enable vxml version 2.0 on the gateway, vxml audioerror is **off** by default. When an audio file cannot be played, error.badfetch will **not** generate an audio error event.

To generate an error in the gateway, enable vxmlaudioerror.

Example:

The following example uses config terminal mode to add both commands:

```
config t
vxml version 2.0
vxml audioerror
exit
```

Configure the Ingress Gateway for Courtesy Callback

Complete the following procedure to configure the ingress gateway for courtesy callback:

Procedure

Step 1 Copy `surviability.tcl` from the Operations Console to the flash memory of the gateway, as follows:

a) Select **Bulk Administration** > **File Transfer** > **Scripts and Media**.

b) In Device Association, select **Gateway** for Device Type.
c) Select the required gateway from the Available list.
d) Click the right arrow icon to move the available gateway to the Selected list.
e) From the default gateway files, highlight **survivability.tcl**.
f) Click **Transfer**.

Step 2 Log onto the ingress gateway.

Step 3 Add the following to the survivability service:

```
param ccb id:<host name or ip of this gateway>;loc:<location name>;trunks:<number of callback trunks>
```

- **id -** A unique identifier for this gateway and is logged to the database to show which gateway processed the original callback request.
- **loc -** An arbitrary location name specifying the location of this gateway.
- **Trunks -** The number of DS0's reserved for callbacks on this gateway. Limit the number of T1/E1 trunks to enable the system to limit the resources allowed for callbacks.

Example:

The following example shows a basic configuration:

```
service cvp-survivability flash:survivability.tcl
param ccb id:10.86.132.177;loc:doclab;trunks:1!
```

Step 4 Create the incoming POTS dial peer, or verify that the survivability service is being used on your incoming POTS dial peer.

Example:

For example,

```
dial-peer voice 978555 pots
service cvp-survivability
incoming called-number 9785551234
direct-inward-dial!
```

Step 5 Create outgoing POTS dial peers for the callbacks. These are the dial peers that place the actual call back out to the PSTN.

Example:

For example,

```
dial-peer voice 978555 pots
destination-pattern 978555....
no digit-strip port 0/0/1:23!
```

Step 6 Use the following configuration to ensure that SIP is set up to forward SIP INFO messaging:

voice service voip signaling forward unconditional

Configure CUBE-E for Courtesy Callback

Note If you are using CUBE-E then you need sip profile configuration and apply it on outgoing dial-peer through cvp. See the below the example:

A "sip-profile¨ configuration is needed on ISR CUBE E for the courtesy callback feature. To configure the "sip-profile", the following must be added

```
voice class sip-profiles 103

request INVITE sip-header Call-Info add "X-Cisco-CCBProbe: <ccb param>"
```

where "<ccb param>" is the "ccb" parameter defined in the survivability service. Add this "sip-profile" to the outgoing dial-peer to the CVP.

The following is a configuration example

```
voice class sip-profiles 103

request INVITE sip-header Call-Info add "X-Cisco-CCBProbe: id:10.10.10.180;sydlab;trunks:4"

dial-peer voice 5001 voip

description Comprehensive outbound route to CVP

destination-pattern 5001

session protocol sipv2

session target ipv4:10.10.10.10

dtmf-relay rtp-nte

voice-class sip profiles 103

codec g711ulaw

no vad
```

In the above example, **10.10.10.180** is the CUBE IP and **10.10.10.10** is the CVP Call Server IP.

Note If CUBE E is used for Courtesy Call Back then under voice service voip class in CUBE E must have media flow-through for Courtesy Call Back to work.

Configure Unified CVP

Configure the Reporting Server for Courtesy Callback

A reporting server is required for the Courtesy Callback feature. Complete the following procedure to configure a reporting server for Courtesy Callback:

Before you begin

Install and configure the Reporting Server.

Procedure

Step 1 In the Operations Console, select **System > Courtesy Callback**.

The *Courtesy Callback Configuration* page displays.

Step 2 Choose the **General** tab.

Step 3 Click the **Unified CVP Reporting Server** drop-down, and select the Reporting Server to use for storing Courtesy Callback data.

Step 4 If required, select **Enable secure communication with the Courtesy Callback database**.

Step 5 Configure allowed and disabled dialed numbers.

These are the numbers that the system should and should not call when it is making a Courtesy Callback to a caller.

Note Initially, there are no allowed dialed numbers for the Courtesy Callback feature. Allow Unmatched Dialed Numbers is de-selected and, the Allowed Dialed Numbers window is empty.

Step 6 Adjust the Maximum Number of Calls per Calling Number to the desired number.

By default, this is set to 0 and no limit is imposed. This setting allows you to limit the number of calls that are eligible to receive a callback from the same calling number.

If this field is set to a positive number (X), then the Courtesy Callback Validate element only allows X callbacks per calling number to go through the preemptive exit state at any time.

If there are already X callbacks offered for a calling number, new calls go through the none exit state of the Validate element.

In addition, if no calling number is available for a call, the call always goes through the none exit state of the Validate element.

Step 7 Choose the **Call Server Deployment** tab and move the Call Server you want to use for Courtesy Callbacks from the Available box to the Selected box.

Step 8 Click **Save**.

The configuration becomes active (is deployed) the next time the Reporting Server is restarted.

Step 9 You can also deploy the new Reporting Server configuration immediately by clicking **Save & Deploy**.

Note After all the updates are configured, restart the Reporting Server to update the configuration.

Configure the Call Studio Scripts for Courtesy Callback

The Courtesy Callback feature is controlled by a combination of Call Studio scripts and ICM scripts. Complete the following procedure to configure the Call Studio scripts:

Procedure

Step 1 Access the .zip file from the CVP OAMP machine from the location `C:\Cisco\CVP\OPSConsoleServer\StudioDownloads\CourtesyCallbackStudioScripts.zip`.

Step 2 Extract the example Call Studio Courtesy Callback scripts contained in CourtesyCallbackStudioScripts.zip to a folder of your choice on the computer running CallStudio.

Each folder contains a Call Studio project having the same name as the folder. The five individual project comprise the Courtesy Callback feature.

Note Do not modify the scripts CallbackEngine and CallbackQueue.

Step 3 Modify the scripts **BillingQueue, CallbackEntry,** and **CallbackWait** to suit your business needs.

Step 4 Start Call Studio by selecting **Start > All Programs > Cisco > Cisco Unified Call Studio**.

Step 5 Select **File > Import**.

The Import dialog box displays.

Step 6 Expand the **Call Studio** folder and select **Existing Call Studio Project Into Workspace**.

Step 7 Click **Next** .

The Import Call Studio Project From File System displays.

Step 8 Browse to the location where you extracted the call studio projects. For each of the folders that were unzipped, select the folder (for example BillingQueue) and select **Finish**.

The project is imported into Call Studio.

Step 9 Repeat the action in previous step for each of the five folders.

The five projects display in the upper-left of the Navigator window.

Step 10 Update the Default Audio Path URI field in Call Studio to contain the IP address and port value for your media server.

Step 11 For each of the Call Studio projects previously unzipped, complete the following steps:

a) Select the project in the Navigator window of Call Studio.
b) Choose **Project > Properties > Call Studio > Audio Settings**.
c) On the Audio Settings window, modify the Default Audio Path URI field to http://<media-server >/en-us/VL/.
d) Click **Apply** then click **OK**.

Step 12 Under **BillingQueue Project**, if required, change the music played to the caller while on hold.

a) Expand the tree structure of the project and click **app.callflow**.
b) Click the node **Audio_01**.
c) Navigate to **Element Configuration** > **Audio** > **Audio Groups** expand the tree structure and click **audio item 1**, Use **Default Audio Path** to change the .wav file to be played.

Step 13 Under CallbackEntry Project, if required, modify the caller interaction settings in the **SetQueueDefault_01** node.

a) In the Call Studio Navigator panel, open the **CallBackEntry** project and double-click **app.callflow** to display the application elements in the script window.
b) Open the Start of Call page of the script using the tab at the bottom of the script display window.
c) Select the **SetQueueDefault_01** node.
d) In the Element Configuration panel, choose the **Setting** tab and modify the default settings as required.

Step 14 In the CallbackEntry project, on the Wants Callback page, configure the following:

a) Highlight the Record Name node and choose the **Settings** tab.

b) In the Path setting, change the path to the location where you want to store the recorded names of the callers.
c) Highlight the **Add Callback to DB 1**node.
d) Change the Recorded name file setting to match the location of the recording folder that you created in the previous step.
e) Ensure the **keepalive Interval**(in seconds) is greater than the length of the queue music being played. In the **Start of Call** page.

   The default is 120 seconds for the **SetQueueDefaults_01 node**.

f) Save the CallbackEntry project.
g) In the CallbackWait Project, modify values in the CallbackWait application.

   In this application, you can change the IVR interaction that the caller receives at the time of the actual callback. The caller interaction elements in CallbackWait > AskIfCallerReady page may be modified. Save the project after you modify it.

h) Validate each of the five projects associated with the Courtesy Callback feature and deploy them to your VXML Server.

Step 15 Right-click each Courtesy Callback project in the **Navigator** window and select **Validate**.

Step 16 Right-click on one of the project and click **Deploy**.

Step 17 Check the check box against each project to select the required projects.

Step 18 In the Deploy Destination area, select **Archive File** and click **Browse**.

Step 19 Navigate to the archive folder that you have set up.

Example:

C:\Users\Administrator\Desktop\Sample.

Step 20 Enter the name of the file.

Example:

For example Samplefile.zip.

Step 21 Click **Save**.

Step 22 In the Deploy Destination area click **Finish**.

Step 23 Log in to OAMP and choose **Bulk Administration\File Transfer\VXMLApplications**.

Step 24 Select the VXML Server to which you want to deploy the applications.

Step 25 Select the zip file that contains the applications.

Example:

Samplefile.zip.

Step 26 Click **Transfer**.

Step 27 Right-click each of the projects and click **Deploy**, then click **Finish**.

Step 28 Using windows explorer, navigate to `%CVP_HOME%\VXMLServer\applications`.

Step 29 For each of the five Courtesy Callback applications, open the project's admin folder, in%CVP_Home%\VXMLServer\applications, and double-click **deployApp.bat** to deploy the application to the VXML Server.

Step 30 Verify that all the applications are running by going into `%CVP_HOME%\VXMLServer\admin` and double-clicking **status.bat**. All five applications should display under Application Name and with the status Running.

Configure the Media Server for Courtesy Callback

Several Courtesy Callback specific media files are included with the sample scripts for Courtesy Callback. Complete the procedure to configure the Media Server for Courtesy Callback:

Procedure

Step 1 During the Unified CVP installation, the media files are copied as: `%CVP_HOME%\OPSConsoleServer\CCBDownloads\CCBAudioFiles.zip`.

Step 2 Unzip the special audio files and copy to your media server `VXMLServer\Tomcat\webapps\CVP\audio`.

The sample scripts are set up to use the default location "\CVP\audio" for the audio files.

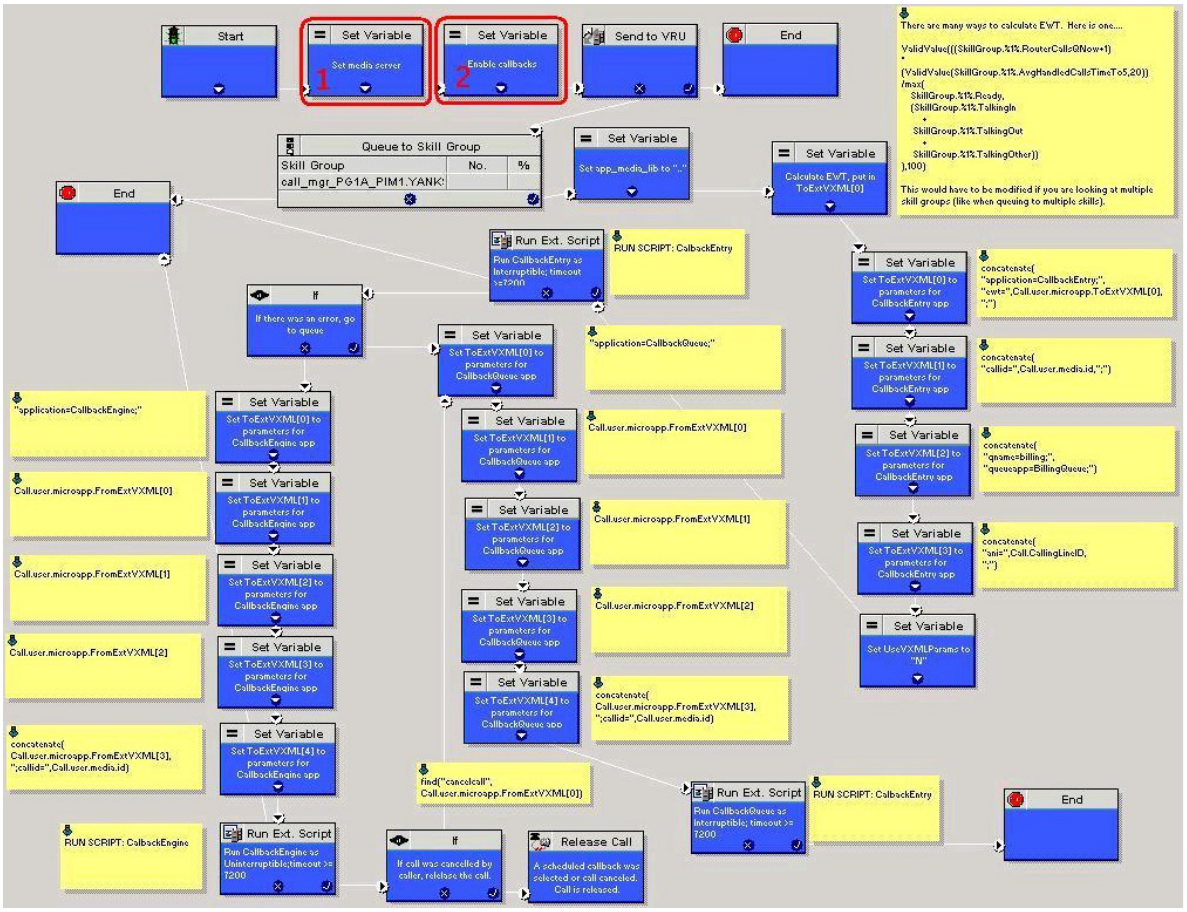
Step 3 Change the default location of the audio files in the sample scripts to be your media server path.

Configure Unified CCE

Configure the ICM Script for Courtesy Callback

Following figure shows the sample Courtesy Callback ICM script.

Figure 10: Sample Courtesy Callback ICM script



Complete the following procedure to configure ICM to use the sample Courtesy Callback ICM script:

Procedure

Step 1 Copy the CCE example script, **CourtesyCallback.ICMS** to the CCE Admin Workstation.
The example CCE script is available in the following locations:

- On the CVP install media in \CVP\Downloads and Samples\.
- From the Operations Console in **%CVP_HOME%\OPSConsoleServer\ICMDownloads**.
- In the Import Script - Manual Object Mapping window, map the route and skill group to the route and skill group available for courtesy callback.

Note For Small Contact Center Deployment Model, copy the CourtesyCallback.ICMS Routing Script on the desktop where Internet Script editor is installed.

Step 2 In Script Editor, select **File > Import Script...**

Note For Small Contact Center Deployment Model follow the below steps.

a. Log In to ISE by sub customer user and Click on File>Import Script.
b. Select the Routing script which is copied in the desktop **CourtesyCallback.ICMS**.

Step 3 In the script location dialog, select the **CourtesyCallback.ICMS** script and click **Open**. You can bypass the set variable "**Set media server**" Highlighted as number 1 node in the Figure 10: Sample Courtesy Callback ICM script, on page 314, as VXML Server, Call Server, and Media Server are collocated.

Step 4 Define a new ECC variable for courtesy callback.

A new ECC variable is used to determine if a caller is in a queue and can be offered a callback.

Step 5 Navigate to **ICM Admin Workstation > ICM Configuration Manager > Expanded Call Variable List tool** to create the ECC Variable **user.CourtesyCallbackEnabled** specific to Courtesy Callback.

Step 6 Set up the following parameters that are passed to CallbackEntry (VXML application):

Example:

- ToExtVXML[0] =concatenate("application=CallbackEntry",";ewt=",Call.user.microapp.ToExtVXML[0])
- ToExtVXML[1] = "qname=billing";
- ToExtVXML[2] = "queueapp=BillingQueue;"
- ToExtVXML[3] = concatenate("ani=",Call.CallingLineID,";");

CallbackEntry is the name of the VXML Server application that is run:

ewt is calculated in **Block #2**.

qname is the name of the VXML Server queue into which the call will be placed. There must be a unique qname for each unique resource pool queue.

queueapp is the name of the VXML Server queuing application that is run for this queue.

ani is the caller's calling Line Identifier.

Step 7 Create Network VRU Scripts.

Step 8 Navigate to **ICM Configuration Manager > Network VRU Script List tool**, create the following Interruptible Script Network VRU Scripts.

Name: **VXML_Server_Interruptible**

Network VRU: Select your Type 10 CVP VRU

VRU Script Name: **GS,Server,V,interrupt**

Timeout: **9000 seconds**

Interruptible: **Checked**

Step 9 Choose **ICM Configuration Manager > Network VRU Script List tool** to create the following Non-Interruptible Script Network VRU Scripts.

Name - **VXML_Server_NonInterruptible**

Network VRU - Select your Type 10 CVP VRU

VRU Script Name - **GS,Server,V, nointerrupt**

Timeout - **9000 seconds (must be greater than the maximum possible call life in Unified CVP)**

Interruptible: **Not Checked**

Step 10 Verify that the user.microapp.ToExtVXMLECC variable is set up for an array of five items with a minimum size of 60 characters and the user.microapp.FromExtVXML variable is set up for an array of four with a minimum size of 60 characters.

Note

Verify that you have at least one available route and skill group to map to the route and skillgroup in the example script.

Step 11 Save the script, then associate the call type and schedule the script.

Note For Small Contact Center Deployment Model ensure the resources used in this Routing Script, like Network VRU Scripts , ECC variables etc are specific to the sub customer.

Configure Agent Greeting

To use Agent Greeting, your phone must meet the following requirements:

- The phones must have the BiB feature.
- The phones must use the firmware version delivered with Unified CM 8.5(1) or greater.

  (In most cases phone firmware is upgraded automatically when you upgrade Unified CM installation.)

Complete the following procedures for Agent Greeting configuration:

- Configure Gateway, on page 316
- Configure Unified CVP, on page 317
- Configure Unified CCE, on page 321
- Configure Unified Communications Manager, on page 326

Configure Gateway

Republish the tcl scripts to VXML Gateway

The .tcl script files that ship with Unified CVP include updates to support Agent Greeting. You must republish these updated files to your VXML Gateway.

Republishing scripts to the VXML Gateways is a standard task in CVP upgrades. You must republish the scripts before you can use Agent Greeting.

Procedure

Step 1 In the Unified CVP Operation Console, select **Bulk Administration** > **File Transfer** > **Scripts and Media**.

Step 2 Set Device to Gateway.

Step 3 Select the gateways you want to update. Typically you would select all of them unless you have a specific reason not to.

Step 4 Select **Default Gateway Files**.

Step 5 Click **Transfer**.

Set Cache Size on VXML Gateway

To ensure adequate performance, set the size of the cache on the VXML Gateway to the maximum allowed. The maximum size is 100 megabytes; the default is 15 kilobytes. Failure to set the VXML Gateway cache to its maximum can result in slowed performance to increased traffic to the media server.

Use the following Cisco IOS commands on the VXML Gateway to reset the cache size:

```
conf t
http client cache memory pool 100000
exit
wr
```

For more information about configuring the cache size, see the *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

Configure Unified CVP

Complete the following procedures for Unified CVP configuration:

- Configure FTP Enabled in Server Manager, on page 317
- Configure Unified CVP Media Server, on page 60
- Configure the Call Studio Scripts for Record Agent Greeting, on page 319

Configure FTP Enabled in Server Manager

Complete the following procedure to configure the FTP enabled in server manager.

Procedure

Step 1 Right- Click **Roles** in the left navigation page of server manager.

Step 2 Select **Add Roles**.

Step 3 Click **Next**.

Step 4 Check the checkbox **Web Server (IIS)** and click **Next**.

Step 5 Check the checkbox **FTP Server** and click **Next**.

Step 6 After the successful installation, click **Close**.

Step 7 Make sure that the FTP and the IIS share the same root directory, because the recording application writes the file to the media server directory structure, and the greeting playback call uses IIS to fetch the file. The en-us/app directory should be under the same root directory for FTP and IIS.

Step 8 Create a dedicated directory on the server to store your greeting files.

This lets you specify a lower cache timeout of 5 minutes for your agent greeting files that does not affect other more static files you may be serving from other directories. By default, the Record Greeting application posts the .wav file to the en-us/app directory under your web/ftp root directory. You may create a dedicated directory

such as ag_gr under the en-us/app directory, and then indicate this in the Unified CCE script that invokes the recording application. Use the array for the ECC variable **call.user.microapp.ToExtVXML** to send the ftpPath parameter to the recording application. Make sure the ECC variable length is long enough, or it may get truncated and fail.

Step 9 In IIS Manager, set the cache expiration for the dedicated directory to a value that allows re-recorded greetings to replace their predecessor in a reasonable amount of time, while minimizing requests for data to the media server from the VXML Gateway.

The ideal value varies depending on the number of agents you support and how often they re-record their greetings. Two minutes may be a reasonable starting point.

Step 10 Find the site you are using, go to the agent greeting folder you created (ag_gr), and then select **HTTP Response Headers** .

Step 11 Select **Add**, then **Set Common Headers** .

Create Voice Prompts for Recording Greetings

You must create audio files for each of the voice prompts that agents hear as they record a greeting. The number of prompts you require can vary, but a typical set can consist of:

- A welcome followed by a prompt to select which greeting to work with (this assumes you support multiple greetings per agent)
- A prompt to select whether they want to hear the current version, record a new one, or return to the main menu
- A prompt to play if a current greeting is not found.

To create voice prompts for recording greetings:

Procedure

Step 1 Create the files using the recording tool of your choice. When you record your files:

- The media files must be in `.wav` format. Your `.wav` files must match Unified CVP encoding and format requirements (G.711, CCITT A-Law 8 kHz, 8 bit, mono).
- Test your audio files. Ensure that they are not clipped and that they are consistent in volume and tone.

Step 2 After recording, deploy the files to your Unified CVP media server. The default deployment location is to the `<web_server_root>\en-us\app` directory.

Step 3 Note the names of the files and the location where you deployed them on the media server. Your script authors need this information for the Agent Greeting scripts.

Built-In Recording Prompts

The Unified CVP Get Speech micro-application used to record Agent Greetings includes the following built-in prompts:

- A prompt that agents can use to play back what they recorded

- A prompt to save the greeting, record it again, or return to the main menu
- A prompt that confirms the save, with an option to end the call or return to the main menu

You can replace these `.wav` files with files of your own. For more information, see the Unified Customer Voice Portal Call Studio documentation at https://www.cisco.com/c/en/us/support/unified-communications/unified-call-studio/tsd-products-support-series-home.html.

Configure Unified CVP Media Server

Procedure

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

Step 2 Click **Add New**.

Step 3 On the **General** tab, configure the following.

a) Enter the IP address and the hostname of the Unified CVP server.
b) Check **FTP Enabled**.
c) Either Check **Anonymous Access** or enter the credentials.
d) Click **Test SignIn** to validate the FTP access.

Step 4 Click **Save**.

Step 5 Repeat Step 1 through 4 for all Media Servers.

Step 6 After you configure all Media Servers, click **Deploy**.

Step 7 Click **Deployment Status** to make sure that you applied the configuration.

Step 8 In the CVP Operations Console, navigate to **Device Management** > **Media Server**.

Step 9 Change Default Media Server from **None** to any one of the Unified CVP servers. Then click **Set**.

Step 10 Click **Deploy**.

Configure the Call Studio Scripts for Record Agent Greeting

The Record Agent Greeting is controlled by a combination of Call Studio script and ICM script. Complete the following procedure to configure the Call Studio script:

Procedure

Step 1 Access the .zip file from the CVP OAMP machine from the location `C:\Cisco\CVP\OPSConsoleServer\StudioDownloads\RecordAgentGreeting.zip`.

Step 2 Extract the example Call Studio Record Agent Greeting scripts contained in RecordAgentGreeting.zip to a folder of your choice on the computer running CallStudio. The folder contains a CallStudio project having the same name as the folder.

Step 3 Start Call Studio by selecting **Start** > **Programs** > **Cisco** > **Cisco Unified Call Studio**.

Step 4 Select **File** > **Import**.
The **Import** dialog box displays.

Step 5 Expand the **Call Studio** folder and select **Existing Call Studio** project Into Workspace.

Step 6 Click **Next**.
The Import Call Studio Project From File System displays.

Step 7 Browse to the location where you extracted the call studio projects. Select the folder and select **Finish**.

Example:

RecordAgentGreeting

Step 8 Follow the below steps, to save the file in a defined path:

a) In the **Call Studio Navigator** panel, open the **RecordAgentGreeting** project and double click **app.callflow** to display the application elements in the **script** window.
b) Select the **Record Greeting With Confirm** node.
c) In the **Element Configuration** panel, choose the **Setting** tab and modify the default path settings to `c:\inetpub\wwwroot\en-us\app\ag_gr`. Save the project after you modify it.
d) Validate the project associated with the **Record Agent Greeting** and deploy them to your VXML Server.

Step 9 Right-click on **Record Agent Greeting** project in the **Navigator** window and select **Validate**.

Step 10 Right-click on the **Record Agent Greeting** project and click **Deploy**.

Step 11 In the **Deploy Destination** area, select **Archive File** and click **Browse**.

Step 12 Navigate to the archive folder that you have set up:

Example:

`C:\Users\Administrator\Desktop\Sample`.

Step 13 Enter the name of the file.

Example:

Samplefile.zip

Step 14 Click **Save**.

Step 15 In the **Deploy Destination**area click **Finish**.

Step 16 Log in to **OAMP** and choose **Bulk Administration\File Transfer\VXMLApplications**.

Step 17 Select the **VXML Server** to which you want to deploy the applications.

Step 18 Select the zip file that contains the applications.

Example:

Samplefile.zip

Step 19 Click **Transfer**.

Step 20 Right-click on the project and click **Deploy**, then click **Finish**.

Step 21 Using windows explorer, navigate to `%CVP_HOME%\VXMLServer\applications\RecordAgentGreeting`, open the project's admin folder and double-click deployApp.bat to deploy the application to the VXML Server.

Step 22 Verify that the application is running in the following path `%CVP_HOME%\VXMLServer\applications\RecordAgentGreeting\admin` and double-click **status.bat**. The application should display under Application Name and with the status Running.

Set Content Expiration in IIS (Windows Server) in Media

Complete the following procedure to set content expiration in IIS on a Windows Server:

Procedure

Step 1 Right-click **My Computer** on the desktop and select **Manage**.

Step 2 Select **Server Manager** > **Roles** > **Web Server (IIS)** > **Internet Information Services (IIS) Manager**.

Step 3 Select the default website and navigate to **Features View**.

Step 4 Double-click **HTTP Response Headers**.

Step 5 Under **Actions**, select **Set Common Headers…**.

Step 6 On **Set Common HTTP Response Headers**, select **Enable HTTP keep-alive** and **Expire Web content** and set **After 5** minutes.

Configure Unified CCE

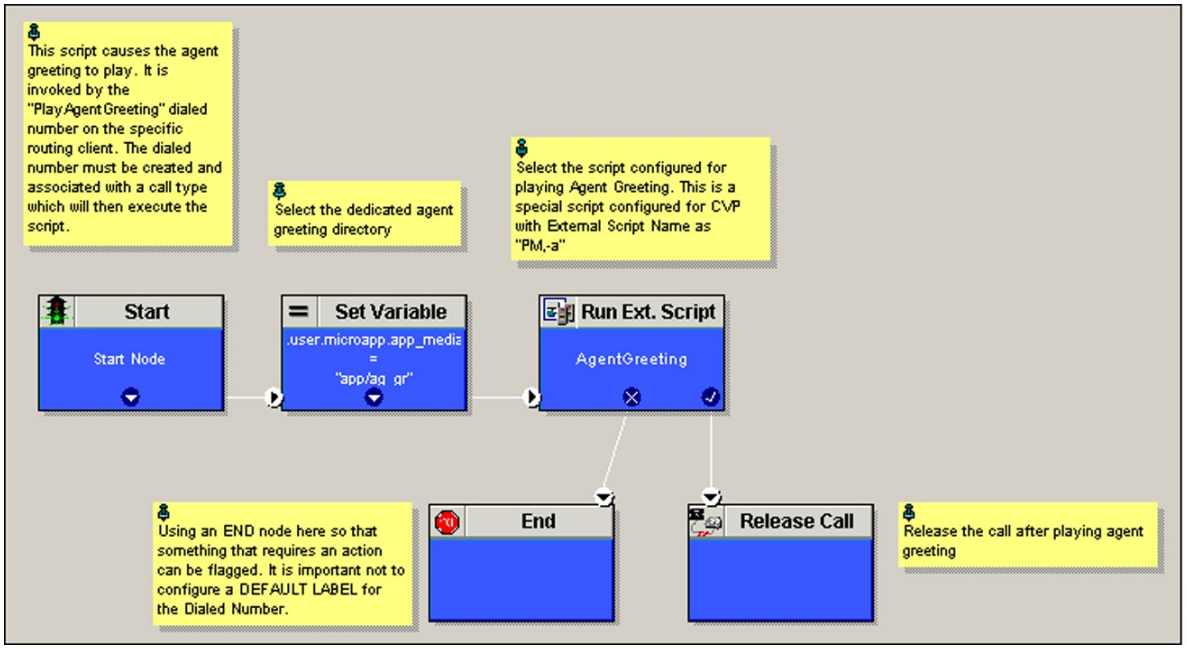
Complete the following procedures forUnified CCE configuration:

- Create Agent Greeting Play Script, on page 321
- Create Agent Greeting Recording Script, on page 322
- Import the Example Agent Greeting Scripts, on page 323

Create Agent Greeting Play Script

A dedicated routing script plays the Agent Greeting. This script is invoked by the PlayAgent Greeting dialed number on the specific routing client. You must create the dialed number and associate it with a call type that runs the script.

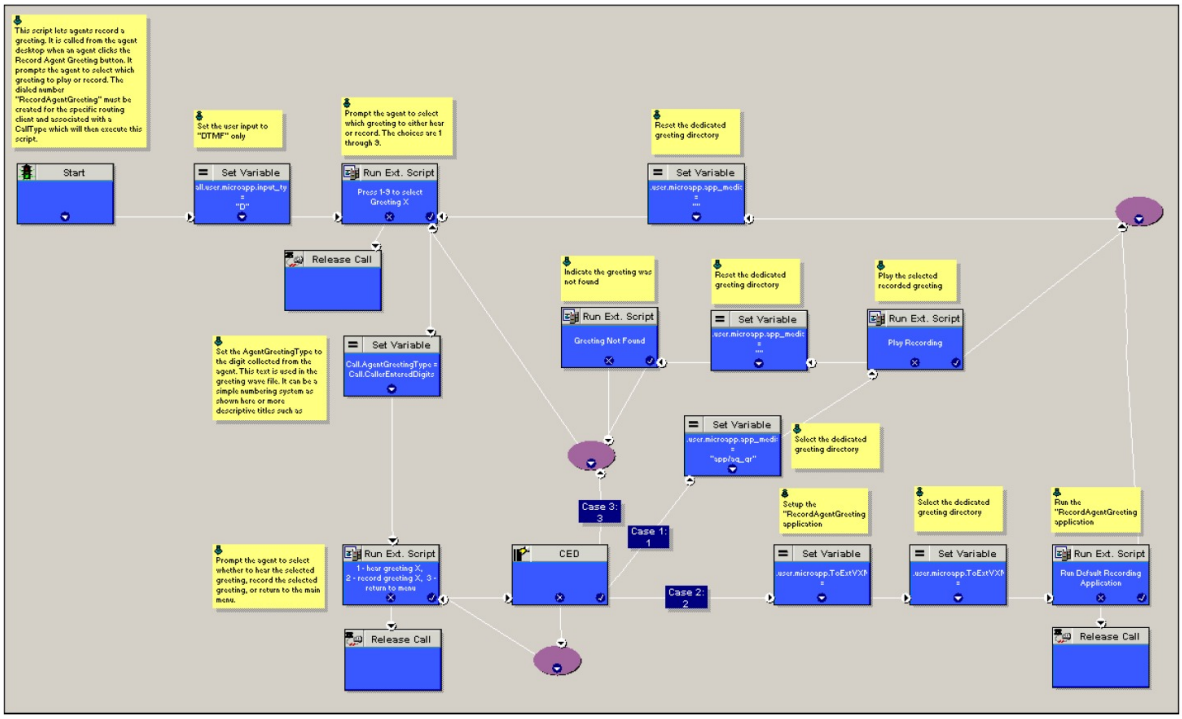
Figure 11: Agent Greeting Play Script



Create Agent Greeting Recording Script

The Agent Greeting Recording script lets agents record a greeting. The agent desktop calls the script when an agent clicks the Record Agent Greeting button, prompting the agent to select which greeting to play or record. Create the dialed number RecordAgentGreeting for the specific routing client and associate it with a call type that then runs this script.

Figure 12: Agent Greeting recording script



Unified CCE Configuration for Record Agent Greeting

- **user.microapp.ToExtVXML** : This is used twice in an Agent Greeting record script, the first time is to queue the Unified CVP Record Agent Greeting application and the second time is to tell the recording application where to save greeting files. Configure it as an array with size 3. Use the Unified CCE Administration tool to ensure this variable includes Maximum Length as 100 and Enabled.
- **user.microapp.app_media_lib** :This is required in Agent Greeting record and play scripts to specify the dedicated directory on the media server where your greeting audio files are stored. Maximum Length is 100 and Enabled.
- **user.microapp.input_type:** This is required in Agent Greeting record scripts to limit the allowable input type to DTMF. Maximum Length is 100 and Enabled.

Note For more information on how to enable the ECC variables, see the *Cisco Hosted Collaboration Solution for Contact Center Configuration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-and-configuration-guides-list.html.

Import the Example Agent Greeting Scripts

To view or use the example Agent Greeting scripts, you must first import them into theUnified CCE Script Editor. Complete the following procedure to import the example Agent Greeting scripts:

Procedure

Step 1 Launch **Script Editor**.

Step 2 Select **File**>**Import Script** and select the following scripts to import:

a) Agent Greeting Play Script

b) Agent Greeting Recording Script

The scripts will be located in the icm\bin directory on the data server (DS) node.

Step 3 Repeat for the remaining scripts.

Note For Small Contact Center Deployment Model, Default Routing Scripts are available in the partners Community. Download the Routing Scripts to the Desktop where ISE is Installed and Login as the Sub Customer User into the ISE to perform the Step 2 and 3. Download the `Routing Script files for all Deployment models` https://software.cisco.com/download/navigator.html?mdfid=284526699.

Note For Small Contact Center Deployment Model ensure the resources used in this Routing script, like Network VRU Scripts , ECC variables etc are specific to the sub customer.

Configure Call Types

Procedure

Step 1 Sign-in to **Unified CCDM Portal** as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**

Step 3 Select the folder where you want to create the call type.

Step 4 Click **Resource**, then click **Call Types**.

Step 5 Create a call type to record agent greetings and enter **RecordAgentGreeting** as the name.

Step 6 Create a call type to play agent greetings and enter **PlayAgentGreeting** as the name.

Configure Dialed Numbers

Procedure

Step 1 Sign-in to **Unified CCDM Portal** as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**

Step 3 Select the folder where you want to create the dialed number.

Step 4 Click **Resource**, then click **Dialed Number**.

Step 5 Create a dialed number to record agent greetings and enter **RecordAgentGreeting** as the name.

Step 6 Create a dialed number to play agent greetings and enter **PlayAgentGreeting** as the name.

Step 7 Complete the following for each dialed number:

a) Select **Internal Voice** for the Routing type.

b) Retain the default domain value.

c) Select the call type appropriate to the dialed number.

This helps to associate each number to its call type and to a script that runs it.

Schedule the Script

Procedure

Step 1 In the **Script Editor**, select **Script** > **Call Type Manager**.

Step 2 From the Call Type Manager screen, select the **Schedules** tab.

Step 3 From the Call type drop-down list, select the call type to associate with the script; for example, PlayAgentGreeting.

Step 4 Click **Add** and select the script you want from the Scripts box.

Step 5 Click **OK** twice to exit.

Configure Agent Greeting

This section describes how to deploy and configure the Agent Greeting feature.

Agent Greeting Deployment Tasks

Procedure

Step 1 Ensure your system meets the baseline requirements for software, hardware, and configuration described in the System Requirements and Limitations section.

Step 2 Configure IIS and FTP on Media Server.

Step 3 In Unified CVP, add media servers, configure FTP connection information, and deploy the media servers.

Step 4 Configure a Unified CVP media server, if you have not already done so. See Configure Unified CVP Media Server, on page 60.

Step 5 In Unified CVP Operations Console, republish the VXML Gateway.tcl scripts with updated Agent Greeting support. See Republish the tcl scripts to VXML Gateway, on page 316 for Agent Greeting support.

Step 6 Set the cache size on the VXML Gateway. See Set Cache Size on VXML Gateway, on page 317.

Step 7 Record the voice prompts to play to agents when they record a greeting and to deploy the audio files to your media server, see Create Voice Prompts for Recording Greetings, on page 318.

Step 8 Configure Call Types, on page 323 to record and play agent greetings.

Step 9 Configure Dialed Numbers, on page 323 to record and play agent greetings.

Step 10 Schedule the Script, on page 324

Step 11 In Script Editor:

- To use the installed scripts to record and play agent greetings, see Import the Example Agent Greeting Scripts, on page 323.

Step 12 Modify the Unified CCE call routing scripts to use Play Agent Greeting script, on page 325.

Modify the Unified CCE call routing scripts to use Play Agent Greeting script

For an Agent Greeting play script to run, you must add an AgentGreetingType Set Variable node to your existing Unified CCE call routing scripts: This variable's value is used to select the audio file to play for the greeting. Set the variable before the script node that queues the call to an agent (that is, the Queue [to Skill Group or Precision Queue], Queue Agent, Route Select, or Select node).

Specify AgentGreetingType Call Variable

To include Agent Greeting in a script, insert a Set Variable node that references the AgentGreetingType call variable. The AgentGreetingType variable causes a greeting to play and specifies the audio file it should use. The variable value corresponds to the name of the greeting type for the skill group or Precision Queue. For example, if there is a skill group or Precision Queue for Sales agents and if the greeting type for Sales is '5', then the variable value should be 5.

You can use a single greeting prompt throughout a single call type. As a result, use one AgentGreetingType set node per script. However, as needed, you can set the variable at multiple places in your scripts to allow different greetings to play for different endpoints. For example, if you do skills-based routing, you can specify the variable at each decision point used to select a particular skill group or Precision Queue.

Note Only one greeting can play per call. If a script references and sets the AgentGreetingType variable more than once in any single path through a script, the last value to be set is the one that plays.

Use these settings in the Set Variable node for Agent Greeting:

- Object Type: Call.
- Variable: Must use the AgentGreetingType variable.
- Type: Must use the PersonID_AgentGreetingType type.
- Value: Specify the value that corresponds to the greeting type you want to play. For example: “2” or “French”
  - You must enclose the value in quotes.
  - The value is not case-sensitive.
  - The value cannot include spaces or characters that require URL encoding.

Configure Unified Communications Manager

Built-in-Bridge

Built-in-Bridge (BIB) is not enabled by default for the phones. It is disabled at the system level as it is not used by all the customer by default. It is used only by the customers having Contact Center.

The provider has to perform the following procedures to enable BIB for the customers having contact center.

Note Create a new Field Display Policies at the customer level and add Built-in Bridge to the list.

- Configure the Built-in-Bridge , on page 297
- Enable or Disable the Built-in-Bridge , on page 297

Configure the Built-in-Bridge

Procedure

Step 1 Login to **Cisco Unified Communication Domain Manager** as provider.
Step 2 Navigate **Role Management** > **Field Display Policies**.
Step 3 Ensure that hierarchy is set to the appropriate customer.
Step 4 Select the **SubscriberPhoneMenuItemProvider**.
Step 5 In the details page, go to **Action** menu and click **Clone**.
Step 6 Enter **SubscriberPhoneMenuItemProvider** as the name.
Step 7 Select **relation/SubscriberPhone** from the **Target Model Type** drop-down list.
Step 8 Expand **Groups** section and enter **Phone** for Title.
Step 9 Select **builtInBridgeStatus** from the **Available** list and click **Select**.
Step 10 Click **Save**.

Enable or Disable the Built-in-Bridge

Before you begin

Ensure that you configure Built-in-Bridge. See, Configure the Built-in-Bridge , on page 297.

Procedure

Step 1 Login to **Cisco Unified Communication Domain Manager** as a provider.
Step 2 Ensure that hierarchy is set to the appropriate customer.
Step 3 Navigate **Subscriber Management** > **Phones** and select the appropriate phone.
Step 4 In the **Phone** tab:

- To enable BIB choose **On** from the **Built in Bridge** drop-down list.
- To disable BIB choose **Off** from the **Built in Bridge** drop-down list.

Step 5 Click **Save**.

Configure Whisper Announcement

Complete the following procedures for Whisper Announcement configuration:

- Configure Gateway, on page 327
- Configure Unified CVP, on page 327
- Configure Unified CCE, on page 328

Configure Gateway

Gateway uses two different dialed numbers for Whisper Announcement.

- 91919191 number calls the ring tone that the caller hears while the whisper plays to the agent
- 9191919100 number calls the whisper itself

Configure a dial peer for incoming number 9191919100 and 91919191 as follows:

```
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

Configure the Whisper Announcement Service Dialed Numbers

Unified CVP uses two different dialed numbers for Whisper Announcement:

The first number calls the ring tone service that the caller hears while the whisper plays to the agent. The Unified CVP default for this number is 91919191.

The second number calls the whisper itself. The Unified CVP default for this number is 9191919100.

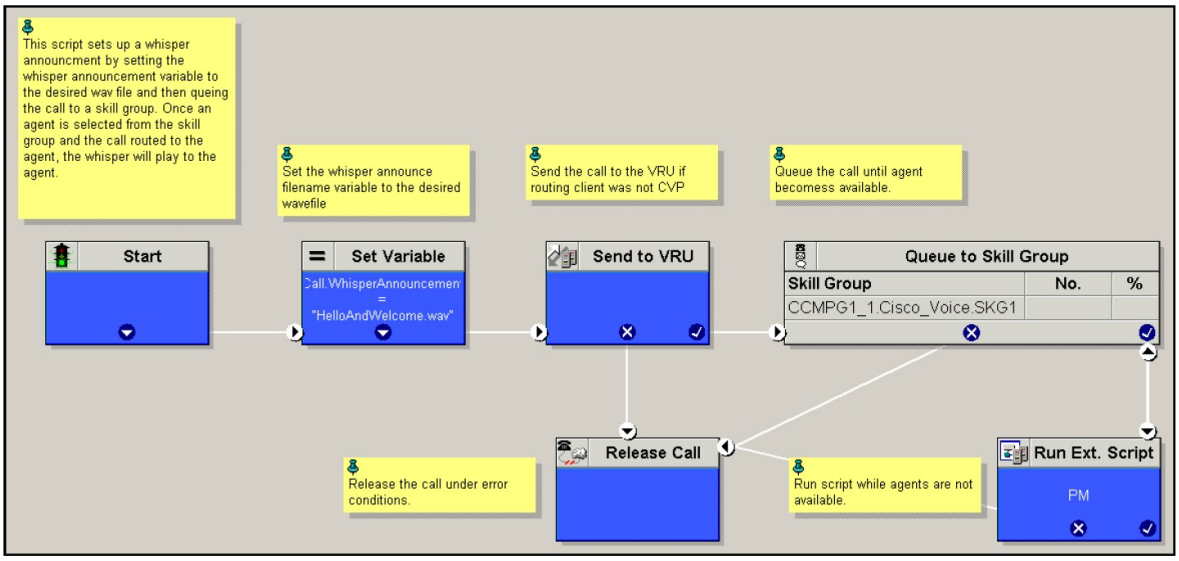
For Whisper Announcement to work, your dial number pattern must cover both of these numbers. The easiest way to ensure coverage is through the use of wild cards such as 9191*. However, if you decide to use an exact dialed number match, then you must specify both 91919191 and 9191919100.

Configure Unified CCE

Create Whisper Announcement Script

It is very important to deploy Whisper Announcement with the Call. Whisper Announcement variable and to set .wav file in your Unified CCE routing scripts.

Figure 13: Whisper Announcement Script



Configure Database Integration

Complete the following procedures for Database Integration configuration:

- Configure Unified CVP, on page 328
- Configure Unified CCE, on page 331

Note Small Contact Center deployment model supports only CVP Database Integration.

Configure Unified CVP

Configure VXML Database Element

You need to configure Java Database Connectivity (JDBC) for VXML Database Element configuration.

Complete the following procedures for JDBC configuration:

- Install JDBC driver, on page 329
- Add JNDI Context, on page 329

- Configure VXML Studio Script, on page 330
- Create ICM Script, on page 330

Install JDBC driver

Complete the following procedure to install the JDBC driver:

Procedure

Step 1 Download the .exe file for Microsoft JDBC Driver for SQL Server

Example:

```
1033\sqljdbc_3.0.1301.101_enu.exe
```

Step 2 Run the executable and install the .exe file in the location `C:\temp\`

Step 3 Copy the file `C:\temp\sqljdbc_3.0\enu\sqljdbc4.jar` to the Unified CVP VXML servers' folder `C:\Cisco\CVP\VXMLServer\Tomcat\common\lib`

Add JNDI Context

Complete the following procedure to add the Java Naming and Directory Interface (JNDI) context configuration:

Procedure

Step 1 Go to the context.xml file located at C:\Cisco\CVP\VXMLServer\Tomcat\conf\context.xml file.

Step 2 Enter the JNDI name, SQL server address, SQL database name, username and password.

The following is an example of the SQL authentication context.xml file:

```
<Context>

<WatchedResource>WEB-INF/web.xml</WatchedResource>

<Manager pathname="" />

<Resource name="jdbc/dblookup"

auth="Container"

type="javax.sql.DataSource"

DriverClassName="com.microsoft.sqlserver.jdbc.SQLServerDriver"

url="jdbc:sqlserver://<dblookupnode_ipaddress>:1433;databaseName=DBLookup;user=sa;password=sa"

>

</Context>
```

Step 3 Perform following steps to restart VXML server services:

a) Goto **Run** window and enter `services.msc` command.
b) Select **Cisco CVP VXML Server** option.
c) Right-click and select **Restart** option.

Note For small contact center agent deployment model , Resource name should be unique for each sub-customers. For example, Sub-cust1 Resource name = "jdbc/dblookup1" and Sub-cust2 Resource name = "jdbc/dblookup2".

Configure VXML Studio Script

Complete the following procedure to configure the VXML studio script:

Procedure

Step 1 Configure the following to create the VXML application with the database element.

a) Select **single** under **Type**.
b) Enter the database lookup name in **JNDI Name**.
c) Query SQL:

```
For example, select AccountNo from AccountInfo where CustomerNo = {CallData.ANI}

Where AccountNo - Value to be retrieved

AccountInfo - Table name

CustomerNo - condition to be queried

Data:

Create a database element with the following values:

Name - AccountNo

Value - {Data.Element.Database_01.AccountNo}
```

Step 2 Deploy the script to the local computer or to the remote computer (VXML call server directly) to create CVP Subdialog return element.

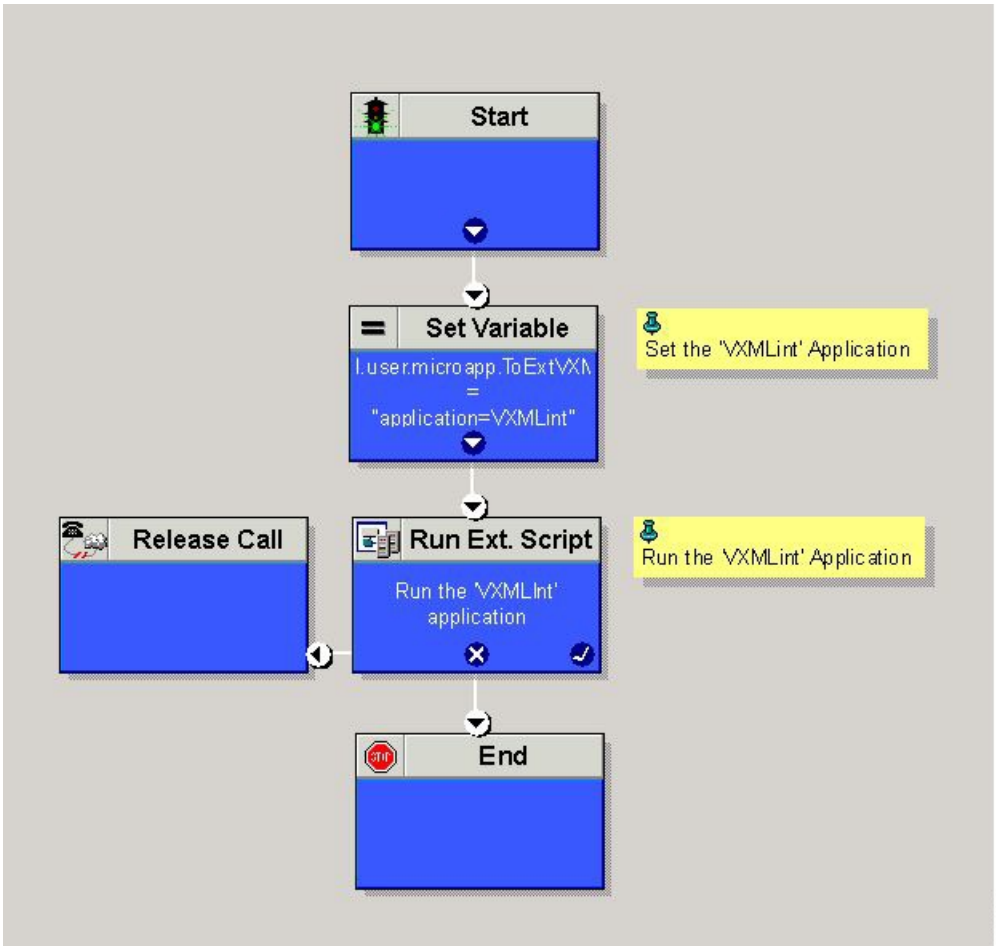
Step 3 If you saved this to the local machine, copy the whole folder to the following location:

<Install dir>:\Cisco\CVP\VXMLServer\applications and deploy it using deployApp windows batch file located inside the admin folder of applications.

Create ICM Script

Create an ICM script similar to the one shown in the following figure:

Figure 14: Sample Script with ICM database Lookup



Configure Unified CCE

Configure ICM Database Lookup

Complete the following procedure to configure ICM Database Lookup.

Procedure

Step 1 Select **Enable Database Routing** in **Router options** to edit Router setup for database lookup changes.

Step 2 Configure Database Lookup explorer:

a) Click **Start** > **All programs** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

b) Open **Tools** > **Explorer Tools** > **Database Lookup Explorer.**

c) Configure Script Table and Script Table Column as shown in the following example:

Script Table:

```
Name: AccountInfo

Side A: \\dblookup1\DBLookup.AccountInfo

Side B: <Update Side B of database here>

Description: <Provide description here>
```

dblookup1 is external database server name, DBLookup is external database name, and AccountInfo is the table name.

Script Table Column:

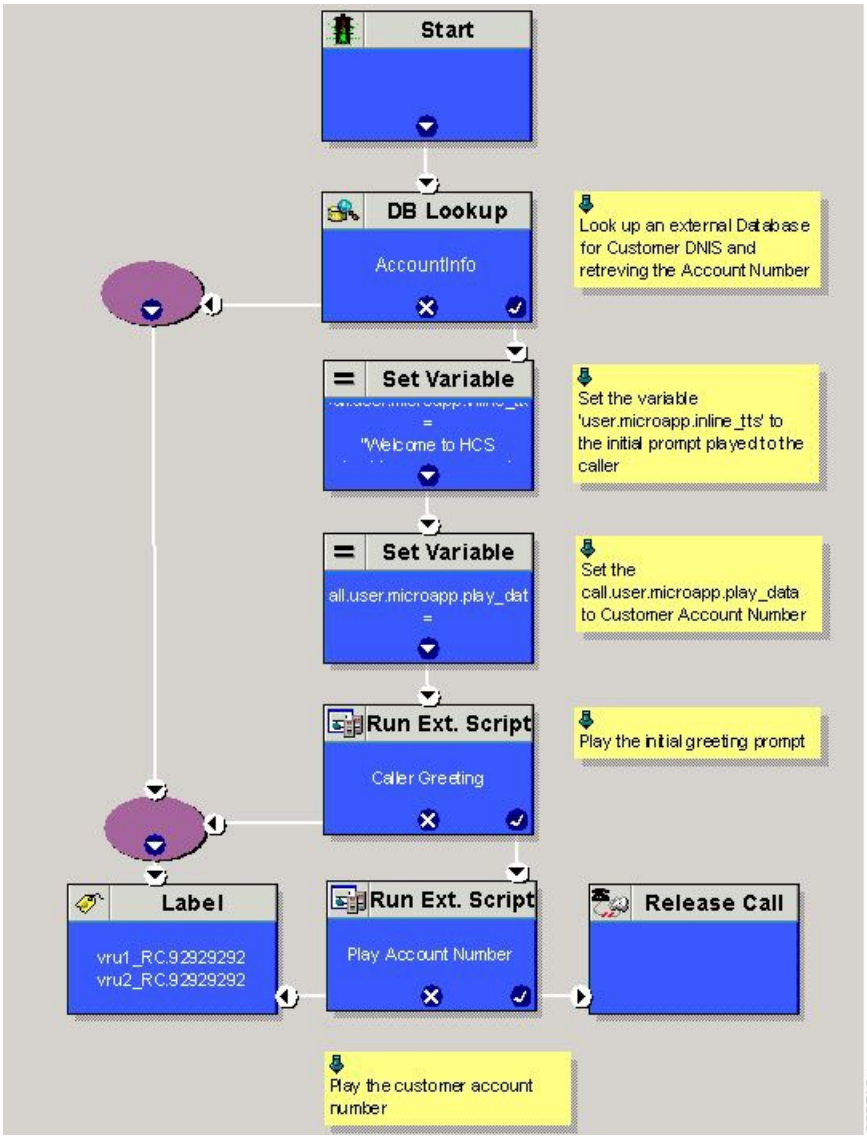
```
Column name: AccountNo

Description: <Provide description here>
```

Step 3 Use the CCEDataProtect Tool to configure the registry settings in Unified CCE. For more information, see **Configure External DBLookUp Registry Value using CCEDataProtect Tool** procedure in the *Administration Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html

Step 4 Create the ICM script with the database lookup node with the respective table and lookup value.

The following figure shows AccountInfo as the table name and Call.CallingLineID as the lookup value.

Figure 15: Example ICM Database Look Up



Configure Unified Mobile Agent

Configure Gateway for SCC Deployment with VRF

Configure Dial Peer for Sub-Customer1 CUCM

```
dial-peer voice 21011 voip
description from CVP towards VRF1 to Sub-Customer1 for mobileagent
destination-pattern 100.
session protocol sipv2
session target ipv4:20.20.20.31
session transport udp
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.100
voice-class sip bind media source-interface GigabitEthernet2.100
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```

Configure Dial Peer for Sub-Customer2 CUCM

```
dial-peer voice 22011 voip
description from CVP towards VRF2 to Sub-Customer2 for mobileagent
destination-pattern 300.
session protocol sipv2
session target ipv4:20.20.20.31
session transport udp
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.200
voice-class sip bind media source-interface GigabitEthernet2.200
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```

Configure Unified CCE

Complete the following procedure to configure Mobile Agent in Unified CCE:

Procedure

Step 1 Sign-in to **Unified CCDM Portal** as Tenant or Sub Customer user.

Step 2 Click the burger icon and select **Provisioning** > **Resource Manager**

Step 3 Select the folder where you want to create the agent desktop.

Step 4 Click **Resource**, then click **Agent Desktop**.

Step 5 Enter unique name of up to 32 characters for the record.

This name can use alphanumeric characters, periods, and underscores.

Step 6 Enter the mandatory fields such as **Incoming Work mode**, **Outgoing Work mode**, **Wrap-up time**, and other required fields.

Step 7 Click **Save**.

Enable Mobile Agent Option in CTI OS Server

Complete the following procedure to enable Mobile Agent option in CTI OS server:

Procedure

Step 1 Invoke the CTI OS Server setup.

Step 2 In **Peripheral Identifier** window, check **Enable Mobile Agent** check box, and select **Mobile Agent Mode** from the drop-down list.

Step 3 Repeat the above steps on both sides of CTI OS server.

Configure Unified Communications Manager

Perform the following to configure unified communications manager:

- Configure CTI Port, on page 335
- Tag CTI Ports as Contact Center Agent Lines, on page 337

Configure CTI Port

Ensure that directory numbers are added. See Add Directory Number Inventory, on page 290.

Unified Mobile Agent needs two configured CTI Port pools on Unified Communications Domain Manager:

- A local CTI port as the agent's virtual extension
- A network CTI port to initiate a call to the Mobile Agent's phone

Note For 12000 agent deployment model, add CTI ports for all three Unified CM clusters.

Complete the following procedure to configure CTI port:

- Configure CTI Port as Provider or Reseller, on page 335
- Configure CTI Port as Customer, on page 336

Configure CTI Port as Provider or Reseller

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider or reseller.

Step 2 Ensure that hierarchy is set to appropriate site

Step 3 Navigate to **Subscriber Management** > **Phones**.

Step 4 Click **Add**.

Step 5 In **Phones** tab:

a) Enter Local CTI Port pool name in **Device Name** field, in *LCPxxxxFyyyy* format.

- LCP - identifies the CTI port as a local device
- xxxx - is the peripheral ID of the Unified Communication Manager PIM
- yyyy - is the local CTI Port

b) Choose **CTI Port** from **Product Type** drop-down list.
c) Choose **Calling Search Space** from the drop-down list.
d) Choose **Device Pool** from the drop-down list.
e) Choose **Location** from the drop-down list.

Step 6 Goto **Lines** tab:

a) Click **Add** icon in **Lines** panel.
b) Choose directory number from **Pattern** drop-down list, in **Drin** Panel.
c) Choose **Route Partition Name** from drop-down list.

Step 7 Click **Save**.

What to do next

Repeat the above steps to create Network CTI port. Enter Network CTI Port pool name in **Device Name** field, in *RCPxxxxFyyyy* format.

- RCP - identifies the CTI port as a network device
- xxxx - is the peripheral ID of the Unified Communication Manager PIM
- yyyy - is the network CTI Port

Note Local CTI port and Network CTI port should be same

Configure CTI Port as Customer

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as Customer admin.
Step 2 Ensure that hierarchy is set to appropriate site
Step 3 Navigate to **Subscriber Management** > **Phones**.
Step 4 Click **Add**.
Step 5 In **Basic Information** tab:

a) Choose **CTI Port** from **Product Type** drop-down list.
b) Enter Local CTI Port pool name in **Device Name** field, in *LCPxxxxFyyyy* format.

- LCP - identifies the CTI port as a local device

- xxxx - is peripheral ID of the Unified Communication Manager PIM
- yyyy - is the local CTI Port

c) Choose **Calling Search Space** from the drop-down list.

Step 6 Goto **Advanced Infromation** tab:

a) Choose **Device Pool** from the drop-down list.
b) Choose **Location** from the drop-down list.

Step 7 Goto **Lines** tab:

a) Click **Add** icon in **Lines** panel.
b) Choose directory number from **Pattern** drop-down list, in **Drin** Panel.
c) Choose **Route Partition Name** from drop-down list.

Step 8 Click **Save**.

What to do next

Repeat the above steps to create Network CTI port. Enter Network CTI Port pool name in **Device Name** field, in *RCPxxxxFyyyy* format.

- RCP - identifies the CTI port as a network device
- xxxx - is the peripheral ID of the Unified Communication Manager PIM
- yyyy - is the network CTI Port

Note Local CTI port and Network CTI port should be same

Tag CTI Ports as Contact Center Agent Lines

Before you begin

Ensure CTI ports are added. See, Configure CTI Port, on page 335

Note For 12000 agent deployment model, the CTI port for all three CUCM clusters should be tagged.

Perform the below steps for both LCP and RCP CTI ports:

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer.
Step 2 Ensure that hierarchy is set to appropriate level.
Step 3 Navigate **Subscribe Management** > **Agent Lines**

Step 4 Click **Add**.

Step 5 Choose **Phones** from **Device Types** drop-down list.

Step 6 Choose **CTI Ports** from **Device Name** drop-down list.

Step 7 Choose **Line** from the drop-down list.

Step 8 Choose **Application User** from drop-down list.

Step 9 Click **Save**.

Configure Outbound Dialer

Complete the following procedure to configure Outbound Dialer:

- Configure Gateway, on page 338
- Configure Unified CVP, on page 340
- Configure Unified CCE, on page 340
- Configure Unified Communications Manager, on page 354

Configure Gateway

Note
- In small contact center agent deployment model customer can choose a dedicated or a shared outbound gateway. If it is shared gateway there should be a PSTN connectivity.
- Outbound Dialer do not support A-law, it is not instructed to configure the A-law under inbound dial-peer in the voice gateway.

Follow the below procedure to configure gateway/CUBE(E):

Procedure

Step 1 Create a voice encapsulation type with following voip parameters

Example:

```
voice service voip
     no ip address trusted authenticate
     mode border-element
     allow-connections sip to sip
     no supplementary-service sip refer
     supplementary-service media-renegotiate
     redirect ip2ip
     signaling forward none
sip
     header-passing
     error-passthru
     asymmetric payload full
     options-ping 60
```

```
     midcall-signaling passthru
     !
```

Step 2 Default, CPA is enabled for gateway/CUBE(E). Otherwise, enable CPA for CUBE(E).

Example:

```
voice service voip
 cpa
```

Step 3 Create a voice codec class

Example:

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

Step 4 Create dial peer configuration to reach the customer PSTN number.

Example:

```
dial-peer voice 978100 voip
     session protocol sipv2
     incoming called-number <Customer Phone Number Pattern>
     voice-class codec 1
     voice-class sip rel1xx supported "100rel"
     dtmf-relay rtp-nte sip-kpml
     no vad

dial-peer voice 97810 pots
     destination-pattern 97810[1-9]
     port 1/0:23
     forward-digits all
     progress_ind alert enable 8
```

Step 5 Create dial peer configuration to reach the agent extension (VOIP)

Example:

```
dial-peer voice 40000 voip
     description ***To CUCM Agent Extension***
     destination-pattern <Agent Extension Pattern to CUCM>
     session protocol sipv2
     session target ipv4:<CUCM IP Address>
     voice-class codec<Codec Preference number>
     voice-class sip rel1xx supported "100rel"
     dtmf-relay rtp-nte
     no vad
     !
```

Note In 12000 agent deployment model dial peer needs to be created for all 3 CUCM clusters.

Step 6 Create dial peer configuration to reach CVP

Example:

```
dial-peer voice 99995 voip
     description ******To CVP for IVR OB*****
     destination-pattern 9999500T
     session protocol sipv2
     session target ipv4:10.10.10.10
     codec g711ulaw
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte h245-signal h245-alphanumeric
     no vad
```

```
!
!
```

Note

Step 7 Configure Transcoding Profile for CUBE E:

Example:

```
dspfarm profile 4 transcode universal
     codec g729r8
     codec g711ulaw
     codec g711alaw
     codec g729ar8
     codec g729abr8
     maximum sessions 250
     associate application CUBE
     !
```

Configure Unified CVP

Add Outbound Configuration to an Existing Unified CVP Call Server

Complete the following procedure to add Outbound configuration to an existing Unified CVP Call Server.

Procedure

Step 1 Go to Unified CVP OAMP server and login to Operations console page.

Step 2 Click the **Device Management** tab and open Unified CVP Call Server from the menu.

Step 3 Open a Call Server and click the **ICM** tab and add DNIS.

DNIS number should match with the label configured in the Network VRU Explorer for Outbound in Unified CCE.

Step 4 Click **Save** and deploy.

Step 5 Repeat step 3 for each CVP Call Server.

Configure Unified CCE

- Add Outbound Option Database Using ICMDBA Tool, on page 341
- Configure the Logger for Outbound Option, on page 341
- Configure Outbound Dialer, on page 342
- Create Outbound PIM, on page 343
- Configure SIP Outbound, on page 343
- Install SIP Dialer Using Peripheral Gateway Setup, on page 351

• Add DNP Host File, on page 353
• Outbound Option Enterprise Data, on page 353

Add Outbound Option Database Using ICMDBA Tool

Note
- For 2000, 4000 agent deployment models and small contact center, perform the configurations on Unified CCE Rogger.
- For 12000 agent deployment model, perform the configurations on Unified CCE Logger.

Procedure

Step 1 Select **Start** > **All Programs** > **Cisco Unified CCE Tools** > **ICMdba**. Click **Yes** at the warnings.

Step 2 Navigate to **Server** > **Instance** > **Logger**. Right-click on the logger that is installed and select **Create** to create the Outbound Option database.

Step 3 In the **Create Database** dialog box, click **Add** to open the Add Device dialog box. Click **Data**. Select the E drive. Leave the DB size with default value and click **OK** to return to the Create Database dialog box.

Step 4 In the **Add Device** dialog box, Click **Log**. Select the E drive. Leave the log size field with default value. Click **OK** to return to the Create Database dialog box.

Step 5 In the **Create Database** dialog box, click **Create**, then click **Start**. When you see the successful creation message, click **OK**, then click **Close**.

Configure the Logger for Outbound Option

Use this procedure to configure the Logger for Outbound Option.

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.

Perform the following procedure on both the Side A and Side B Loggers to configure Outbound Option or Outbound Option High Availability. Both Logger machines must be up and operational.

Important Before you configure the Logger for Outbound Option High Availability:
- Confirm that an Outbound Option database exists on Logger Side A and Logger Side B.

Procedure

Step 1 Open the Web Setup tool.

Step 2 Choose **Component Management** > **Loggers**.

Step 3 Choose the Logger that you want to configure, and click **Edit**.

Step 4 Click **Next** twice.

Step 5 On the Additional Options page, click the **Enable Outbound Option** check box.

Step 6 Click the **Enable High Availability** check box to enable Outbound Option High Availability on the Logger. Checking this check box enables 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 have enabled 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 7 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 8 If you enable High Availability, enter the **Active Directory Account Name** that the opposite side Logger runs under or a security group that includes that account.

Note While using Outbound Option High Availability, if you want to change the **Logger Public Interface** or **Active Directory Account Name**, you must disable Outbound Option High Availability using logger setup. Only after disabling Outbound Option HA, change the **Logger Public Interfaces** or **Active Directory Account Name**, then re-enable Outbound Option High Availability to update the new **Logger Public Interface** or **Active Directory Account Name**.

Step 9 Select the **Syslog** box to enable the Syslog event feed process (cw2kfeed.exe).

Note The event feed is processed and sent to the Syslog collector only if the Syslog collector is configured. For more information about the Syslog event feed process, 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.

Step 10 Click **Next**.

Step 11 Review the Summary page, and click **Finish**.

Configure Outbound Dialer

Procedure

Step 1 On the Unified CCE Admin Workstation Server, navigate to **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 In the **Configuration Manager** window, select **Outbound** > **Dialer**.

Step 3 For Small Contact Center, click **Retrieve** > **Add** and configure:

a) Enter the Dialer name.
b) Enter the ICM Peripheral Name.
c) Enter Hangup Delay (1-10) value as `1`.

d) Enter Port Throttle value as `10`.
e) Click **Save**.

Step 4 Click the **Port Map Selection** tab to display the port map configuration.

Step 5 Click **Add** to configure a set of ports and their associated extensions.

Step 6 Click **OK**.

Step 7 Click **Save**, then click **Close**.

Note For different sub customers, the port and extension range can be same, because each sub customer has separate dialer.

Create Outbound PIM

Configure Media Routing Peripheral Gateway, then add Outbound PIM. For more information, see Configure MR Peripheral Gateway, on page 41.

Configure SIP Outbound

Add Import Rule

Procedure

Step 1 Goto **Unified CCE AW-HDS-DDS** machine.

Step 2 Navigate to **Configuration Manager** > **Outbound Option** > **Import Rule** and click **Retrieve**.

Step 3 Click **Add**.

Step 4 In **Import Rule General** tab:

a) Enter **Import Name**.
b) Choose **Import Type** from the drop-down list.
c) Enter **Target Table Name**.
d) Browse **Import File Path**.

Note
- For the import type **Contact**, browse the Contact Import file. See, Create Contact Import File, on page 349
- For the import type **Do Not Call**, browse the Do Not Call List file. See, Create Do Not Call List, on page 350

e) Choose **Comma Delimited** option from **Import Data Type** panel.
f) Check **Overwrite** Table check box.

Note During Campaign, do not use both **Import File Path** and **Overwrite** option. Otherwise, dialer becomes unavailable to access records.

Step 5 Goto **Definition** tab:
a) Click **Add**.
b) Choose **Standard Column Type** from the drop-down list and retain the default values for remaining fields.

Step 6 Click **Save**.

Import Rule Deletion

When you delete an import rule, the corresponding contact table is deleted.

If you are using Outbound Option High Availability and either Side A or Side B is down when the rule is deleted, the corresponding table on that side is not deleted. However, when the side restarts, the table is then automatically deleted.

Add Query Rule

Before you begin

One or more Import rules must be defined. See Add Import Rule, on page 343

Procedure

Step 1 Goto **Unified CCE AW-HDS-DDS** machine.
Step 2 Navigate to **Configuration Manager** > **Outbound Option** > **Query Rule** and click **Retrieve**.
Step 3 Click **Add**.
Step 4 Enter **Query Rule Name**.
Step 5 Choose **Import Rule** from the drop-down list.
Step 6 Enter **Rule Clause**.
Step 7 Click **Save**.

What to do next

1. Goto **Configuration Manager** > **Tools** > **List Tools** > **Call Tye List** and add two call types; one for agent-based and another for IVR-based campaigns.

2. Goto **Configuration Manager** > **Tools** > **List Tools** > **Dialed Number / Script Selector List** and add two dialed numbers under Media routing domain. Map the dial numbers with the call types created in the previous step (one dial number for each call type).
3. Goto **Configuration Manager** > **Tools** > **Explorer Tools** > **Skill Group Explorer** and add a skill group under the call manger peripheral. Add a route for this skill group.
4. Goto **Configuration Manager** > **Tools** > **Explorer Tools** > **Agent Explorer** and add an agent. Associate the agent with the skill group created in the previous step.

Delete a Query Rule

When you delete a query rule, the corresponding Dialing List table is also deleted.

If you are using Outbound Option High Availability and either Side A or Side B is down when the rule is deleted, the corresponding table on that side is not deleted. However, when the side restarts, the table is then automatically deleted.

Add Campaign

- -
- -

Add IVR Based Campaign

Procedure

Step 1 Goto **Unified CCE AW-HDS-DDS** machine.

Step 2 Navigate to **Configuration Manager** > **Outbound Option** > **Campaign** and click **Retrieve**.

Step 3 Click **Add**.

Step 4 Enter **Campaign Name**.

Step 5 Goto **Campaign Purpose** tab:

a) Choose **Tranfer to IVR Campaign** option.
b) Check **Enable IP AMD** check box.
c) Choose **Transfer to IVR Route Point** option.

Step 6 Goto **Query Rule Selection** tab and click **Add**:

a) Choose **Query Rule Name** from the drop-down list and click **OK**.

Step 7 Goto **Skill Group Selection** tab:

a) Choose appropriate CUCM PG from **Peripheral** drop-down list, click **Retrieve**.
b) Choose **Skill Group** from the drop-down list.
c) Enter **Overflow Agents per Skill** value.
d) Enter **Dialed number**.
e) Enter **Records to cache** value.
f) Enter **Number of IVR Ports**.
g) Click **OK**.

Step 8 Goto **Call Target** tab, choose **Daylight Savings Zone** from the drop-down list.

Step 9 Click **Save**.

Add Agent Based Campaign

Procedure

Step 1

Step 2 Navigate to **Configuration Manager** > **Outbound Option** > **Campaign** and click **Retrieve**.

Step 3 Click **Add**.

Step 4 Enter **Campaign Name**.

Step 5 Goto **Campaign Purpose** tab:

a) Choose **Agent Based Campaign** option.
b) Check **Enable IP AMD** check box.
c) Choose **Transfer to Agent** option.

Step 6 Goto **Query Rule Selection** tab and click **Add**:

a) Choose **Query Rule Name** from the drop-down list and click **OK**.

Step 7 Goto **Skill Group Selection** tab:

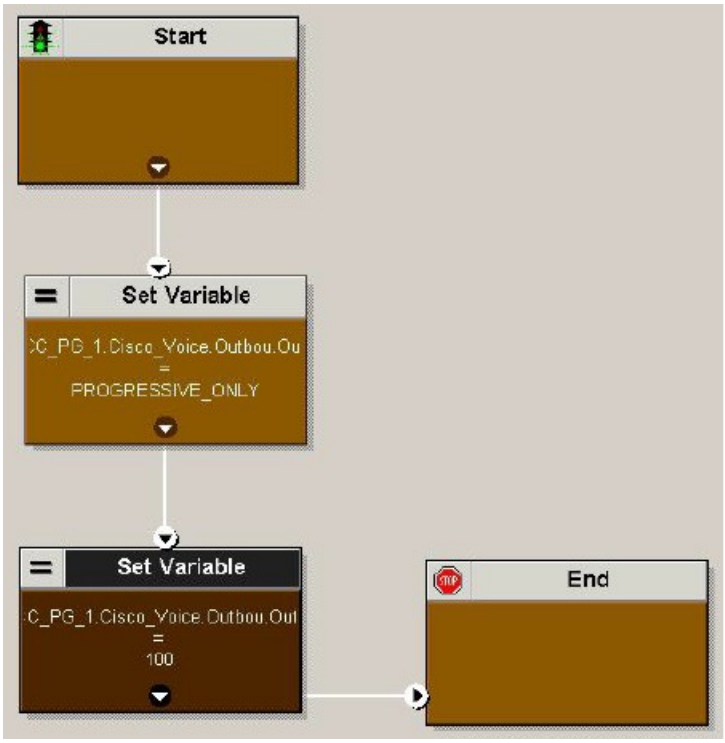
a) Choose appropriate CUCM PG from **Peripheral** drop-down list, click **Retrieve**.
b) Choose **Skill Group** from the drop-down list.
c) Enter **Overflow Agents per Skill** value.
d) Enter **Dialed number**.
e) Enter **Records to cache** value.
f) Enter **Number of IVR Ports**.
g) Click **OK**.

Step 8 Goto **Call Target** tab, choose **Daylight Savings Zone** from the drop-down list.

Step 9 Click **Save**.

Create Admin Script

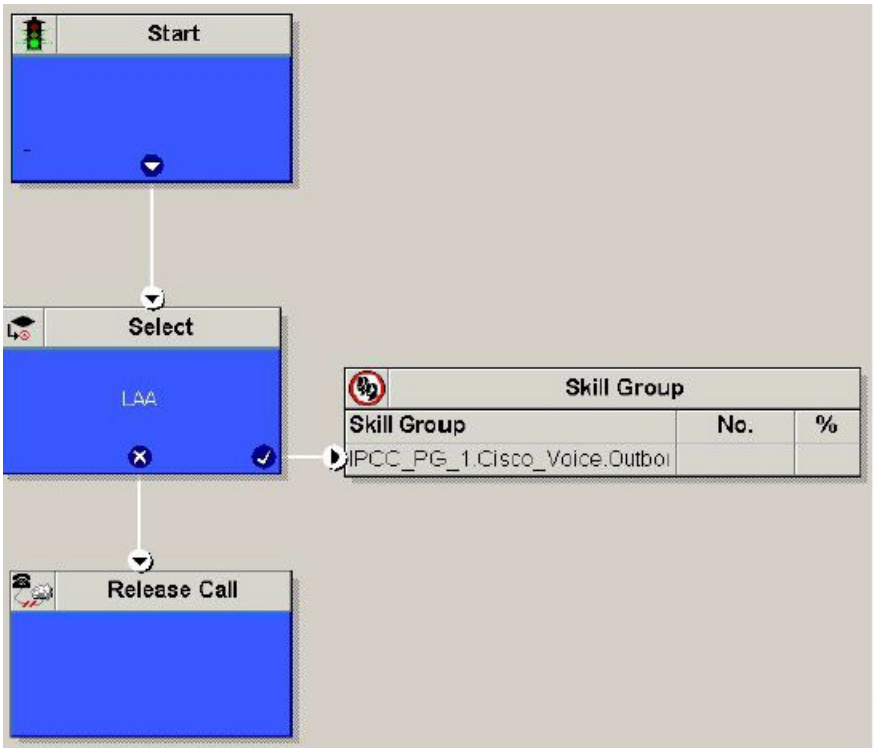
Figure 16: Create Admin Script



For more information, see Outbound Option Guide.

Add Routing Script for Agent Based Campaign

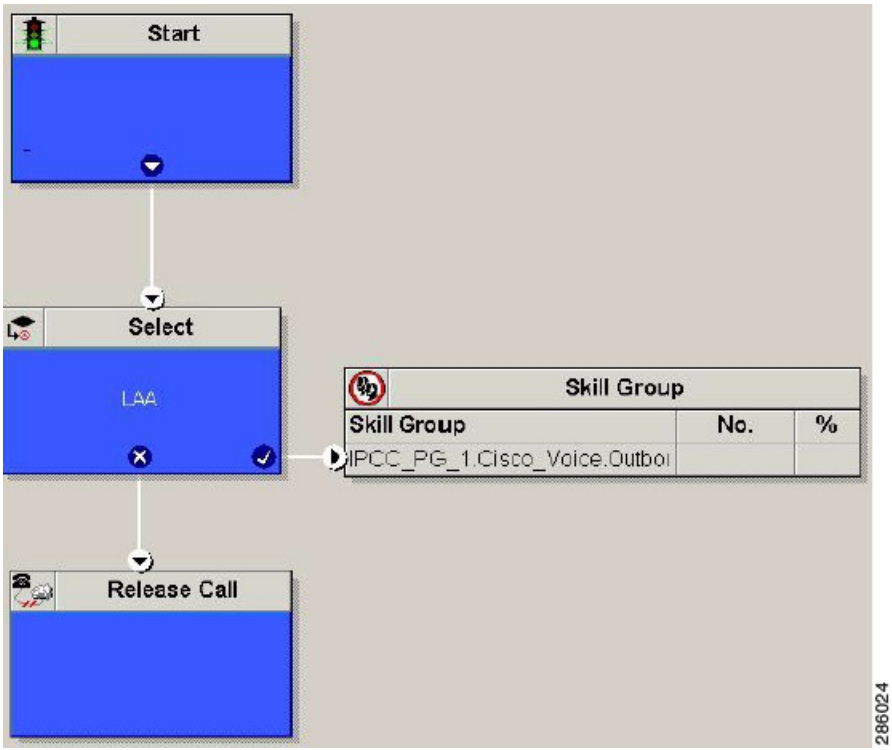
Figure 17: Add Routing Script for Agent Based Campaign



For more information, see Outbound Option Guide.

Add Routing Script for IVR Based Campaign

Figure 18: Add Routing Script for IVR Based Campaign



Configure the following for IVR based campaign:

Procedure

Step 1 Open Network VRU Explorer Tool from Configuration Manager tool. Add a label (label should match with the DNIS value configured in CVP call server) to the existing Network VRU of type 10 and select Media Routing type as "Outbound" from drop down list.

Step 2 Add the IVR based campaign.

What to do next

- Create Contact Import File, on page 349
- Create Do Not Call List, on page 350

Related Topics

Add IVR Based Campaign, on page 345

Create Contact Import File

When creating a contact import file, observe the format you designed according to the database rules set up in Import Rule Definition Tab Page.

The following example assumes that you have contact information with AccountNumber, FirstName, LastName, and Phone column types.

Procedure

Step 1 Using a text editor, create a text file that contains the information for these fields.

Step 2 Enter an account number, first name, last name, and phone number for each entry on a new line.

Use either Comma Delimited, Pipe Delimited, or Fixed Format, as defined on the Import Rule General Tab Page.

Step 3 Save the text file to the local server.

Example

The following is an example of a contact import file in the comma-delimited format:

```
6782,Henry,Martin,2225554444
3456,Michele,Smith,2225559999
4569,Walker,Evans,2225552000
```

The following is the same example in Fixed Format with the following column definitions:

- Custom - VARCHAR(4)
- FirstName - VARCHAR(10)
- LastName - VARCHAR(20)
- Phone - VARCHAR(20)

```
6782Henry     Martin              2225554444
3456Michele   Smith               2225559999
4569Walker    Evans               2225552000
```

Create Do Not Call List

When creating a Do_Not_Call list file, format it correctly using the following instructions.

Procedure

Step 1 Using a text editor, create a text file that contains all the do-not-call phone numbers.

Step 2 Enter a phone number for each Do Not Call entry on a new line.

Step 3 Observe the following characteristics for each Do Not Call entry:

- Each phone number can be a maximum of 20 characters long.
-

Step 4 Save the text file to the local server.

The following is an example of a Do_Not_Call list:

```
2225554444

2225556666

2225559999
```

To add a customer to this list, import a Do Not Call list.

The Campaign Manager reads from the Do_Not_Call table. Dialing List entries are marked as Do Not Call entries only when the Campaign Manager fetches the Dialing List entry *and only when there is an exact, digit-for-digit match*. This allows Do Not Call imports to happen while a Campaign is running without rebuilding the Dialing List.

Note If the Dialing List includes a base number plus extension, this entry must match a Do Not Call entry for that same base number and same extension. The dialer will not dial the extension.

Note To clear the Do Not Call list, import a blank file with the Overwrite table option enabled.

Install SIP Dialer Using Peripheral Gateway Setup

Procedure

Step 1 Stop all ICM Services.

Step 2 On the Unified CCE PG Side A and Side B, run Peripheral Gateway Setup. Select **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Peripheral Gateway Setup**.

Step 3 In the **Cisco Unified ICM/Contact Center Enterprise & Hosted Components Setup** dialog, select an instance from the left column under **Instances**.

Step 4 Click **Add** in the **Instance Components** section.

The **ICM Component Selection** dialog opens.

Step 5 Click **Outbound Option Dialer**.

The **Outbound Option Dialer Properties** dialog opens.

Step 6 Check **Production mode** and **Auto start at system startup**, unless your Unified ICM support provider specifically tells you otherwise. These options set the Dialer Service startup type to Automatic, so the dialer starts automatically when the machine starts up.

The **SIP (Session Initiation Protocol)** Dialer Type is automatically selected.

Step 7 Click **Next**.

Step 8 On the **Outbound Option Dialer Properties** dialog, specify the following information:

- **Outbound Option server**—The hostname or IP address of the Outbound Option server in Unified CCE. This server is typically the same VM where the Outbound Option Campaign Manager (Dataserver Side A) is located.
- **Campaign Manager server A**—If the Campaign Manager is set up as duplex, enter the hostname or IP address of the machine where the Side A Campaign Manager is located. If the Campaign Manager is set up as simplex, enter the same hostname or IP address in this field and the **Campaign Manager server B** field. You must supply a value in this field.
- **Campaign Manager server B**—If the Campaign Manager is set up as duplex, enter the hostname or IP address of the machine where the Side B Campaign Manager is located. If the Campaign Manager is set up as simplex, enter the same hostname or IP address in this field and the **Campaign Manager server A** field. You must supply a value in this field.
- **Enable Secured Connection**— Allows you to establish secured connection between the following:
  - CTI server and dialer
  - MR PIM and dialer

  Check the **Enable Secured Connection** check box to enable secured connection.

  Note If you check the **Enable Secured Connection** check box, secured connection is established between the dialer and the servers, such as MR PIM and CTI server.

  Note Before you enable secured connection between the components, ensure to complete the security certificate management process.

  For more information, see 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.
- **CTI server A**—The hostname or IP address of the VM with CTI server Side A. This server is typically the same VM where the PG is located (Call Server Side A).
- **CTI server port A**—The port number that the dialer uses to create an interface with CTI server Side A. The default is 42027 for non-secured connection and 42030 for secured connection. Make sure the CTI server port matches with the CG configuration. Locate the CTI OS Server port number by running the **Diagnostic Framework Portico** page from the call server machine, and selecting **ListProcesses**.
- **CTI server B**—The hostname or IP address of the VM with CTI server Side B.
- **CTI server port B**—The port number that the dialer uses to create an interface with CTI server Side B. The default is 43027 for non-secured connection and 43030 for secured connection.
- **Heart beat**—The interval between dialer checks for the connection to the CTI server, in milliseconds. The default value is 500.
- **Media routing port**—The port number that the dialer uses to create an interface with the Media Routing PIM on the Media Routing PG. The default is 38001. Make sure the Media routing port matches that of the MR PG configuration. For example, you can access this registry key: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\mango\PG3A\PG\CurrentVersion\PIMS\pim1\MRData\Config\ApplicationTcpServiceName1`.

Step 9 Click **Next**. A **Summary** screen appears.

Step 10 Click **Next** to begin the dialer installation.

Optional - Edit Dialer Registry Value for AutoAnswer

If you enable auto answer in the CallManager with a zip tone, you must disable auto answer in the Dialer or Dialers, if there are more than one. A zip tone is a tone sent to the agent's phone to signal that a customer is about to be connected.

To disable auto answer in the Dialer, after the Dialer process runs for the first time, change the value of the following registry key to 0:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\pra01\Dialer\AutoAnswerCall

For information on other Dialer registry settings, see the *Outbound Option Guide for Unified Contact Center Enterprise*.

Add DNP Host File

Complete this procedure to add DNP Host file.

Procedure

Step 1 In the C drive of the virtual machine where dialer is installed, navigate to \icm\customerInstanceName\Dialer directory.

Step 2 Modify the DNP Host file for static route mapping.

The format for a static route is `wildcard pattern, IP address or hostname of the Gateway that connects to the dialer, description.`

Example : `7????? (Dial pattern), 10.86.227.144 (gateway ip) , calls to agent extensions`

Note Repeat these steps for each sub customer Dialer.

Outbound Option Enterprise Data

In order for Outbound Option enterprise data to appear in the Cisco Agent Desktop Enterprise Data window, the administrator must edit the Default layout to include some or all Outbound Option variables. These variables are prefixed with “BA.” (Edit the default enterprise data layout in the Cisco Desktop Administrator.)

- BAAccountNumber
- BABuddyName
- BACampaign
- BADialedListID
- BAResponse
- BAStatus
- BATimeZone

Note To enable the ECC variables, See Configure Expanded Call Variable, on page 231. The BAStatus field is required. All other BA fields are optional for Progressive and Predictive modes. In Preview mode, the Skip button will not work if BADialedListID is not enabled.

- The BABuddyName field is required, if you want to see the customer's name being called.
- If a call is part of a Preview dialing mode campaign, the first letter in the BAStatus field entry is a P. If a call is part of a Direct Preview dialing mode campaign, the first letter in the BAStatus field entry is a "D."

Configure Unified Communications Manager

Add Normalization Script

This script is needed to disable Ringback during Transfer to Agent for SIP calls.

Procedure

Step 1 Log in to **Unified Communications Manager Administration** page.

Step 2 Navigate to **Devices** > **Device Settings** > **SIP Normalization Scripts**.

Step 3 Click **Add New**.
Displays **SIP Normalization Script** page.

Step 4 Enter **Name** of the script.

Step 5 Enter the following script in **Content** field:

```
M = {}
function M.outbound_180_INVITE(msg)
msg:setResponseCode(183, "Session in Progress")
end
return M
```

Step 6 Keep default values for remaining fields.

Step 7 Click **Save**.

Configure Trunk towards the Outbound Gateway

To configure trunk towards the outbound gateway, see Add SIP Trunks, on page 282. While updating **SIP info** tab:

Procedure

Step 1 Enter IP address of outbound gateway in **Address IPv4** field.

Step 2 Choose newly added **Normalization Script** from the drop-down list.

Configure Post Call Survey

Complete the following procedures to configure post call survey:

- Configure Post Call Survey in CVP, on page 355
- Configure Unified CCE, on page 355

Configure Post Call Survey in CVP

Complete the following procedure to configure Post Call Survey in Unified CVP.

Procedure

Step 1 Log in to the Unified CVP Operations Console and choose **System** > **Dialed Number Pattern**.

Step 2 Enter the following configuration settings to associate incoming dialed numbers with survey numbers:

- **Dialed Number Pattern** - Enter the appropriate dialed number.

  The incoming Dialed Number for calls being directed to a Post Call Survey Dialed. This is the Dialed Number you want to redirect to the survey.

- **Enable Post Call Survey for Incoming Calls** - Select to enable post call survey for incoming calls.
- **Survey Dialed Number Pattern** - Enter the dialed number of the Post Call Survey. This is the dialed number to which the calls should be transferred to after the call flow is completed.
- Click **Save** to save the Dialed Number Pattern.

Step 3 Click **Deploy** to deploy the configuration to all Unified CVP Call Server devices.

Configure Unified CCE

Configure ECC Variable

You need not configure Unified CCE to use Post Call Survey, however, you can turn the feature off (and then on again) within an ICM script by using the ECC variable **user.microapp.isPostCallSurvey** and a value of n or y (value is case insensitive) to disable and re-enable the feature.

Configure the ECC variable to a value of n or y before the label node or before the Queue to Skillgroup node. This sends the correct value to Unified CVP before the agent transfer. This ECC variable is not needed to initiate a Post Call Survey call, but you can use it to control the feature when the Post Call Survey is configured using the Operations Console.

When the DN is mapped in the Operations Console for Post Call Survey, the call automatically transfers to the configured Post Call Survey DN.

Complete the following procedure to enable or disable the Post Call Survey:

Procedure

Step 1 On the Unified CCE Administration Workstation, using configuration manager, select the **Expanded Call Variable List tool**.

Step 2 Create a new ECC Variable with **Name:user.microapp.isPostCallSurvey**.

Step 3 Set **Maximum Length** to 1.

Step 4 Select the **Enabled** check box then click **Save**.

Configure a-Law Codec

Configure the following in Cisco HCS for CC core components to support a-law codec:

- Configure Gateway, on page 356
- Configure Unified CVP, on page 358
- Configure Unified Communication Manager, on page 360

Configure Gateway

- Configure Ingress Gateway, on page 356
- Configure VXML Gateway, on page 357

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

dial-peer voice 5 voip
     description for SIP TTS Media Call
     preference 1
     session protocol sipv2
```

```
     session target ipv4: <ASR primary server IP>
     destination uri tts
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 6 voip
     description for SIP ASR Media Call
     preference 1
     session protocol sipv2
     session target ipv4: <TTS primary server IP>
     destination uri asr
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 7 voip
     description for SIP TTS Media Call
     preference 2
     session protocol sipv2
     session target ipv4: <ASR secondary server IP>
     destination uri tts
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 8 voip
     description for SIP ASR Media Call
     preference 2
     session protocol sipv2
     session target ipv4: <TTS secondary server IP>
     destination uri asr
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     codec g711alaw
     no vad
```

Configure Unified CVP

Unified CVP does not require any specific configuration in OAMP.

You must convert the following files to A-law:

1. C:\inetpub\wwwroot\en-us\app
2. C:\inetpub\wwwroot\en-us\app\ag_gr
3. C:\inetpub\wwwroot\en-us\sys
4. C:\Cisco\CVP\OPSConsoleServer\GWDownloads in OAMP server
5. C:\Cisco\CVP\VXMLServer\Tomcat\webapps\CVP\audio

Note

- After converting the files in the OAMP server, access the Unified CVP OAMP page to upload the newly converted A-law files to the gateway.
- If gateways are previously used for u-law, then restart the gateway to clear the u-law files in the gateway cache.

Complete the following procedure to convert mu-law audio files to a-law format:

Procedure

Step 1 Copy the wav file from Unified CVP to your local desktop.
Step 2 Go to **All programs** > **Accessories** > **Entertainment**.
Step 3 Open the **Sound Recorder**.
Step 4 Select **File** and click **Open**.
Step 5 Browse for the mu-law audio file and click **Open**.
Step 6 Go to **Properties**.
Step 7 Click **Convert Now**.
Step 8 Select **CCITT A-Law** from **Format**.
Step 9 Click **OK**.
Step 10 Select **Files** > **Save As** and provide a filename.
Step 11 Copy the new a-law format file into the following directory of media server:

```
C:\inetpub\wwwroot\en-us\app
```

Enable Recording for Agent Greeting and Courtesy Callback

Complete the following procedure to enable recording for Agent Greeting and Courtesy Callback.

Procedure

Step 1 Open the call studio and go to the callback entry application.
Step 2 Double-click **app.callflow**.
Step 3 Go to **Record Name** element settings and change the File Type to **other** (default is wav).
Step 4 Set the MIME type to **audio/x-alaw-basic**.
Step 5 Set the File extension as **wav**
Step 6 Open the **RecordAgentGreeting** application and double-click **app.callflow**.
Step 7 Go to **Record Greeting With Confirm** element settings and change the File Type to **other** (default is wav).
Step 8 Set the MIME type to **audio/x-alaw-basic**.
Step 9 Set the File extension as **wav**.
Step 10 Validate, save, and deploy the application.

Step 11 Restart the Unified CVP services.

Configure Unified Communication Manager

Complete the following procedure to provision a-Law through Cisco Unified Communications Manager:

Procedure

Step 1 Login to the **Cisco Unified Communication Manager Administration** page.

Step 2 Navigate to **System** > **Service Parameter**.

Step 3 Choose publisher server from **Server** drop-down list.

Step 4 Choose **Cisco CallManager (Active)** from **Service** drop-down list.

Step 5 In **ClusterWide Parameters (System - Location and region)**, choose **Enabled for All Devices** from **G.711 A-law Codec Enabled** drop-down list.

Step 6 Choose **Disable** from following drop-down lists:

- **G.711 mu-law Codec Enabled**
- **G.722 Codec Enabled**
- **iLBC Codec Enabled**
- **iSAC Codec Enabled**

Step 7 Click **Save**.

Configure Unified CM Based Silent Monitoring

Perform the following steps to configure unified CM based silent monitoring:

- Enable or Disable the Built-in-Bridge. See, Enable or Disable the Built-in-Bridge , on page 297
- Add Monitoring Calling Search Space for the device

Add Monitoring Calling Search Space for the device

Before you begin

Ensure that agent phones are added. See, Add Phones, on page 291.

Note During CTIOS Server installation, for **IPCC Silent Monitor Type**, select **CCM Based**.

Procedure

Step 1 Log in to Unified Communication Domain Manager as provider, reseller or customer.
Step 2 Add Calling Search Space for monitoring purpose. See, Add Class of Service, on page 295.
Step 3 Edit **Lines**, choose newly added **Calling Search Space** from the drop-down list. See, Edit Lines, on page 291.
Step 4 Click **Save**.

Configure Unified Communication Manager

A Unified Communications Manager Music On Hold (MoH) server can generate MoH stream from an audio file or a fixed source. Either of this can be transmitted as unicast or multicast.

MoH server can be deployed in two modes.

1. Along with Unified CM on the same server for HCS for CC deployments with less than 1250 users in a CM Cluster.
2. As standalone node (TFTP/MoH Server) for HCS for CC deployments with more than 1250 users in a CM Cluster

- Configure Music On Hold Server Audio Source, on page 361
- Set up Service Parameters for Music on Hold, on page 362
- Set up Phone Configuration for Music on Hold, on page 362

Configure Music On Hold Server Audio Source

Procedure

Step 1 Login to **Cisco Unified Communications Manager Administration** page.
Step 2 Select **Media Resources** > **Music On Hold Audio Source**.
Step 3 Retain the default sample audio source.
Step 4 Select **Initial Announcement** from drop down list (optional).
Step 5 Click **Save**.
Step 6 Perform the following steps to create new Audio Source.
a) Click **Add New**.
b) Select MOH audio stream number from the drop down list.
c) Select MOH audio source file from the drop down list.
d) Enter the MOH source name .
e) Choose **Initial Announcement** from the drop-down list.
f) Click **Save**.

Set up Service Parameters for Music on Hold

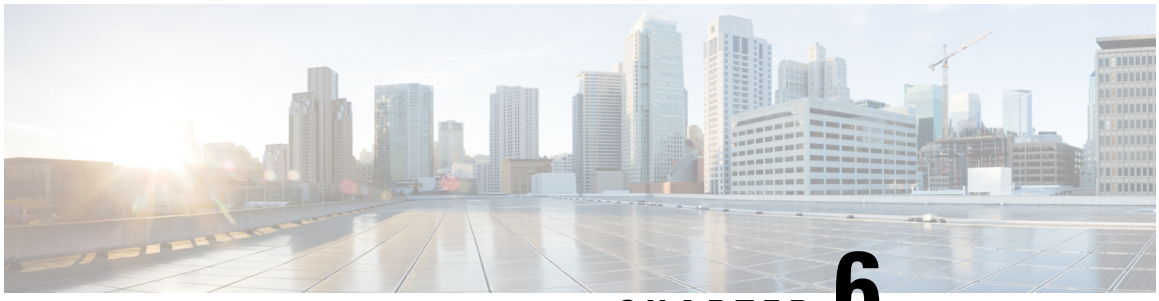
Procedure

Step 1 Login to **Cisco Unified Communications Manager Administration** page.
Step 2 Select **System** > **Service Parameters**.
Step 3 Select the MoH server from the drop-down list .
Step 4 Select the app service from **Cisco IP Voice Media Streaming App Service** drop-down list.
Step 5 Select the required codec in the **Supported MOH Codecs** field and click **Ok**.
Step 6 Click **Save**.

Set up Phone Configuration for Music on Hold

Procedure

Step 1 Login to **Cisco Unified Communications Manager Administration** page.
Step 2 Select **Device** > **Phone**.
Step 3 Select the phone to configure MOH.
Step 4 Select a audio source from **User Hold MOH Audio Source** drop-down list.
Step 5 Select a audio source from **Network Hold MOH Audio Source** drop-down list.
Step 6 Click **Save** and click **Apply** and reset the phone.



CHAPTER 6

Install and Configure Optional Cisco Components

SPAN-Based Silent Monitoring

Install SPAN-Based Silent Monitoring

Procedure

Step 1 Mount the Cisco Unified CCE CTI ISO image.

Step 2 Run `setup.exe` file to install SPAN based Silent Monitoring.

Step 3 On the **CTIOS Silent Monitoring Service** page, Click **Yes** to stop CTIOS Silent Monitor process

Step 4 Accept the Software License Agreement, then click **Continue**.

Step 5 Enter the MR patch browse location and click **Next**.

If you do not know the MR patch browser location, leave the filed blank and click **Next**.

Step 6 In the **Choose Destination Location** page, browse to the directory where you want to install, then click **Next**.

Step 7 In the **Cisco CTIOS Silent Monitor - Install Shield Wizard** window:

a) In the **Hostname\IP Address** field, enter the hostname of the silent monitor server.

b) In the **Port** field, enter the port number **42228** on which the Silent Monitor Service listens for incoming connections.

c) Check the **Silent Monitor Server** check box to allow the Silent Monitor Service to monitor multiple Mobile Agents simultaneously.

d) Enter the peer(s) information: Select this if this Silent Monitor Service is part of a cluster of Silent Monitor Services.

Step 8 Click **Next**.

Step 9 On the **CTIOS Silent Monitor** page, do not check the **Enable Security** check box, then click **OK**.

Step 10 Click **Finish**.

SPAN-Based Silent Monitoring Configuration

Configurations for SPAN from Gateway

This section describes the additional configuration required for Mobile Agent deployment:

1. For Mobile Agents, the voice path crosses the Public Switched Telephone Network (PSTN) and two gateways.

   One gateway control calls from customer phones. The other gateway controls calls from agents, known as agent gateway.

   In a Mobile Agent deployment, the Silent Monitor service uses a SPAN port to receive the voice traffic that passes through the agent gateway. This requires the computer running the Silent Monitor service to have two NIC cards; one to handle communications with clients and another to receive all traffic spanned from the switch.

   For example, if the agent gateway is connected to port 1 and the NIC (on the Silent Monitor Server that receives SPAN traffic) is connected on port 10, use the following commands to configure the SPAN session:

   ```
   monitor session 1 source interface fastEthernet0/1

   monitor session 1 destination interface fastEthernet0/10
   ```

2. To deploy Silent Monitoring for the Mobile Agent, there must be two gateways; one gateway for agent traffic and another for caller traffic.

   If you use one gateway for both agent and caller traffic, the voice traffic does not leave or cross the agent gateway and therefore cannot be silently monitored.

   For example, agent-to-agent and consultation calls between Mobile Agents share the same gateway and cannot be silently monitored. Most Mobile Agent deployments only allow silent monitoring for calls between agents and customers.

3. Install Silent Monitor service on the supervisors desktop, but you need not configure Silent Monitor service for the Mobile Agents. You must configure the agent to use one or more Silent Monitor Servers in the CTI OS Server setup program.

4. Agents who are both mobile and regular agents require at least two profiles.

   The profiles for regular agents do not contain any Silent Monitor service information.

   The profiles for Mobile Agents, contains information used to connect to a Silent Monitor Server.

Silent Monitor Service Clusters

If more than one agent gateway is present in the call center and an agent can use either gateway to log in, cluster the Silent Monitor services to support Silent Monitor as follows.

1. Deploy a separate silent monitor server for each gateway.
2. Configure a SPAN port for each silent monitor server as described in the previous section.
3. Run the Silent Monitor server installer to install and configure two Silent Monitor servers as peers.
4. Configure the following to set up a connection profile to instruct the agent desktops to connect to one of the peers:
   a. Check the Enter peers information check box.
   b. Enter the IP address of the other silent monitor service in the Hostname/IP address.

Configurations for SPAN from Call Manager

Use span from Call Manager for small agent contact center only as in this deployment model CUCM software resources are being used .

Before you begin

To Span from CUCM ensure that SM server should be on the same blade as CUCM. Ensure that CUCM uses its own mtp resources ,when the agent is logged into a phone across a gateway.

This requires the computer running the Silent Monitor service to have two NIC cards; one to handle communications with clients and another to receive all traffic spanned from the nexus.

Procedure

Use the following commands to configure the LOCAL SPAN session in nexus :

```
monitor session 1
description LOCAL-SPAN
source interface Vethernet76 both
```

where : Vethernet76 is the interface of CUCM(used for spanning) on the switch.

Cisco Unified SIP Proxy

Install Cisco Unified SIP Proxy

Installation of CUSP

Procedure

Step 1 Download all Cisco Unified SIP Proxy 8.5.7 software files.

Step 2 Copy the files to the FTP server.

Step 3 Starting from router EXEC mode, enter the following:

```
ping <ftp_server_ip_address>
```

Step 4 Enter the following and Install the software:

```
Service-Module 1/0 install url ftp://<ftp_server_ip_address>/cusp-k9.sme.8.5.7.pkg
```

Step 5 Enter **Y** to confirm installation.

Step 6 Enter Cisco Unified SIP Proxy Service Module to monitor and complete the installation.

Example of Installation on a Service Module

```
CUSP#service-nodule SM4/0 inst
CUSP#$ule SM4/0 install url ftp://10.10.10.203/cusp-k9.snc.8.5.7.pkg
Delete the installed Cisco Unified SIP Proxy and proceed with new installation?
[no]:yes
Loading cusp-k9.snc.8.5.7.pkg.install.src !
[OK - 1850/4096 bytes]
cur_cpu: 1862
cur_disk: 953880
cur_nem: 4113488
cur_pkg_name: cusp-k9.sne.8.5.7.pkg
cur_ios_version: 15.2<4>M5,
cur_image_name:c3900e-universalk9-mz
cur_pid: SM-SRE-900-K9
bl_str:
inst_str:
app_str:
key_filename: cusp-k9.sne.8.5.7.key
helper_filename:cusp-helper.sme.8.5.7
Resource check passed…
```

Post Installation Configuration Tool

Run the command: **CUSP#service-module SM 4/0 session** to open the first session.

When you open the first session, the system launches the post installation configuration tool, and asks you if you want to start configuration immediately.

Enter the appropriate response, y or n. If you enter n, the system will halt. If you enter “y”, the system will ask you to confirm, then begin the interactive post installation configuration process.

The following is an example:

```
IMPORTANT::
IMPORTANT:: Welcome to Cisco Systems Service Engine
IMPORTANT:: post installation configuration tool.
IMPORTANT::
IMPORTANT:: This is a one time process which will guide
IMPORTANT:: you through initial setup of your Service Engine.
IMPORTANT:: Once run, this process will have configured
IMPORTANT:: the system for your location.
IMPORTANT::
IMPORTANT:: If you do not wish to continue, the system will be halted
IMPORTANT:: so it can be safely removed from the router.
IMPORTANT::

Do you wish to start configuration now (y,n)? yes
Are you sure (y,n)? yes

IMPORTANT::
IMPORTANT:: A configuration has been found in flash. You can choose
IMPORTANT:: to restore this configuration into the current image.
IMPORTANT::
IMPORTANT:: A stored configuration contains some of the data from a
IMPORTANT:: previous installation, but not as much as a backup.
IMPORTANT::
IMPORTANT:: If you are recovering from a disaster and do not have a
IMPORTANT:: backup, you can restore the saved configuration.
IMPORTANT::
IMPORTANT:: If you choose not to restore the saved configuration, it
IMPORTANT:: will be erased from flash.
IMPORTANT::

Would you like to restore the saved configuration? (y,n) n

Erasing old configuration...done.

IMPORTANT::
IMPORTANT:: The old configuration has been erased.
IMPORTANT:: As soon as you finish configuring the system please use the
IMPORTANT:: "write memory" command to save the new configuration to flash.
IMPORTANT::

Enter Hostname
(my-hostname, or enter to use se-10-50-30-125):
Using se-10-50-30-125 as default

Enter Domain Name
(mydomain.com, or enter to use localdomain): cusp

IMPORTANT:: DNS Configuration:
IMPORTANT::
IMPORTANT:: This allows the entry of hostnames, for example foo.cisco.com, instead
IMPORTANT:: of IP addresses like 1.100.10.205 for application configuration. In order
IMPORTANT:: to set up DNS you must know the IP address of at least one of your
IMPORTANT:: DNS Servers.

Would you like to use DNS (y,n)?y

Enter IP Address of the Primary DNS Server
(IP address): 180.180.180.50
```

```
Found server 180.180.180.50

Enter IP Address of the Secondary DNS Server (other than Primary)
(IP address, or enter to bypass):

E

Enter Fully Qualified Domain Name(FQDN: e.g. myhost.mydomain.com)
or IP address of the Primary NTP server
(FQDN or IP address, or enter for 10.50.30.1): 10.50.10.1
Found server 10.50.10.1

Enter Fully Qualified Domain Name(FQDN: e.g. myhost.mydomain.com)
or IP address of the Secondary NTP Server
(FQDN or IP address, or enter to bypass):

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa 4) Arctic Ocean 7) Australia 10) Pacific Ocean
2) Americas 5) Asia 8) Europe
3) Antarctica 6) Atlantic Ocean 9) Indian Ocean
#? 2
Please select a country.
1) Anguilla 27) Honduras
2) Antigua & Barbuda 28) Jamaica
3) Argentina 29) Martinique
4) Aruba 30) Mexico
5) Bahamas 31) Montserrat
6) Barbados 32) Netherlands Antilles
7) Belize 33) Nicaragua
8) Bolivia 34) Panama
9) Brazil 35) Paraguay
10) Canada 36) Peru
11) Cayman Islands 37) Puerto Rico
12) Chile 38) St Barthelemy
13) Colombia 39) St Kitts & Nevis
14) Costa Rica 40) St Lucia
15) Cuba 41) St Martin (French part)
16) Dominica 42) St Pierre & Miquelon
17) Dominican Republic 43) St Vincent
18) Ecuador 44) Suriname
19) El Salvador 45) Trinidad & Tobago
20) French Guiana 46) Turks & Caicos Is
21) Greenland 47) United States
22) Grenada 48) Uruguay
23) Guadeloupe 49) Venezuela
24) Guatemala 50) Virgin Islands (UK)
25) Guyana 51) Virgin Islands (US)
26) Haiti
#? 47
Please select one of the following time zone regions.
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Time - Indiana - most locations
6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
7) Eastern Time - Indiana - Pulaski County
8) Eastern Time - Indiana - Crawford County
9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
```

```
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Mountain Time
18) Mountain Time - south Idaho & east Oregon
19) Mountain Time - Navajo
20) Mountain Standard Time - Arizona
21) Pacific Time
22) Alaska Time
23) Alaska Time - Alaska panhandle
24) Alaska Time - Alaska panhandle neck
25) Alaska Time - west Alaska
26) Aleutian Islands
27) Hawaii
#? 21

The following information has been given:
United States
Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Is the above information OK?
1) Yes
2) No
#? 1

Local time is now: Mon Apr 5 11:20:17 PDT 2010.
Universal Time is now: Mon Apr 5 18:20:17 UTC 2010.
executing app post_install
executing app post_install done
Configuring the system. Please wait...
Changing owners and file permissions.
Tightening file permissions ...
Change owners and permissions complete.
Creating Postgres database .... done.
INIT: Switching to runlevel: 4
INIT: Sending processes the TERM signal
==> Starting CDP
STARTED: cli_server.sh
STARTED: ntp_startup.sh
STARTED: LDAP_startup.sh
STARTED: SQL_startup.sh
STARTED: dwnldr_startup.sh
STARTED: HTTP_startup.sh
STARTED: probe
STARTED: fndn_udins_wrapper
STARTED: superthread_startup.sh
STARTED: /bin/products/umg/umg_startup.sh

Waiting 49 ...

IMPORTANT::
IMPORTANT:: Administrator Account Creation
IMPORTANT::
IMPORTANT:: Create an administrator account.
IMPORTANT:: With this account, you can log in to the
IMPORTANT:: Cisco Unified SIP Proxy
IMPORTANT:: GUI and run the initialization wizard.

IMPORTANT::

Enter administrator user ID:
(user ID): test
tesEnter password for test:
```

```
(password):
Confirm password for test by reentering it:
(password):

SYSTEM ONLINE
cusp-sre-49# show software version
Cisco Unified SIP Proxy version <8.5.7>
Technical Support: http://www.cisco.com/techsupport Copyright <c> 1986-2008 by Cisco
Systems,Inc.
Cusp-src-49# show software packages

Installed Packages:
- Installer <Installer application >  <8.5.7.0>
- Infrastructure <Service Engine Infrastructure> <8.5.7>
- Global <Global manifest > <8.5.7>
- Bootloader <Secondary> <Service Engine Bootloader> <2.1.30>
- Core <Service Engine OS Core > <8.5.7>
- GPL Infrastrucutre <Service Engine GPL Infrastructure > <8.5.7>
```

Obtaining New or Additional Licenses

Required Information

Collect the following information before you obtain new or additional CSL licenses:

- The SKU for the features that you need. The SKU is used in the ordering process to specify the desired licenses for the Cisco Unified SIP Proxy features that you want.
- The Product ID (PID) and the Serial Number (SN) from the device. Together, these form the unique device identifier (UDI). The UDI is printed on a label located on the back of most Cisco hardware devices or on a label tray visible on the front panel of field-replaceable motherboards. The UDI can also be viewed via software using the show license udi command in privileged EXEC mode.

Using the Licensing Portal to Obtain Licenses for Additional Features or Applications

Note You must have a Cisco.com password to access some of the URLs in the following procedure.

Follow these steps to obtain additional licenses for Cisco Unified SIP Proxy Release 8.5.7 features.

Procedure

Step 1 Go to http://www.cisco.com/web/ordering/root/index.html and choose one of the ordering processes (through partner, Cisco direct, etc.) and order licenses. When you purchase a license, you will receive a product activation key (PAK), which is an alphanumeric string that represents the purchase.

Step 2 To get your license file, return to the **Cisco Product License Registration Portal** at http://www.cisco.com/web/ordering/root/index.html. When prompted, and enter the PAK and the unique device identifier (UDI) of the device where the license will be installed.

Step 3 Download the license file or receive the license file by email.

Step 4 Copy the license file(s) to a FTP or TFTP server.

Using the CLI to Install the Cisco Unified SIP Proxy Release 8.5.7 Licenses

Follow these steps to install the licenses for Cisco Unified SIP Proxy

Procedure

Step 1 Login to the CLI.

Step 2 Enter `license install` <*URL*>, where <*URL*> is the FTP URL that you copied the license in the previous procedure.

Step 3 Verify the license by entering either `show license` or `show software licenses`.

Step 4 Activate the new license by entering `license activate`.

Step 5 Reload the module by entering `reload` and confirming that you really want to reload the module.

Note You cannot remove evaluation licenses.

Configure Cisco Unified SIP Proxy Server

Login to CUSP portal *http://<cusp module IP>/admin/Common/HomePage.do* and configure the Cisco Unified SIP Proxy server, in the following order:

Required Software	Tasks
Configure CUSP	Configure Cisco Unified SIP Proxy, on page 371
Configure Gateway	Configure Gateway, on page 378
Configure Unified CVP	Configure Unified CVP, on page 379
Configure Unified Call Manager though UCDM	Configure Cisco Unified Communications Manager , on page 380

Configure Cisco Unified SIP Proxy

Perform the following procedures to configure Unified SIP Proxy

Sequence	Done?	Tasks	Notes
1		Configure Networks, on page 372	
2		Configure Triggers, on page 372	
3		Configure Server Groups, on page 373	
4		Configure Route Tables, on page 374	

Sequence	Done?	Tasks	Notes
5		Configure Route Policies, on page 375	
6		Configure Route Triggers, on page 375	

For complete configuration details of Cisco Unified SIP Proxy, see Full Configuration for Cisco Unified SIP Proxy, on page 375

Table 25: Example CUSP Deployment Details

Server Name	IP Address	FQDN
CUSP	10.10.10.49	cusp.hcsdc1.icm
CVP	10.10.10.10	cvp.hcsdc1.icm
CUCM	10.10.10.30	ccm.hcsdc1.icm
Gateway	10.10.10.180	gw.hcsdc1.icm

Configure Networks

Procedure

Step 1 Login to CUSP portal.

Step 2 Navigate to **Configure** > **Networks** and click **Add**.

Step 3 Enter a unique name for the Network.

Example:

hcs

Step 4 Choose **Standard** from the **TYPE** drop-down list.

Step 5 Enable the **Allow Outbound Connections**.

Step 6 Click **Add** on the **SIP Listen Points** tab.

Step 7 Choose newly added **Network** and select **SIP Listen Points** tab.

Step 8 Select the IP address of the CUSP, from the **IP address** drop-down list, See Table 25: Example CUSP Deployment Details, on page 372.

Step 9 Keep the default port 5060.

Step 10 Select the **Transport Type** as **TCP** and click **Add**.

Step 11 Repeat the **step 6** to **step 8**, select **Transport Type** as UDP and click **Add**.

Step 12 Disable **SIP Record-Route**, select and disable all the networks for the CVP that includes callflows.

Configure Triggers

Procedure

Step 1 Login to CUSP Portal.

Step 2 Navigate to **Configure** > **Triggers** and click **Add**.

Step 3 Enter a name for the Trigger and click **Add**.

Example:

hcs trigger in

Step 4 Choose the appropriate **Trigger conditions** from the drop-down lists.

Example:

Inbound Network,

Is exactly, and

hcs

Step 5 Click **Add**.

Configure Server Groups

Procedure

Step 1 Login to CUSP portal.

Step 2 Navigate to **Configure** > **Server Groups** > **Groups**.

Step 3 Enter a name (FQDN) for the **Server Group**.

Example:

ccm.hcsdc1.icm

Step 4 Choose **global (default)** from **Load Balancing Scheme** drop-down list.

Step 5 Choose **hcs** from **Network** drop-down list.

Step 6 Check the **Pinging Allowed** check-box.

Step 7 Click **Add**.

Step 8 Select newly added **Server Group** to add the elements for a respective server group.

Step 9 Select **Elements** tab and click **Add**.

Step 10 In **<IP Address>** text-box, enter the IP address of the Server Group, see Table 25: Example CUSP Deployment Details, on page 372.

Step 11 In **Port** text-box, enter the port value.

Step 12 Choose **tcp** from **Transport Type** drop-down list.

Step 13 In **Q-Value** text-box, enter the Q-Value as `1.0`.

Step 14 In **Weight** text-box, enter the weight `10`.

Step 15 Click **Add**.

Step 16 Repeat the above steps to configure cvp, gateway, ccm server groups.

Configure Route Tables

Table 26: Example Route Table

Key	Description	Host / Server Group (FQDN)	Network
4000	Agent Extension	ccm.hcsdc1.icm	hcs
7777	Network VRU label for CVP client	gw.hcsdc1.icm	hcs
8881	Network VRU label for CUCM client	cvp.hcsdc1.icm	hcs
811	Dialed number	cvp.hcsdc1.icm	hcs
912	Post call survey dialed number	cvp.hcsdc1.icm	hcs
9191	Ringtone	gw.hcsdc1.icm	hcs
9292	Error Tone	gw.hcsdc1.icm	hcs
6661111000	Network VRU label for MR client	cvp.hcsdc1.icm	hcs
978	Customer Dialed Number	out.hcsdc1.icm	hcs

Procedure

Step 1 Login to CUSP portal.

Step 2 Navigate to **Configure** > **Route Tables**.

Step 3 Click **Add**.

Step 4 Enter a name for a Route Table, click **Add**.

Example:

hcs

Step 5 Select the **Route Table** to add the rules for a respective route table.

Step 6 Click **Add**.

Step 7 In the **Key** text-box, enter key, see Table 26: Example Route Table, on page 374.

Step 8 Choose a **Destination** from **Route Type** drop-down list.

Step 9 In **Host / Server Group** text-box, enter Hostname (FQDN) / IP address, see Table 25: Example CUSP Deployment Details, on page 372.

Step 10 In **Port** text-box, enter the Port value.

Step 11 Choose an appropriate **Transport Type** from the drop-down list

Step 12 Choose an appropriate **Network** from the drop-down list.

Configure Route Policies

Procedure

Step 1 Login to CUSP portal.
Step 2 Navigate to **Configure** > **Route Policies**.
Step 3 Click **Add**.
Step 4 Enter a name for a Route Policy, click **Add**.
Step 5 Choose a **Name** from the drop-down list.
Step 6 Choose a **Lookup Key Matches** from the drop-down list.
Step 7 Choose the **Lookup Key** from the drop-down lists.
Step 8 Click **Add**.

Configure Route Triggers

Procedure

Step 1 Login to CUSP portal.
Step 2 Navigate to **Configure** > **Route Triggers**.
Step 3 Click **Add**.
Step 4 Choose a **Routing Trigger** from the drop-down list.
Step 5 Choose a **Trigger** from the drop-down list.
Step 6 Click **Add**.
Step 7 Select newly added **Trigger** to add trigger condition.
Step 8 Select the **Trigger Condition** from the drop-down lists.
Step 9 Click **Add**.

Full Configuration for Cisco Unified SIP Proxy

```
cusp(cusp)# show configuration active ver
cusp(cusp)# show configuration active verbose
Building CUSP configuration...
!
server-group sip global-load-balance call-id
server-group sip retry-after 0
server-group sip element-retries udp 2
server-group sip element-retries tls 1
server-group sip element-retries tcp 1
sip dns-srv
 enable
 no naptr
 end dns
!
no sip header-compaction
no sip logging
!
```

```
sip max-forwards 70
sip network hcs standard
 no non-invite-provisional
 allow-connections
 retransmit-count invite-client-transaction 3
 retransmit-count invite-server-transaction 5
 retransmit-count non-invite-client-transaction 3
 retransmit-timer T1 500
 retransmit-timer T2 4000
 retransmit-timer T4 5000
 retransmit-timer TU1 5000
 retransmit-timer TU2 32000
 retransmit-timer clientTn 64000
 retransmit-timer serverTn 64000
 tcp connection-setup-timeout 0
 udp max-datagram-size 1500
 end network
!
sip overload reject retry-after 0
!
no sip peg-counting
!
sip privacy service
sip queue message
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 20
 end queue
!
sip queue radius
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 20
 end queue
!
sip queue request
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 20
 end queue
!
sip queue response
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 20
 end queue
!
sip queue st-callback
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 10
 end queue
!
sip queue timer
 drop-policy none
 low-threshold 80
 size 2500
 thread-count 8
 end queue
```

```
!
sip queue xcl
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 2
 end queue
!
route recursion
!
sip tcp connection-timeout 30
sip tcp max-connections 256
!
no sip tls
!
sip tls connection-setup-timeout 1
!
trigger condition hcs_trigger_in
 sequence 1
  in-network ^\Qhcs\E$
  end sequence
 end trigger condition
!
trigger condition hcs_trigger_out
 sequence 1
  out-network ^\Qhcs\E$
  end sequence
 end trigger condition
!
trigger condition mid-dialog
 sequence 1
  mid-dialog
  end sequence
 end trigger condition
!
accounting
 no enable
 no client-side
 no server-side
 end accounting
!
server-group sip group ccm.hcsdc1.icm hcs
 element ip-address 10.10.10.31 5060 tcp q-value 1.0 weight 10
 element ip-address 10.10.10.131 5060 tcp q-value 1.0 weight 10
 failover-resp-codes 503
 lbtype global
 ping
 end server-group
!
server-group sip group cvp.hcsdc1.icm hcs
 element ip-address 10.10.10.10 5060 tcp q-value 1.0 weight 10
 failover-resp-codes 503
 lbtype global
 ping
 end server-group
!
server-group sip group gw.hcsdc1.icm hcs
 element ip-address 10.10.10.180 5060 tcp q-value 1.0 weight 10
 failover-resp-codes 503
 lbtype global
 ping
 end server-group
!
route table hcs
```

```
 key 4000 target-destination ccm.hcsdc1.icm hcs
 key 77777 target-destination gw.hcsdc1.icm hcs
 key 8881 target-destination cvp.hcsdc1.icm hcs
 key 91100 target-destination cvp.hcsdc1.icm hcs
 end route table
!
policy lookup hcs_policy
 sequence 100 hcs request-uri uri-component user
  rule prefix
  end sequence
 end policy
!
trigger routing sequence 1 by-pass condition mid-dialog
trigger routing sequence 3 policy hcs_policy condition hcs_trigger_out
trigger routing sequence 4 policy hcs_policy condition mid-dialog
trigger routing sequence 5 policy hcs_policy condition hcs_trigger_in
!
server-group sip ping-options hcs 10.10.10.49 4000
 method OPTIONS
 ping-type proactive 5000
 timeout 2000
 end ping
!
server-group sip global-ping
sip cac session-timeout 720
sip cac hcs 10.10.10.10 5060 tcp limit -1
sip cac hcs 10.10.10.131 5060 tcp limit -1
sip cac hcs 10.10.10.180 5060 tcp limit -1
sip cac hcs 10.10.10.31 5060 tcp limit -1
!
no sip cac
!
sip listen hcs tcp 10.10.10.49 5060
sip listen hcs udp 10.10.10.49 5060
!
call-rate-limit 200
!
end
cusp(cusp)#
```

Configure Gateway

- Create a Sip-Server with the CUSP IP, on page 378
- Create a Dial-Peer, on page 378

Create a Sip-Server with the CUSP IP

```
sip-ua
 retry invite 2
 retry bye 1
 timers expires 60000
 timers connect 1000
 sip-server ipv4:10.10.10.49:5060
 reason-header override
```

Create a Dial-Peer

```
dial-peer voice 9110 voip
 description Used for CUSP
 preference 1
 destination-pattern 911T
 session protocol sipv2
 session target sip-server
```

```
session transport tcp
voice-class codec 1
dtmf-relay rtp-nte
no vad
```

Configure Unified CVP

Configure SIP Proxy

Procedure

Step 1 Login to Unified Customer Voice Portal.

Step 2 Navigate to **Device Management** > **SIP Proxy Server**, click **Add New**.

Step 3 Enter the IP Address, Hostname. Select **Cisco Unified SIP Proxy** from **Device Type** drop-down list .

Step 4 Click **Save**.

Configure SIP Server Groups

Procedure

Step 1 Login to Unified Customer Voice Portal.

Step 2 Navigate to **System** > **SIP Server Groups**, click **Add New**.

Step 3 Enter the FQDN name, IP Address, Port, Priority, Weight of CUSP and click **Add**.

Step 4 Click **Save**.

Configure Call Server

Procedure

Step 1 Login to Unified Customer Voice Portal.

Step 2 Navigate to **Device Management** > **Call Server**.

Step 3 Select **Call Server** > **Click Edit** > **Click SIP tab**.

Step 4 Select **Yes** to enable Outbound Proxy Server.

Step 5 Enter **Outbound SRV domain name / Server Group Name (FQDN)**, click **Save and Deploy**.

Note As CUSP provides centralized dialed plan , delete the existing Dialed number patterns.

Configure Cisco Unified Communications Manager

Login to the Unified Communications Domain Manager administration interface and perform the following steps to complete a route configuration toward the Unified CUSP server.

- Add Trunk to CVP, on page 380
- Add Trunk to CUSP, on page 380

Add Trunk to CVP

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **SIP Trunks**:

- For provider or reseller administrator **Device Management** > **CUCM** > **SIP Trunks**
- For customer administrator **Device Management** > **Advanced** > **SIP Trunks**

Step 4 Click **Add** to create SIP trunk.

Step 5 Perform the following, In **Device Information** tab:

a) Choose required IP address from **CUCM** drop-down list that you want to add SIP trunk.
b) Enter a unique SIP trunk name in **Device Name** field.
c) Choose **Device Pool** from the drop-down list.
d) Check **Run On All Active Unified CM Nodes** check-box.

Step 6 Goto **SIP Info** tab and perform the following:

a) Click **Add** icon in **Destination** panel.
b) Enter destination IP address of CVP **Address IPv4** field.
c) Change **Port** to 5090.
d) Enter **Sort Order** to prioritize multiple destinations.

Note Lower sort order indicates higher priority.

e) Choose newly added **SIP Trunk Security Profile** from the drop-down list.
f) Choose **sip profile** from the drop-down list.

Repeat this step to add another trunk.

Step 7 Click **Save**.

Add Trunk to CUSP

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **SIP Trunks**:

- For provider or reseller administrator **Device Management** > **CUCM** > **SIP Trunks**
- For customer administrator **Device Management** > **Advanced** > **SIP Trunks**

Step 4 Click **Add** to create SIP trunk.

Step 5 Perform the following, In **Device Information** tab:

a) Choose required IP address from **CUCM** drop-down list that you want to add SIP trunk.
b) Enter a unique SIP trunk name in **Device Name** field.
c) Choose **Device Pool** from the drop-down list.
d) Select **Run On All Active Unified CM Nodes** check-box.

Step 6 Goto **SIP Info** tab and perform the following:

a) Click **Add** icon in **Destination** panel.
b) Enter destination IP address of CUSP in **Address IPv4** field.
c) Change **Port**, if required.
d) Enter **Sort Order** to prioritize multiple destinations.

Note Lower sort order indicates higher priority.

e) Choose newly added **SIP Trunk Security Profile** from the drop-down list.
f) Choose **sip profile** from the drop-down list.

Repeat this step to add another trunk.

Step 7 Click **Save**.

Configure Outbound with Cisco Unified SIP Proxy

Configure Unified CCE

Procedure

Step 1 Select **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Peripheral Gateway Setup**.

Step 2 Click **Add** under **Instance Component**, then click **Outbound Dialer** to add the dialer.

Step 3 On the **Outbound Dialer properties** page, ensure that the **SIP** radio button is selected and then click **Next**.

Step 4 In the **SIP Dialer Name** text box, enter the SIP dialer name exactly as it is configured in the **Dialer Tool** under **Configuration Manager**.

Step 5 In **SIP Server Type**, ensure that **(CUSP)/(CUBE)** is selected.

Step 6 Enter **CUSP IP** in the **SIP Server** text box and click **Next**.

Step 7 In the **Campaign Manager Server** text box, enter **Unified CCE DataserverA /RoggerA side IP** address.

Step 8 Check the **Enable Secured Connection** checkbox to enable secured connection.

Note Before you enable secured connection between the components, ensure to complete the security certificate management process.

For more information, see 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.

Step 9 In the **CTI Server A** text box, enter **A side CTIOS server IP Address**; in the **CTI Server Port A** text box, enter the appropriate port number. The default port is**42027** for non-secured connection and **42030** for secured connection.

Step 10 In the **CTI Server B** text box, enter **B side CTIOS server IP address**; in the **CTI Server Port B** text box, enter the appropriate port number. The default port is**42027** for non-secured connection and **42030** for secured connection.

Step 11 Keep all other fields as **default** and click **Next**. In the following window, click **Next** to complete the install.

Configure Gateway

```
dial-peer voice 811 voip
 description ******To CUCM*****
 destination-pattern 811T
 session protocol sipv2
 session target sip-server
 voice-class codec 1
 voice-class sip rel1xx supported "100rel"
 dtmf-relay rtp-nte h245-signal h245-alphanumeric
 no vad
!

 sip-ua
retry invite  2
retry bye 1
timers expires 60000
timers connect 1000
sip-server dns:out.hcsdc1.icm
reason header override
permit hostname dns:out.hcsdc1.icm
```

Configure Cisco Unified SIP Proxy for IVR based Campaign

Procedure

Step 1 Login to CUSP portal.

Step 2 Navigate to **Configure** > **Route Tables**.

Step 3 Click the existing route table.

Example:

HCS.

Step 4 Select the Route Table to add the rules for a respective route table.

Step 5 Click **Add**.

Step 6 In **Key** text-box, enter key, 8881.

Step 7 Choose **Destination** from **Route Type** drop-down list.

Step 8 In **Host / Server Group** text-box, enter Hostname (FQDN) / IP address of CVP.

Example:

cvp.hcsdc1.icm

Step 9 In **Port** text-box, enter the Port value.

Step 10 Choose an appropriate **Transport Type** from the drop-down list.

Step 11 Choose an appropriate **Network** from the drop-down list.

Note As CUSP provides centralized dial plan management you can directly route the IVR call to CVP.

Avaya PG

Follow the below procedures for 4000 and 12000 agent deployment model:

- Create Golden Template for Avaya PG, on page 383
- Configure Avaya PG, on page 387

Create Golden Template for Avaya PG

Follow this sequence of tasks to create the golden template for Avaya PG. After each task, return to this page to mark the task "done" and continue the sequence:

Sequence	Done?	Tasks	Notes
1		Download `UCCE_12.5_Win2016_vmv13_v1.0`	See Download OVA Files, on page 384.
2		Create the virtual machine for the Unified CCE Avaya PG	Follow the procedure Create Virtual Machines, on page 384.
3		Install Microsoft Windows Server	Follow the procedure Install Microsoft Windows Server, on page 385.
4		Install Antivirus Software	Follow the procedure Install Antivirus Software, on page 17.
5		Install the Unified Contact Center Enterprise	Follow the procedure Install Unified Contact Center Enterprise, on page 386.
6		Convert the virtual machine to a template.	Follow the procedure Convert the Virtual Machine to a Golden Template, on page 386.

After you create all golden templates, you can run the automation process (Automated Cloning and OS Customization, on page 2). After you run the automation process, you can configure the Avaya PG server on the destination system. See Configure Avaya PG, on page 387.

Download OVA Files

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

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

Before you begin

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

Procedure

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

Step 2 Select the required software type.

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

Create Virtual Machines

Procedure

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

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

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

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

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

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

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

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

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

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

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

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

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

- Public to Visible Network
- Private to Private Network

Step 10 Click **Finish**.

Install Microsoft Windows Server

Procedure

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

Step 2 Switch on the virtual machine.

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

Step 4 Click **Install Now**.

Step 5 Enter the product activation key, then click **Next**.

Step 6 Select the Windows Server you want to install, then click **Next**.

Step 7 Accept the license agreement, then click **Next**.

Step 8 Select **Custom: Install Windows Only (Advanced)**, select the disk, then click **Next**.
The installation begins.

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

Step 10 Refer related topics to install the VMware tools.

Step 11 Enable **Remote Desktop Connection**:

a) Select **Start** > **Control Panel** > **System and Security**.
b) Click **Allow remote access** > **OK**.
c) Select **Allow connections from computers running any version of Remote Desktop** and click **Apply**.
d) Click **OK**.

Step 12 Open the **Network and Sharing Center** and select **Ethernet**.

Step 13 In the **Ethernet Status** dialog box, configure the network settings and the Domain Name System (DNS) data:

a) Select **Properties**. Uncheck the **Internet Protocol Version 6 (TCP/IP6)**.
b) Select **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**.
c) Select **Use the following IP Address** option.
d) Enter the IP address, Subnet mask, and Default gateway.
e) Select **Use the following DNS Server Address** option.
f) Enter **Preferred DNS Server** address, then click **OK**.

Note All network configurations are overwritten with new settings.

Step 14 Go to **Settings** > **Update & Security** and run Microsoft Windows Update.

Note Edge Chromium (Microsoft Edge) is not installed by default on the Windows server. To install Edge Chromium (Microsoft Edge), see *Microsoft* documentation.

Install Unified Contact Center Enterprise

Procedure

Step 1 Add the virtual machine template into the domain.

Step 2 Mount the Unified Contact Center Enterprise ISO image to the virtual machine.

Step 3 From the `ICM-CCE-CCH` Installer directory, run `setup.exe` and follow the InstallShield procedures.

Step 4 In the **Select the installation method** window, select **Fresh Install**, then click **Next**.

Step 5 In the **Maintenance Release (MR)** window, keep the **Maintenance Release Location** field blank, then click **Next**.

Step 6 In the **Installation Location** window, select the drive `C`, then click **Next**.

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

Step 8 In the **Installation Complete** window, click **Yes, I want to restart my computer now**, then click **Finish**.

Step 9 Apply the Unified Contact Center Enterprise maintenance release, if applicable.

Step 10 Unmount the Unified Contact Center Enterprise ISO image.

Step 11 Move the virtual machine template back to the workgroup.

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

Convert the Virtual Machine to a Golden Template

Perform this procedure for the golden-template install option.

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

Before you begin

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

Procedure

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

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

Configure Avaya PG

This section explains the configuration procedures you must perform for the Avaya PG:

Sequence	Done?	Tasks	Notes
1		Configure Network Cards	Follow the procedure Configure Network Cards, on page 21.
2		Verify the Machine in Domain	Follow the procedure Verify the Machine in Domain, on page 23.
3		Configure Unified CCE Encryption Utility	Follow the procedure Configure Unified CCE Encryption Utility, on page 25.
4		Add Avaya PG from Configuration Manager	Follow the procedure Add Avaya PG, on page 388.
5		Setup Avaya PG	Follow the procedure Setup Avaya PG, on page 388.
6		Configure CTI server	Follow the procedure Configure CTI Server, on page 43.
7		Configure CTI OS server	Follow the procedure Configure CTI OS Server, on page 389.
8		Configure Avaya ACD	Follow the procedure in *ACD Configuration* and *Unified ICM Software Configuration* sections of *Cisco Unified ICM ACD Supplement for Avaya Communication Manager* https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/e9288eff-12af-4b91-b9f7-2c28528860cf.
9		Verify Cisco Diagnostic Framework Portico	Follow the procedure Verify Cisco Diagnostic Framework Portico, on page 45.
10		Cisco SNMP Setup	Follow the procedure Cisco SNMP Setup, on page 45.

Add Avaya PG

Complete the following procedure to add an Avaya PG using Unified CCE Configuration Manager.

Procedure

Step 1 Login to Unified CCE Admin Workstation server and navigate to **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 Choose **Tools** > **Explorer Tools** and open **PG Explorer** in **Configuration Manager** window.

Step 3 Click **Add PG** and enter the following values in **Logical Controller** pane.

a) Enter *Avaya_PG_XX* , where XX is the Avaya PG number, in the **Peripheral Name** field.
b) Choose **Avaya (Definity)** in the **Client Type** field .

Step 4 Click **Peripheral** and enter the following values in **Peripheral** tab.

a) Choose **None** in the **Default Desk Settings** field.
b) Check **Enable post routing**.

Step 5 Click **Routing Client** tab and enter a name for Routing client.

Step 6 Click **Save** and **Close** .

Setup Avaya PG

Procedure

Step 1 Choose **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Peripheral Gateway Setup**.

Step 2 Click **Add** in the **Instance Components** pane, and choose **Peripheral Gateway**

Step 3 Select the following in the **Peripheral Gateway Properties** dialog box:

a) Check **Production Mode**.
b) Check **Auto Start System Startup**.
c) Check **Duplexed Peripheral Gateway**.
d) Choose an appropriate PG from PG node Properties ID drop-down list.
e) Select the appropriate side (**Side A** or**Side B**) accordingly.
f) Under Client Type pane, add **Avaya (Definity)** to the selected types.
g) Click **Next**.

Add PIM1 (Avaya PIM)

Procedure

Step 1 Enter the logical controller ID in the **Peripheral Gateway Configuration** pane.

Step 2 Select **EAS-PHD Mode** and check **Using MAPD** check-box in the **Avaya (Definity)ECS Setting** pane.

Step 3 Click **Add**, in the **Peripheral Interface Manager** pane.

Step 4 Select **Avaya(Definity)** and **PIM1**, click **OK**.

Step 5 Check **Enabled** in **Avaya(Definity) ECS PIM Configuration** dialog box.

Step 6 Enter the peripheral name in the **Peripheral Name** field.

Step 7 Enter the peripheral id in the **Peripheral ID** field.

Step 8 Check **CMS Enabled** and enter port number in **Port number to listen on** field, in **Call Management System (CMS) Configuration** pane

Step 9 Check **Host1** as **Enabled** in the **CVLAN/MAPD Configuration** pane.

Step 10 Enter **Hostname** of ASAI link, check configured ASAI link number for **Monitor ASAI** links and **Post-Route ASAI** links

Step 11 Click **OK** and click **Next**.

Step 12 Select the preferred side in the **Device Management Protocol Properties** dialog-box.

Step 13 Click **Next**.

Step 14 Enter the PG Private Interfaces and the PG Public (Visible) Interfaces in the **Peripheral Gateway Network Interfaces** dialog box.

Step 15 Click the QoS button in the private interfaces section for Side A and check the **Enable QoS** check-box and click **OK**.

This step applies only to Side A.

Step 16 Click the QoS button in the public interfaces section for Side A and check the **Enable QoS** check-box and click **OK**.

This step applies only to Side A.

Step 17 Click **Next** and **Finish**.

Note Do not start Unified **ICM/CCNodeManager** until all ICM components are installed.

Configure CTI OS Server

Procedure

Step 1 Mount the CTI OS ISO image or copy the CTI OS installer to the local drive of the Unified CCE machine with an Agent PG..

Step 2 If a maintenance release for CTI OS is available, copy the maintenance release to the local drive .

Step 3 Navigate to **%Home\CTIOS\Installs\CTIOS Server** and run setup.exe. Click **Yes** to the warning that the SNMP service will be stopped and then restarted after the installation completes.

Step 4 Accept the Software License Agreement.

Step 5 Browse to the location for the latest Maintenance Release, if any. Click **Next**.

Step 6 In CTI OS Instance dialog box, click in the CTI OS Instance List pane. In the Add CTI OS Server Instance window, enter your instance name and click **OK**.

Note The CTIOS Instance Name must match with ICM Instance Name, else it will not reflect in the Diagnostics portico.

Step 7 Click **Add** in the CTI OS Server List pane and click **OK**.

Step 8 In the Enter Desktop Drive dialog box, choose drive C and click **OK**.

Step 9 In the CTI Server Information dialog box, enter the IP address of the Unified CCE machines where CTI Server is installed, and enter the ports for Side A (**42027**) and Side B (**43027**).

Step 10 To enable secured connection, click the **Enable Secure Connection** checkbox.

Before establishing secured connection between the components, ensure that the security certificate management process is completed. For more information on secured connections, see *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.

Step 11 Click **Next**.

Step 12 In the Peripheral Identifier dialog box, enter the following values and Click **Next** .

a) Enter the peripheral ID of respective PG.
b) Select the peripheral type as **G3** for Avaya PG.
c) Choose **Agent ID** .

Step 13 In the Connect Information dialog box, enter Listen Port **42028** and accept all defaults and then click **Next**.

Step 14 In the Statistics Information dialog box, check **Polling for Agent Statistics at End Call** and then click **Next**.

Step 15 In the IPCC Silent Monitor Type dialog box, set Silent Monitor Type to **CCM Based** and click **Next**.

Step 16 In the Peer CTI OS Server dialog box, configure as follows:

a) Check **Duplex CTIOS Install**.
b) In the Peer CTI OS Server field, set the *hostname/IP address of the other CTIOS Server* in the duplex configuration.
c) In the Port field, enter **42028.**

Step 17 Click **Finish**.

Step 18 In the Cisco CTI OS Server Security dialog box, uncheck **Enable Security**. Click **OK**.

Step 19 In the CTI OS Security dialog box, click **Finish**.

Step 20 When prompted to restart the computer, click **Yes**. If there is a Maintenance Release, its installation begins automatically.

Step 21 Follow all prompts to install the Maintenance Release, if there is one.

Step 22 When the Maintenance Release install completes, click **Finish** and follow the prompts to restart.

Step 23 Access Registry Editor (**Run > regedit**).

Step 24 Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,Inc.\Ctios\CTIOS_<instance name>\CTIOS1\Server\Agent**.

Step 25 Set **forceLogoutOnSessionClose** to **1**.

Translation Route for Avaya

A translation route is a temporary destination for a call that allows call information to be delivered with the call. Network Blind Transfer is used to return the destination label to the originating CVP routing client.

Configure Unified CCE

Enable Network Transfer Preferred

Perform the following steps for Avaya, CVP, and CUCM PIMs:

Procedure

Step 1 In Unified CCE Admin Workstation Server, navigate to **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**

Step 2 Select **Tools** > **Explorer Tools** > **PG Explorer**.

Step 3 Select appropriate PG from the list and expand the PG.

Step 4 Select appropriate PIM from the list.

Step 5 Goto **Routing Client** tab, check the **Network Transfer Preferred** check box.

Create Service

Procedure

Step 1 Log in to Unified CCDM portal as a tenant or sub customer.

Step 2 Select **Resource Manager**.

Step 3 Select the folder from the left hand side panel that you want to create service.

Step 4 Select **Service** from **Resource** drop-down list.

Step 5 Enter **Name**.

Step 6 Select appropriate Avaya peripheral from **Peripheral** drop-down list.

Step 7 Select **Advanced** tab, choose **Cisco_Voice** from **Media Routing Domain** drop-down list.

Step 8 Click **Save**.

Configure Translation Route

Procedure

Step 1 In Unified CCE Admin Workstation Server, navigate to **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 Select **Tools** > **Explorer Tools** > **Translation Route Explorer**.

Step 3 In the **Translation Route** tab:

a) Enter **Name**.

b) From the **Type** drop-down list, select **DNIS**.

Step 4 Click **Add Route**.

Step 5 In the **Route** tab:

a) Enter **Name**.

b) From the **Service** drop-down list, select newly created service.

Step 6 Click **Add Peripheral Target**.

Step 7 In the **Peripheral Target** tab:

a) Enter **DNIS**.

Note DNIS should be same as label.

b) Select **Network Trunk Group** from the drop-down list.

Step 8 Click **Add Label**.

Step 9 In the **Label** tab:

a) Select **Routing Client** from the drop-down list.

b) Enter the **Label**.

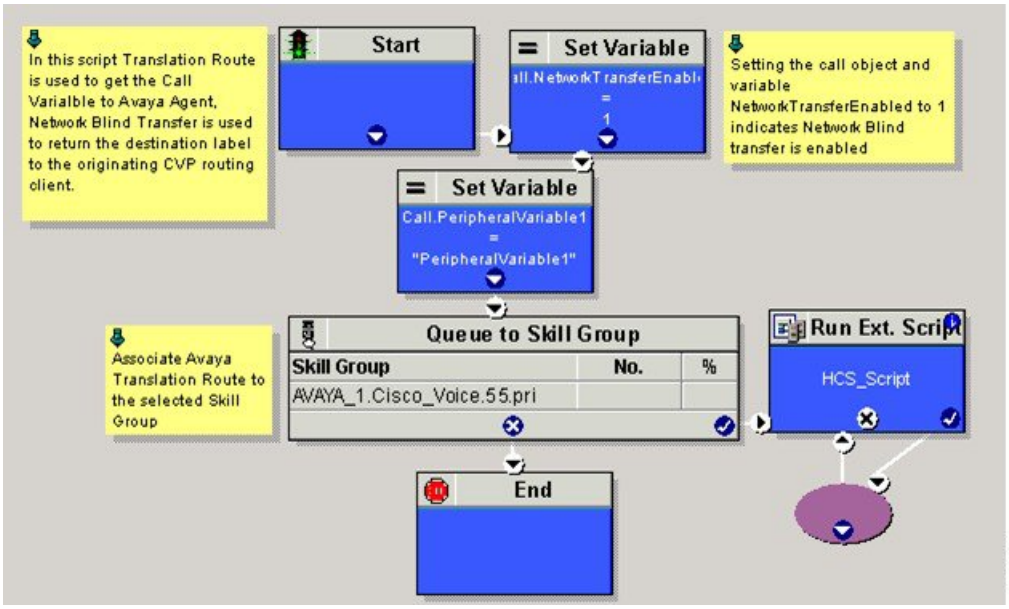
Note Post route VDN should be created as label for the CVP routing client.

Step 10 Click **Save**.

Configure Script

Following illustration explains to configure scripts.

Figure 19: Configure Scripts



Cisco Virtualized Voice Browser

- Create Golden Template for Cisco Virtualized Voice Browser, on page 393
- Configure Unified CVP, on page 394
- Configure Cisco Virtualized Voice Browser, on page 395

Create Golden Template for Cisco Virtualized Voice Browser

Follow this sequence of tasks to create the golden template for Voice Browser. After each task, return to this page to mark the task "done" and continue the sequence:

Sequence	Done?	Tasks	Notes
1		Download `VVB_12.5_vmv13_v2.5.ova`	See Download OVA Files, on page 384.
2		Create the virtual machine for Cisco Virtualized Voice Browser.	Follow the procedure Create Virtual Machines, on page 384.
3		Install Cisco Virtualized Voice Browser.	Follow the procedure for installing VOS applications for golden templates. See Install Voice OS-Based Applications, on page 394.

4		Convert the virtual machine to a Golden Template.	Follow the procedure Convert the Virtual Machine to a Golden Template, on page 386.

After you create all golden templates:

Procedure

Step 1 Run the automation process. See Automated Cloning and OS Customization, on page 2.

Step 2 Configure Cisco Virtualized Voice Browser. See Configure Cisco Virtualized Voice Browser, on page 395.

Install Voice OS-Based Applications

Use the following procedures to install Voice OS-basedapplications:

- Cisco Virtualized Voice Browser
- Cloud Connect

Procedure

Step 1 Mount the ISO file to the virtual machine and switch on.

Step 2 Follow the Install wizard:

a) On the **Disk found** page, click **OK** to check the media before installation.
b) Click **OK**.
c) On the **Product Deployment Selection** page, select the required product and click **OK**.
d) On the **Proceed with Install** page, click **Yes**.
e) On the **Platform Installation Wizard** page, select the **Skip** option.

After installation, displays the **Pre-existing Configuration Information** page.

f) Press `Ctrl+Alt` to free your cursor.

Step 3 Shut down the virtual machine.

Step 4 Unmount the ISO image.

Configure Unified CVP

- Add Cisco Virtualized Voice Browser, on page 395
- Associate Dialed Number Pattern, on page 395

Add Cisco Virtualized Voice Browser

Procedure

Step 1 Login CVP operation console.
Step 2 Navigate to **Device Management** > **Gateway** > **Virtualized Voice Browser**.
Step 3 Enter **IP Address** and **Hostname** of Cisco Virtualized Voice Browser.
Step 4 Keep the default trunk option in **Group ID** field.
Step 5 Enter **Username** and **Password**.
Step 6 Enter **Enable Password**.
Step 7 Keep default option in **Port** field.
Step 8 Click **Sign in**.
Step 9 Click **Save**.

Associate Dialed Number Pattern

Procedure

Step 1 Login CVP Operation Console.
Step 2 Select **System** > **Dialed Number Pattern**.
Step 3 Select the **Dialed Number Pattern** from the list that you want to associate.
Step 4 From the **Route to Device** drop-down list, select Cisco Virtualized Voice Browser IP.
Step 5 Click **Save**.
Step 6 Click **Deploy**.

Configure Cisco Virtualized Voice Browser

Access Virtualized VB Administration Web Interface

The web pages of the Virtualized VB Administration web interface allow you to configure and manage the Virtualized VB system and its subsystems.

Use the following procedure to navigate to the server and log in to Vitualized VB Administration web interface.

Procedure

Step 1 Open the Cisco Virtualized Voice Browser Administration Authentication page from a web browser and enter the following case-sensitive URL:*https://<servername>/appadmin*

In this example, replace <*servername*> with the hostname or IP address of the required Virtualized VB server.

Displays Security Alert dialog box.

Step 2 Login **Cisco Virtualized VB Administration** using your credentials.

Note
- If you are accessing Virtualized VB for the first time, enter the Application User credentials that you specified during installation of the Virtualized VB.
- For security purposes, Cisco Virtualized VB Administration logs out after 30 minutes of inactivity.
- Virtalized VB Administration detects web-based cross-site request forgery attacks and rejects malicious client requests. It displays the error message, “The attempted action is not allowed because it violates security policies.”

Step 3 Import the license file and click **Next** to configure.
Displays **Component Activation** page.

Step 4 After all the components status shows **Activated**, click **Next**.
Displays **System Parameters Configuration** page.

Step 5 Choose **codec** from the drop-down list and click **Next**.
Displays **Language Confirmation** page.

Step 6 Choose **Language** from the drop down list and appropriate options.

Step 7 Click **Next**.

Access Virtualized VB Serviceability Web Page

The Vitrualized VB Serviceability is used to view alarm and trace definitions for Virtualized VB services; start and stop the Virtualized VB Engine; monitor Virtualized VB Engine activity and to activate and deactivate services. After you log in to Cisco Virtualized VB Administration web page, you can access Virtualized VB Serviceability:

- From Navigation drop-down list, or
- From Web Browser, enter: *https://<server name or IP address>/uccxservice/*.

Add a SIP Trigger

Follow the below steps to add a SIP trigger:

Procedure

Step 1 Log in to **Cisco Virtualized Voice Browser Administration** page.
Step 2 Select **Subsystems** > **SIP Telephony** > **SIP Triggers**.
Step 3 Click **Add New**.
Step 4 In **Directory Information** tab, enter **Directory Number**.
Step 5 Select **Language** from the drop-down list.
Step 6 Select **Application Name** from the drop-down list.
Step 7 Optional, click **Show More** to associate the trigger for ASR.
Step 8 In **Override Media Termination** field, select **Yes** option.
Step 9 Move required dialog groups between **Select Dialog Groups** and **Available Dialog Groups**.
Step 10 Click **Add** or **Update** to save the changes.

Configure Agent Greeting

- Configure Unified CVP, on page 411
- Configure Unified CCE, on page 381

Configure Whisper Announcement

Procedure

Step 1 Sign-in to Cisco Virtualized Voice Browser Administration page.
Step 2 Select **Application** > **Application Management**.
Step 3 Ensure that the **ringtone** application is listed and associated with the trigger `919191*`.

What to do next

- Configure Unified CVP, on page 411
- Configure Unified CCE, on page 381

Configure ASR and TTS

Cisco Virtualized Voice Browser supports ASR and TTS through two subsystems. Follow the procedure to configure ASR and TTS subsystems:

- Configure ASR Subsystem, on page 398
- Configure TTS Subsystem, on page 398

Configure ASR Subsystem

ASR subsystem allows user to choose options through IVR:

Procedure

Step 1 Log in to **Cisco Virtualized Voice Browser Administration** page.
Step 2 Select **Subsystems** > **Speech Servers** > **ASR Servers**
Step 3 Click **Add New**.
Step 4 In **Server Name** field, enter hostname or IP address.
Step 5 Enter **Port Number**.
Step 6 Select **Locales** from the drop-down list and click **Add Language**.
Step 7 Check **Enabled Languages** check-box.
Step 8 Click **Add**.

Configure TTS Subsystem

TTS subsystem converts plain-text (UNICODE) into IVR.

Procedure

Step 1 Log in to **Cisco Virtualized Voice Browser Administration** page.
Step 2 Select **Subsystems** > **Speech Servers** > **TTS Servers**
Step 3 Click **Add New**.
Step 4 In **Server Name** field, enter hostname or IP address.
Step 5 Enter **Port Number**.
Step 6 Select **Locales** from the drop-down list and click **Add Language**.
Step 7 Check **Enabled Languages** check-box.
Step 8 Select **Gender** from the below options:

- Male
- Female
- Neutral

Note Select at least one gender for each enabled language.

Step 9 Click **Add**.

Note Click **Update** to modify the existing configuration.

Configure Courtesy Callback for Cisco VVB

Procedure

Step 1 Log in to **Cisco Virtualized Voice Browser Administration** page.

Step 2 Select **Application** > **Application Management**.

Step 3 Select **Comprehensive** from the list.

Step 4 Ensure **Comprehensive** application is associated with the trigger **777777777***

What to do next

Configure courtesy callback for gateway, Unified CVP, and Unified CCE.

Cloud Connect

Create Golden Template for Cloud Connect

Follow this sequence of tasks to create the golden template for Cloud Connect. After each task, return to this page to mark the task "**done**" and continue the sequence:

Sequence	Done?	Tasks	Notes
1		Download `cloudconnect_12.5_VOS_vmv13_v1.0.ova`	See Download OVA Files, on page 384.
2		Create the virtual machine for Cloud Connect.	Follow the procedure Create Virtual Machines, on page 384.
3		Install Cloud Connect.	Follow the procedure Install Voice OS-Based Applications, on page 394.
4		Convert the virtual machine to a Golden Template.	Follow the procedure Convert the Virtual Machine to a Golden Template, on page 386.

After you create all golden templates, run the automation process. For more information, see Automated Cloning and OS Customization, on page 2.

Initial Configuration for Cloud Connect

Before adding Cloud Connect to the inventory, you will have to install the certificates from both Cloud Connect publisher and subcriber.

For more information, see the section *Certificates for CCE Web Administration* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Procedure

Step 1 In the Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings**, click **Inventory**.

Step 2 In the Inventory page, click **New** to add the new machine to the System Inventory.

Step 3 In the Add Machine dialog box:

a) Select **Cloud Connect Publisher** from the Type list.
b) Enter Hostname or IP Address of the Cloud Connect Publisher Node.
c) Enter Username and Password for your Cloud Connect cluster Administrator.
d) Click **Save**.

Note When you configure Cloud Connect Publisher, its Cloud Connect Subscriber is added to the Inventory automatically.

Edit Cloud Connect Configuration

Procedure

Step 1 In the Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings**, click **Inventory**.

Step 2 Click the Cloud Connector Publisher device to open the Edit window.

Note If you edit the Cloud Connect Publisher, the Cloud Connect Subscriber associated with the publisher is updated automatically. You cannot edit Cloud Connect Subscriber from the Inventory page.

Step 3 Edit the Username and Password for your Cloud Connect cluster Administrator.

Step 4 Click **Save**.

Monitor Server Status Rules

In CCE deployments, the Unified CCE Administration page displays the total number of alerts for machines with validation rules. Click the alert count to view the list of all alerts for each machine. Upon clicking Alerts for the respective machine, you can view the details of the alerts grouped by the following categories:

Server Status Category	Description	Example Rules
Configuration	Rules for installation and configuration of a component. These rules identify problems with mismatched configuration between components, missing services, and incorrectly configured services.	**Cloud Connect:** The status and alerts will appear only if the Cloud Connect is added to the Inventory. **Note** When the machine status is out of sync, every 10mins auto sync will be triggered to synchronize the machine configuration.
Operation	Rules for the runtime status of a component. These rules identify services and processes that cannot be reached, are not running, or are not in the expected state.	

Delete Cloud Connect Configuration

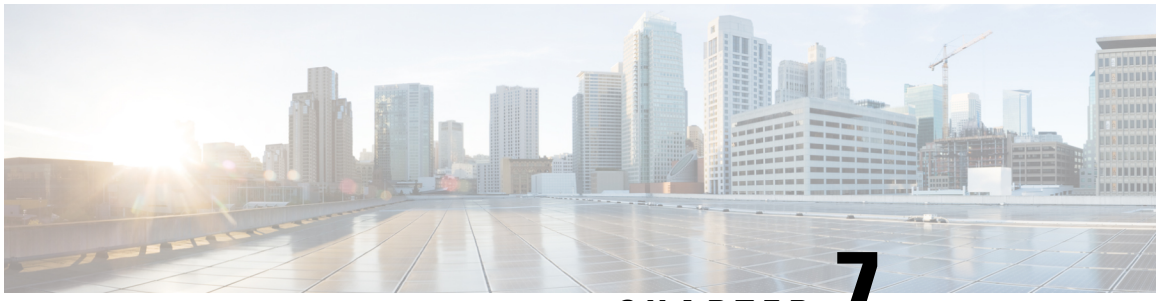
Procedure

Step 1 Navigate to **Unified CCE Administration** > **Infrastructure Settings** > **Inventory**.

Step 2 Hover over the Cloud Connect Publisher device and click the **x** icon.

Step 3 Click **Yes** to confirm the deletion.

Note If you delete the Cloud Connect Publisher, the Cloud Connect Subscriber associated with the publisher is deleted automatically. You cannot delete Cloud Connect Subscriber from the Inventory page.



CHAPTER 7

Remote Deployment Options

Global Deployments

Global deployments allows service providers to deploy remote sites with centralized management. The following global deployment topologies are supported with standard HCS for CC for CC deployment models.

Remote CVP Deployment

The Remote CVP deployment requires the following servers deployed at the remote sites. The maximum RTT with central controller over the WAN is restricted up to 400 ms.

Prerequisite: Standard HCS for CC for CC deployment model at the Data center.

Unified CVP Servers for Remote CVP Deployment

Use the Golden Template tool to deploy the remote CVP servers from the Golden templates. This section explains the procedures to configure Unified CVP servers at Remote Site.

Configure Remote CVP Server

To configure the remote CVP servers, See Configure Unified CVP Server, on page 48

Configure Operations Console for Remote CVP for Remote Deployment

Add the remote CVP server components in CVP OAMP and change the UDP transmission, Heartbeat properties.

Sequence	Task	Done?
1	Validate Network Card, on page 49	
2	Enable Unified CVP Operations Console, on page 57	
3	Configure Unified CVP Call Server for Remote Deployment, on page 404	
4	Configure Unified CVP Server Component, on page 59	
5	Configure Unified CVP Reporting Server, on page 59	
6	Configure Unified CVP Media Server, on page 60	
7	Install Unified CVP licenses, on page 60	
8	Configure Gateways, on page 61	
9	Add Unified CCE Devices, on page 62	
10	Add Unified Communications Manager Devices, on page 62	
11	Add Unified Intelligence Center Devices , on page 63	
12	Transfer Scripts and Media Files, on page 61	
13	Configure SNMP, on page 61	
14	Configure SIP Server Group for Remote Deployment, on page 405	
15	Configure Dialed Number Patterns, on page 64	

Configure Unified CVP Call Server for Remote Deployment

Procedure

Step 1 On the Unified CVP OAMP server, go to **Start** > **All Programs** > **Cisco Unified Customer Voice Portal**.

Step 2 Click **Operations Console** and log in.

Step 3 Navigate to **Device Management > Unified CVP Call Server**.

Step 4 Click **Add New**.

Step 5 On the General tab, enter the IP address and the hostname of the Cisco Unified CVP Server. Check **ICM**, **IVR**, and **SIP**. Click **Next**.

Step 6 Click the **ICM** tab. For each of the Cisco Unified CVP Call Servers, retain the default port of 5000 for the VRU Connection Port.

Step 7 Click the **SIP** tab:

a) In the Enable outbound proxy field, select **No**.
b) In the Use DNS SRV type query field, select **Yes**.
c) Check **Resolve SRV records locally**.
d) Set the UDP Retransmission Count to 3 in Advanced Configuration.

Step 8 Click the **Device Pool** tab. Make sure the default device pool is selected.

Step 9 (Optional) Click the **Infrastructure** tab. In the Configuration Syslog Settings pane, configure these fields as follows:

a) Enter the IP address or the hostname of the syslog server.

Example:

Prime server

b) Enter **514** for the port number of the syslog server.
c) Enter the name of the backup server to which the reporting server writes log messages.
d) In the Backup server port number field, enter the port number of the backup syslog server.

Step 10 Click **Save & Deploy**.

Step 11 Repeat this procedure for the remaining Unified CVP Call Servers.

Configure SIP Server Group for Remote Deployment

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 the Unified Communications Manager node.
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 SCC deployment as there is no direct SIP trunk created from Communications Manager to CVP in SCC model.

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 each gateway.
d) Click **Add**.
e) Repeat Steps c and d for each gateway. Click **Save**.

Add all VXML gateways as appropriate for deployment and branches. 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**.

Step 5 Click **Heartbeat Properties** and make the following changes, else skip this step.

a) Change the **Number of Failed Heartbeats** for **Unreachable Status field to 3**.

b) Change the **Heartbeat Timeout** field to **800 ms**.

Step 6 Click **Deployment Status** to make sure that you applied the configuration.

Note In the small contact center agent deployment, CUBE(SP) does not support FQDN configuration, therefore, you cannot create SIP server group pointing to CUBE(SP) for each sub customer.

Unified CCE Servers for Remote CVP Deployment

Use the Golden Template tool to deploy the remote CCE VRU PG from the Golden templates. This section explains the procedures to configure Unified CCE at Remote Site.

Modify Unified CCE Router

See Configure the Unified CCE Router, on page 29 and modify the value in **Enable Peripheral Gateways** dialog box by incrementing the value.

Add Remote VRU PG Using Unified CCE Configuration Manager

Complete the following procedure to add remote VRU PG using Unified CCE Configuration Manager.

Procedure

Step 1 On the Unified CCE Admin Workstation Server, navigate to **Start > Cisco Unified CCE Tools > Administration Tools > Configuration Manager**.

Step 2 In Configuration Manager Window, expand **Tools > Explorer Tools** and open **PG Explorer**. Add the Remote VRU PG, PIMs and Routing clients.

Step 3 Navigate **Tools > Explorer Tools** and open **Network VRU Explorer**. Associate the Network VRU label with the remote VRU PG Routing clients.

Step 4 Navigate **Tools > List Tools** and open **Expanded Call Variable List**. Enable the ECC variable user.microapp.media_server.

Step 5 Navigate **Tools > List Tools** and open **Agent Targeting Rule**. Add the remote VRU PG routing clients.

Configure VRU PG for Remote CVP Deployment

Complete the following tasks to configure the Unified CCE peripheral gateways for the PG Server on Side A and then repeat the same procedure for Side B.

Procedure

Step 1 Choose **Start > All programs > Cisco Unified CCE Tools >Peripheral Gateway Setup**.

Step 2 Click **Add** in the ICM Instances pane.

a) In the Add Instance window, select **Facility** and **Instance** from the drop-down list.
b) Enter **0** in the Instance Number field. Click **Save**.

Step 3 Click **Add** in the Instance Components pane, and from the Component Selection dialog box choose **Peripheral Gateway**.

Step 4 In the Peripheral Gateway Properties dialog box:

a) **Check** Production Mode.
b) **UnCheck** Auto start system startup.
c) **Check** Duplexed Peripheral Gateway.
d) Choose **PGXX** in the PG node Properties ID field.
e) Click the appropriate Side (**Side A** or **Side B**).
f) Under Client Type pane, add **VRU** to the selected types.
g) Click **Next**.

Step 5 In the Peripheral Interface Manager pane of the Peripheral Gateway Component Properties dialog box, click **Add** and configure PIM1 with the Client Type of VRU as follows:

a) Check **Enabled**.
b) In the peripheral name field, enter a name of your choice.
c) In the Peripheral ID field, Refer to PG explorer and enter the value.
d) In the VRU hostname field, enter the hostname of Remote CVP server.
e) In the VRU Connect port field, enter **5000**.
f) In the Reconnect interval (sec) field, enter **10**.
g) In the Heartbeat interval (sec) field, enter **5**.
h) In the DSCP field, choose **CS3(24)**.
i) Click **OK**.

Step 6 Refer to PG Explorer and Enter the value in the Logical Controller ID field.

Step 7 Enter **0** in the CTI Call Wrapup Data delay field.

Step 8 In the VRU Reporting pane, select **Service Control** and check **Queue Reporting**, Click **Next**.

Step 9 In the Device Management Protocol Properties dialog box, configure as follows:

a) Click **Side A Preferred**, if you are configuring Side A, or click **Side B Preferred**, if you are configuring Side B.
b) Choose **Call Router is Remote** in Side A Properties panel.
c) Choose **Call Router is Remote** in Side B Properties panel.
d) Accept the default value in the Usable Bandwidth (kbps) field.
e) Enter **4** in the Heartbeat Interval (lOOms) field. Click **Next**.

Step 10 In the Peripheral Gateway Network Interfaces dialog box, enter the PG Private Interfaces and the PG Public (Visible) Interfaces.

a) Click the **QoS** button in the private interfaces section for Side A. In the PG Private Link QoS Settings, check **Enable QoS** and click **OK**. This step applies only to Side A.
b) Click the **QoS** button in the Public (Visible) Interfaces section. In the PG Visible Link QoS Settings, check **Enable QoS**, click **OK**. This step applies only to Side A.
c) In the Peripheral Gateway Network Interfaces dialog box, click **Next**.

Step 11 In the Check Setup Information dialog box, click **Next**.

Step 12 In the Setup Complete dialog box, click **Finish**.

Note Do not start Unified CCE/CC Node Manager until all Unified CCE components are installed.

Remote CVP and CUCM Deployment

The Remote CVP and CUCM deployment requires the following servers deployed at the remote sites. The maximum RTT with central controller over the WAN is restricted up to 400 ms. Use the Golden Template tool to deploy the remote CCE, CVP, CUCM, and Finesse servers from the Golden templates.

Prerequisite: Standard HCS for CC for CC deployment model at the Data Center:

- Configure Unified CVP, on page 48
- Unified CCE Servers for Remote CVP and CUCM Deployment, on page 408
- Configure Unified Communications Manager, on page 72
- Configure Cisco IOS Enterprise Voice Gateway, on page 66
- Configure Cisco Finesse, on page 93

Unified CCE Servers for Remote CVP and CUCM Deployment

Use the Golden Template tool to deploy the remote CCE Agent PG from the Golden templates. This section explains the procedures to configure Unified CCE servers at Remote Site.

Modify Unified CCE Router

See Configure the Unified CCE Router, on page 29 and modify the value in **Enable Peripheral Gateways** dialog box by incrementing the value.

Add Remote Agent PG Using Unified CCE Configuration Manager

Complete the following procedure to add remote Agent PG using Unified CCE Configuration Manager.

Procedure

Step 1 On the Unified CCE Admin Workstation Server, navigate to **Start > Cisco Unified CCE Tools > Administration Tools > Configuration Manager**.

Step 2 In Configuration Manager Window, expand **Tools > Explorer Tools** and open **PG Explorer**. Add the Remote Agent PG, CUCM and VRU PIMs and their Routing clients.

Step 3 Navigate **Tools > Explorer Tools** and open **Network VRU Explorer**. Associate the Network VRU label with the remote Agent PG Routing clients.

Step 4 Navigate **Tools > List Tools** and open **Expanded Call Variable List**. Enable the ECC variable user.microapp.media_server.

Step 5 Navigate **Tools > List Tools** and open **Agent Targeting Rule**. Add the remote Agent PG routing clients.

Configure Agent PG for Remote CVP and CUCM Deployment

Complete the following tasks to configure the Unified CCE peripheral gateways for the PG Server on Side A and then repeat the same procedure for Side B.

Procedure

Step 1 Choose **Start > All programs > Cisco Unified CCE Tools >Peripheral Gateway Setup**.

Step 2 Click Add in the ICM Instances pane.

a) In the Add Instance window, select **Facility** and **Instance** from the drop-down list.
b) Enter **0** in the Instance Number field. Click **Save**.

Step 3 Click **Add** in the Instance Components pane, and from the Component Selection dialog box choose **Peripheral Gateway**.

Step 4 In the Peripheral Gateway Properties dialog box:

a) **Check** Production Mode.
b) **UnCheck** Auto start system startup.
c) **Check** Duplexed Peripheral Gateway.
d) Choose **PGXX** in the PG node Properties ID field.
e) Click the appropriate Side (**Side A** or **Side B**).
f) Under Client Type pane, add **CUCM** and **VRU** to the selected types.
g) Click **Next**.

Step 5 In the Peripheral Interface Manager pane of the Peripheral Gateway Component Properties dialog box, click **Add** and configure PIM1 with the Client Type of CUCM as follows:

a) **Check** Enabled.
b) In the Peripheral name field, enter a name of your choice.
c) In the Peripheral ID field, Refer to PG explorer and enter the value.
d) In the Agent extension length field, enter extension length for this deployment.
e) In the Unified Communications Manager Parameters pane, configure as follows:

- In the Service field, enter the hostname of the Unified Communications Manager Subscriber.
- In the User ID field, enter pguser.
- In the User password field, enter the password of the user that will be created on Unified Communications Manager.

f) In the Mobile Agent Codec field, choose either G711 ULAW/ALAW or G.729.
g) Click **OK**.

Step 6 In the Peripheral Interface Manager pane of the Peripheral Gateway Component Properties dialog box, click **Add** and configure PIM2 with the Client Type of VRU as follows:

a) **Check** Enabled.
b) In the peripheral name field, enter a name of your choice.
c) In the Peripheral ID field, Refer to PG explorer and enter the value.
d) In the VRU hostname field, enter the hostname of Remote CVP server.
e) In the VRU Connect port field, enter **5000**.
f) In the Reconnect interval (sec) field, enter **10**.

g) In the Heartbeat interval (sec) field, enter **5**.
h) In the DSCP field, choose **CS3(24)**.
i) Click **OK**.

Step 7 Refer to PG Explorer and Enter the value in the Logical Controller ID field.

Step 8 Enter **0** in the CTI Call Wrapup Data delay field.

Step 9 In the VRU Reporting pane, select **Service Control** and check **Queue Reporting**. Click **Next**.

Step 10 In the Device Management Protocol Properties dialog box, configure as follows:

a) Click **Side A Preferred**, if you are configuring Side A, or click **Side B Preferred**, if you are configuring Side B.
b) Choose **Call Router is Remote** in Side A Properties panel.
c) Choose **Call Router is Remote** in Side B Properties panel.
d) Accept the default value in the Usable Bandwidth (kbps) field.
e) Enter **4** in the Heartbeat Interval (lOOms) field. Click Next.

Step 11 In the Peripheral Gateway Network Interfaces dialog box, enter the PG Private Interfaces and the PG Public (Visible) Interfaces.

a) Click the **QoS** button in the private interfaces section for Side A. In the PG Private Link QoS Settings, check **Enable QoS** and click **OK**. This step applies only to Side A.
b) Click the **QoS** button in the Public (Visible) Interfaces section. In the PG Visible Link QoS Settings, check **Enable QoS**, click **OK**. This step applies only to Side A.
c) In the Peripheral Gateway Network Interfaces dialog box, click **Next**.

Step 12 In the Check Setup Information dialog box, click **Next**.

Step 13 In the Setup Complete dialog box, click Finish.

Note Do not start Unified CCE/CC Node Manager until all Unified CCE components are installed.

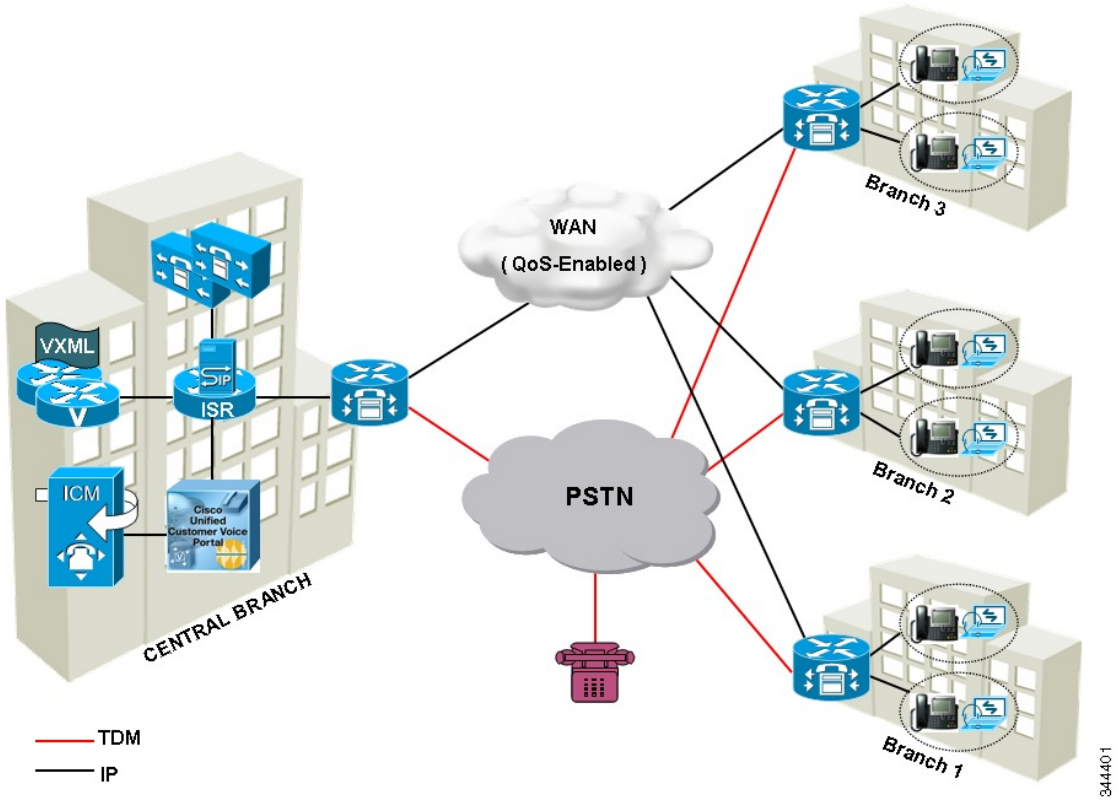
Configure Local Trunk

Complete the following procedures to configure Local Trunk.

- Configure Unified CVP, on page 411
- Configure Unified Communications Manager, on page 412

The following figure shows the Local Trunk configuration.

Figure 20: Local Trunk configuration



Configure Unified CVP

Complete the following procedure to configure Unified CVP using Operation Console for local trunk:

Procedure

Step 1 In **Device Management** > **Unified CM** > **Enable Synchronization for Location**, enable synchronization and provide the credentials required for login.

Step 2 Choose **System** > **Location** and click **Synchronize** to retrieve the locations defined on Unified CM (Publisher).

Step 3 Choose **System** > **Location** and verify that the locations have been synchronized from Unified CM (Publisher).

Step 4 Choose **Device Management** > **Gateway** and define the gateways Ingress, VXML, and Voice Browser.

Step 5 Choose **System** > **Location** and select a location:

a) Assign a Site ID and Location ID to the location, and then add the associated gateways Ingress, VXML, and Voice Browser to the location.

Step 6 Choose **System** > **Location**; navigate to Call Server Deployment and select the Call Servers where you want to deploy configuration.

Step 7 Click **Save and Deploy**.

Step 8 For the insertion point of the SiteID, use the default location between the Network VRU label and the correlation ID.

Step 9 Choose **System** > **Dialed Number Pattern** to create static routes to send calls to the branch VXML gateway or Voice Browser. It appends the site ID to the Network VRU label of Unified CVP routing client.

Example:

Consider Unified CCE Network VRU label for Unified CVP routing client is 9999331010. For queuing purpose, CVP route sends the call that is originated from branch 1 phone to branch 1 VXML gateway or Voice browser, it uses "001" as a site code for branch 1. Also, this site code define the routes for ringtone and error to send to local branch VXML gateway or Voice Browser.

Configure Unified Communications Manager

Complete the following procedures to configure Unified Communications Manager for the Local Trunk.

- Add Location, on page 412
- Verify Application User Roles, on page 413
- Configure SIP Profile for LBCAC, on page 413
  - Deploy SIP Trunk for Central Branch , on page 413
  - Deploy SIP Trunk for Local Branches, on page 414
- Configure Location Bandwidth Manager, on page 414

Add Location

Procedure

Step 1 Login to **Cisco Unified Communication Manager Administration** console.

Step 2 Navigate **System** > **Location Info** > **Location**.

Step 3 Click **Add New**.

Step 4 In **Location Information** panel, enter the location name in **Name** field.

Step 5 In **Links - Bandwidth Between This Location and Adjacent Locations** panel, enter the following.

a) Select the location

b) Enter the bandwidth configurations.

Step 6 Click **Save**.

What to do next

Select the created location on Phone, seeAdd Phones, on page 291.

Verify Application User Roles

Procedure

Step 1 Login to **Cisco Unified Communications Manager Administration** page.
Step 2 Choose **Unified Serviceability** from **Navigation** drop-down list and click **Go**.
Step 3 Choose **Tools** > **Control Center** > **Feature Services**.
Step 4 Choose **Server** from the drop-down list.
Step 5 Start the **Cisco AXL Web Service**, if it is not started.
Step 6 Select **Cisco Unified CM Administration** from **Navigation** drop-down list and click **Go**.
Step 7 Choose **User Management** > **Application User**.
Step 8 Check if you have an application user with the role of Standard AXL API Access , in **Permissions Information** panel, if it is not there, create a new application user, or add the user to a group that has the role of Standard AXL API Access.

Configure SIP Profile for LBCAC

Procedure

Step 1 Log into the **Cisco Unified Communication Manager Administration** page.
Step 2 Navigate **Device** > **Device Settings** > **SIP Profile**.
Step 3 Click **Add New**.
Step 4 Enter a name for the SIP Profile.
Step 5 In **Trunk Specific Configuration** panel **,** select **Call-Info Header with the Purpose Equal to x-cisco-orig IP** from the **Reroute Incoming Request to New Trunk Based on** drop-down list.
Step 6 In the **SIP OPTIONS Ping** panel, check **Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None(Default)"** check-box.
Step 7 Click **Save**.

Deploy SIP Trunk for Central Branch

Procedure

Step 1 Create a SIP Trunk Security Profile, see Create SIP Trunk Security Profile, on page 442.
Step 2 Create a SIP Trunk towards the CVP/SIP proxy server.

Note

a. In step 5 of creating SIP Trunk procedure, select **Run On All Active Unified CM Nodes** check-box.

b. Associate the new SIP profile with the SIP trunk. See, Create SIP Trunk, on page 442.

This routes the Network VRU label of the Unified Communications Manager routing client to the Unified CVP Call Servers.

Step 3 Create a route pattern pointing the Network VRU Label of the Unified Communications Manager routing client to the SIP trunk towards the CVP/SIP proxy, see Add Route Pattern, on page 287.

Deploy SIP Trunk for Local Branches

Procedure

Create a SIP trunk for each ingress gateway and assign the location of these ingress TDM-IP gateways as the actual branch location.

Note

a. In step 5 of creating SIP Trunk procedure, select **Run On All Active Unified CM Nodes** check-box.

b. Associate the new SIP profile with the SIP trunk. See, Create SIP Trunk, on page 442.

Configure Location Bandwidth Manager

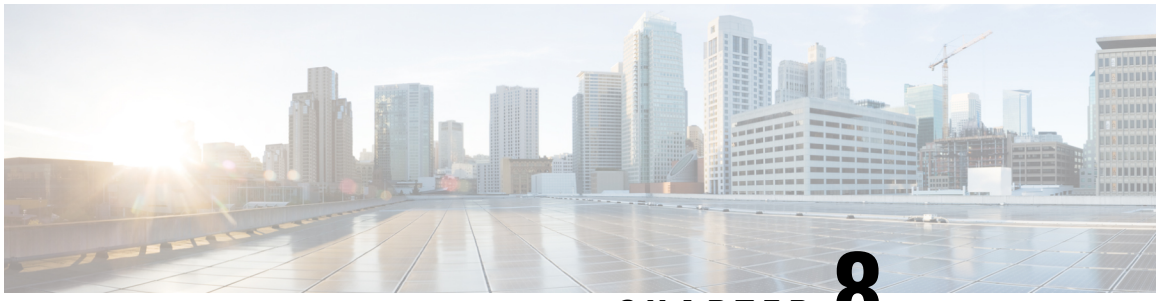
Procedure

Step 1 Choose **Tools** > **Control Center** > **Feature Services** from Cisco Unified Serviceability.

Step 2 Start the **Cisco Location Bandwidth Manager**, if it is not started

Step 3 Choose **System** > **Location info** > **Location Bandwidth Manager group** from Cisco Unified CM Administration.

Step 4 Click **Add New** enter the name and select the active and standby member (CUCM node) and click **Save**.



CHAPTER 8

Solution Serviceability

Monitor System Performance

Monitoring system performance is one way to help maintain the system. Use vCenter to monitor the following critical HCS for CC components to ensure that the virtual machines perform within system tolerances:

- CPU
- Memory
- Disk
- Network

Virtual Machine Performance Monitoring

The virtual machines must operate within the specified limits of the Virtual Machine performance counters listed in the following table.

Table 27: Virtual Machine Performance Counters

Category	Counter	Description	Threshold
CPU	CPU Usage (Average)	The CPU usage average in percentage for the VM and for each of the vCPUs.	65%
	CPU Usage in MHz (Average)	The CPU usage average in MHz.	95 percentile is less than 65% of the total MHz available on the VM. Total MHz = vCPUs x (Clock Speed).
	CPU Ready	The time a virtual machine or other process waits in the queue in a ready-to-run state before it can be scheduled on a CPU.	150 mSec.
Memory	Memory Usage (Average)	Memory Usage = Active/ Granted * 100	80%
	Memory Active (Average)	Memory that the guest OS and its applications actively use or reference. The server starts swap when it exceeds the amount of memory on the host.	95 percentile is less than 80% of the granted memory.
	Memory Balloon (Average)	ESXi uses balloon driver to recover memoryfrom less memory-intensive VMs so it can be used by those with larger active sets of memory.	0
	Memory Swap used (Average)	ESX Server swap usage. Use the disk for RAMswap.	0

Category	Counter	Description	Threshold
Disk	Disk Usage (Average)	Disk Usage =Disk Read rate + Disk Write rate	Ensure that your SAN is configured to handlethis amount of disk I/O.
	Disk Usage Read rate	The rate of reading data from the disk.	Ensure that your SAN is configured to handlethis amount of disk I/O.
	Disk Usage Write rate	The rate of writing data to the disk.	Ensure that your SAN is configured to handlethis amount of disk I/O.
	Disk Commands Issued	The number of disk commands issued on this disk in the period.	Disk IO per second IOPS = Disk Commands Issued / 20 Ensure that your SAN is configured to handle this amount of disk I/O.
	Stop Disk Command	The number of disk commandsstopped on this disk in the period. The disk command stops when the disk array takes too long to respond to the command (Command timeout).	0
Network	Network Usage (Average)	Network Usage = Data receive rate + Data transmit rate	30% of the available network bandwidth.
	Network Data Receive Rate	The average rate at which data is received on this Ethernet port.	30% of the available network bandwidth.
	Network Data Transmit Rate	The average rate at which data is transmitted on this Ethernet port.	30% of the available network bandwidth.

ESXi Performance Monitoring

The virtual machines must operate within the specified limits of the ESXi performance counters listed in the following table. The counters listed apply to all hosts that contain contact center components.

Table 28: ESXi Performance Counters

Category	Counter	Description	Threshold
CPU	CPU Usage (Average)	CPU Usage Average in percentage for ESXi Server overall and for each of the CPU processors.	60%
	CPU Usage in MHz (Average)	CPU Usage Average in MHz for ESXi server overall and for each of the CPU processors.	60% of the available CPU clock cycles.

Category	Counter	Description	Threshold
Memory	Memory Usage (Average)*	Memory Usage = Active / Granted * 100	80%
	Memory Active (Average)	Memory that the guest OS and its applications actively use or reference. The server starts swap when it exceeds the amount of memory on the host.	95 percentile is less than 80% of 2GB.
	Memory Balloon (Average)	ESX use balloon driver to recover memory from less memory-intensive VMs so it can be used by those with larger active sets of memory.	0
	Memory Swap Used	ESX Server swap usage. Use the disk for RAM swap.	0
Disk	Disk Commands Issued	Number of disk commands issued on this disk in the period.	Disk IO per second IOPS = Disk Commands Issued / 20
	Disk Command Aborts	Number of disk commands stopped on this disk in the period. Disk command stops when the disk array is taking too long to respond to the command (Command timeout).	0
	Disk Command Latency	The average amount of time taken for a command from the perspective of a Guest OS. Disk Command Latency = Kernel Command Latency + Physical Device Command Latency.	20 mSec.
	Kernel Disk Command Latency	The average time spent in ESX Server VMKernel per command.	Kernel Command Latency should be very small compared to the Physical Device Command Latency, and it should be close to zero.

Category	Counter	Description	Threshold
Network	Network Usage (Average)	Network Usage = Data receive rate + Data transmit rate	30% of the available network bandwidth.
	Network Data Receive Rate	The average rate at which data is received on this Ethernet port.	30% of the available network bandwidth.
	Network Data Transmit Rate	The average rate at which data is transmitted on this Ethernet port.	30% of the available network bandwidth.
	droppedTx	Number of transmitting packets dropped.	0
	droppedRx	Number of receiving packets dropped.	0

* The CVP Virtual Machine exceeds the 80% memory usage threshold due to the Java Virtual Machine memory usage.

Collect System Diagnostic Information Using Unified System CLI

When a Unified Contact Center operation issue arises, you can use the Unified System CLI tool to collect data for Cisco engineers to review.

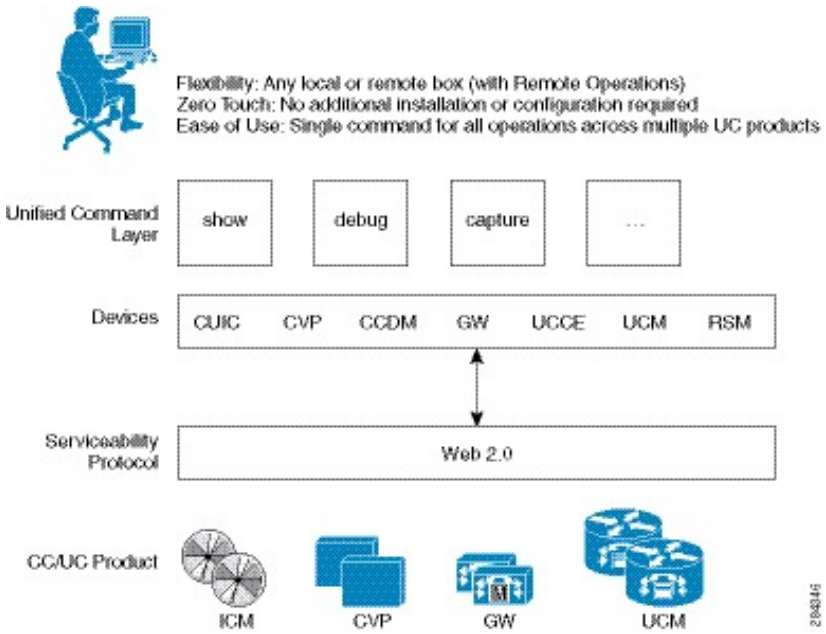
For example, you can use the System CLI if you suspect a call is not handled correctly. In this case you use the **show tech-support** system command to collect data and send the data to Cisco support.

The Unified System CLI includes the following features:

- Installs automatically on all Unified CCE and Unified CVP servers
- Retrieves your entire solution topology automatically from the Unified CCDM/OAMP server.
- Uses a consistent command across multiple products and servers.
- Runs as a Windows scheduled job.

The following figure shows the devices and Cisco Unified products that the Unified System CLI interacts with.

Figure 21: Unified System CLI Commands



To collect system diagnostic information from the components perform the following.

- Run Unified System CLI in the Local Machine, on page 420
- Run Unified System CLI in the Remote Machine, on page 421

Run Unified System CLI in the Local Machine

Procedure

Step 1 Start system CLI from Unified CCE servers.

a) Go to **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Unified System CLI**.
b) Enter the username(domain.com\username) and password.
c) Enter the Instance (optional) and click **Enter**.

Step 2 Start system CLI from Unified CVP servers.

a) Go to **Start** > **All Programs** >**Cisco Unified Customer Voice Portal** > **Unified System CLI**
b) Enter the username(wsmadmin) and password for the wsmadmin user.
c) Click **Enter**.

Step 3 Start system CLI from CCDM servers.

a) Go to **Start** > **All Programs** > **Domain Manager** > **Unified System CLI**.
b) Enter the username(wsmadmin) and password for the wsmadmin user.
c) Enter the Instance (optional) and click **Enter**.

Run Unified System CLI in the Remote Machine

Procedure

Step 1 Install the Unified CVP Operations Console Resource Manager (ORM) component on a separate network management virtual machine to ensure that performance of critical components is not affected during log collections.

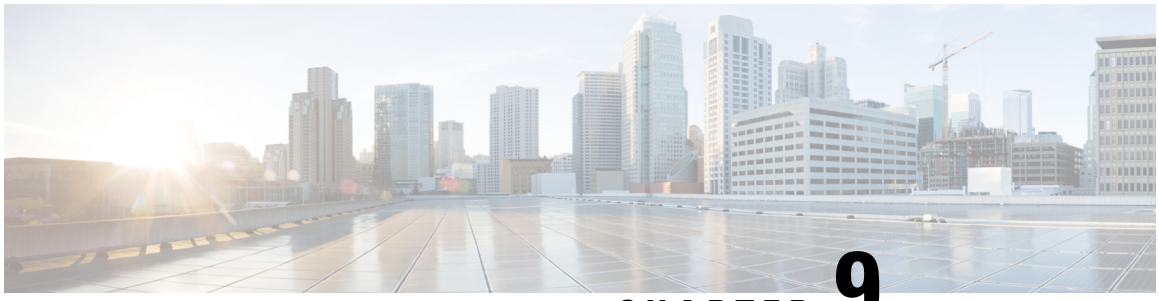
Step 2 Add and deploy the network management machine as a web service using Unified CVP OAMP.

Step 3 Make sure that you added all solution components as devices using OAMP as described in these sections:

- Add Unified CCE Devices, on page 62
- Add Unified Communications Manager Devices, on page 62
- Add Unified Intelligence Center Devices , on page 63
- Configure Unified CVP Reporting Server, on page 59

Step 4 Run the Unified System CLI to collect system diagnostic information from any of the components.

You can use the **show tech-support** system command to collect all information and logs from some or all of the components. You can use other commands to collect a subset of the information.



CHAPTER 9

Appendix

Migrate CCE Servers to the New Domain

Associate Virtual Machine with New Domain

Complete the following procedure to associate the virtual machine with the new domain.

Procedure

Step 1 Login to the machine using the local Administrator account.

Step 2 Launch **Server Manger** and click **Change System Properties**.

Step 3 Remove the machine from the old domain and reboot.

Step 4 Login to the machine again using the local Administrator account.

Step 5 Launch **Server Manger** and click **Change System Properties**.

Step 6 Enter the **`Fully Qualified Domain Name`** and click **OK**.

Step 7 Enter the domain administrator username and password.

Step 8 Reboot the server and log in to the domain with the domain credentials.

Associate Unified CCE with New Domain

Complete the following steps to associate the Unified CCE with the new domain.

Procedure

Step 1 Open the **Domain Manager** application from the **Cisco Unified CCE Tools** folder.

Step 2 Choose **All Programs** > **Cisco Unified CCE Tools** > **Domain Manager**.

Step 3 Choose the Domain Name.

Step 4 Add the Cisco Root organizational unit (OU), a Facility organizational unit (OU), and an Instance organizational unit (OU).

Step 5 Configure the following to change the domain for Unified CCE applications:

a) Run Web Setup.

b) Choose **Instance Management**.

c) Select the Instance to be modified, then click **Change Domain**.

The **Change Domain** page appears, displaying the currently configured domain and the new domain name.

d) Click **Save**.

A query is sent to confirm that you want to change the domain.

e) Click **Yes**.

The **Instance List** page appears.

Note Ensure that the domain user is created in the new domain to perform the service operation of Loggers and Administration & Data Servers component.

Caution Use the same domain user account for all the distributor and logger services. If you want to use different domain accounts for the logger and the distributor, ensure that the distributor service user account is added to the local logger `UcceService` groups on Side A and Side B.

Add CUCM SUBSCRIBER Mobile Agent Call flow

In this example, the adjacency is created for one of the sub-customer, that is SUBCUST1-CUCM-SUB-MOBILE-AGENT. For mobile agent login.

```
config
 sbc
  signaling
   adjacency sip SUBCUST1-CUCM-SUB-MOBILE-AGENT
        description "Trunk SUBCUSTOMER 1 CUCM subscriber for Mobile Agent call flow"
        account cust1
        interop
          preferred-transport tcp
          message-manipulation
            edit-profiles inbound he-dtmf
        force-signaling-peer all-requests
        adjacency-type preset-core
        service-address SA-cust1
          # service-network 1
          # signaling-local-address ipv4 20.20.20.2
        signaling-local-port 5078
        signaling-peer 20.20.20.130
        signaling-peer-port 5060
        statistics-setting summary
        activate
```

Supported Gadgets for HCS for CC

To access the gadget, on the Administration and Data server, click **Start** and navigate to **All Programs > Cisco Unified CCE Tools->Administration Tools** and open Unified CCE Web administration. The following table shows the CRUD operations supported by the HCS for CC gadgets.

Gadget	Create	Read	Update	Delete
Agent		x	x (only attribute assignment)	
Agent State Trace		x	x	
Attribute	x	x	x	x
Bucket Interval	x	x	x	x
Bulk Jobs	x	x	x	x
Deployment	x	x	x	x
Media Routing Domain	x	x	x	x
Network VRU Script	x	x	x	x
Precision Queue	x	x	x	x
Reason Code	x	x	x	x
Settings (Congestion Control)		x	x	
Single Sign-On		x	x	

x- Stands for supported

Supported API for HCS for CC

Note Agents can only perform attribute update.

API filters are built to look at the URL and the deployment model to determine if the API is accessible. It also supports read-write (GET/PUT/POST/DELETE) or read-only access to each API.

The following tables show the supported API for the HCS for CC deployment model.

Table 29: Supported API for HCS for CC

API	Create	Read	Update	Delete
Active Directory Domain		x		
Administrator	x	x	x	x
Agent		x	x (only attribute assignment)	
Agent State Trace		x	x	
Agent Team		x		
Attribute	x	x	x	x
Bucket Interval	x	x	x	x
Bulk Jobs	x	x	x	x
Congestion Control		x	x	
Deployment Type Info		x	x	
Dialed Number		x		
Machine Inventory	x	x	x	x
Media Routing Domain	x	x	x	x
Network VRU Script	x	x	x	x
Operation	x	x	x	x
Outbound API: Outbound Campaign	x	x	x	x
Outbound API: Campaign Status		x		

API	Create	Read	Update	Delete
Outbound API: Do Not Call	x	x	x	x
Outbound API: Import	x	x		x
Outbound API: Personal Callback	x	x	x	x
Outbound API: Time Zone		x		
Peripheral Gateway		x		
Precision Queue	x	x	x	x
Reason Code	x	x	x	x
Scan			x	
Serviceability		x		
Single Sign-On Global State		x	x	
Single Sign-On Registration		x	x	
Single Sign-On Status		x	x	
Skill Group		x	x	
Status		x		

x- Stands for supported

Administrator API

An administrator is an Active Directory user who has been provided access to the system.

Use the Administrator API to list the administrators currently defined in the database, define new administrators, and view, edit, and delete existing administrators.

URL

```
https://<server>:<serverport>/unifiedconfig/config/administrator
```

For more details on Administrator API, see the *Cisco Packaged Contact Center Enterprise Developer Reference Guide* at https://developer.cisco.com/site/packaged-contact-center/documentation/index.gsp.

Cisco Unified Communications Manager Configurations

- Provision Cisco Unified Communications Manager, on page 428
- Provision Cisco Unified Communications Manager for Core Component Integrated Options, on page 438

Provision Cisco Unified Communications Manager

Complete the following procedures to provision Cisco Unified Communications Manager.

Note This section is only for reference. You must configure Unified CM using Unified Communications Domain Manager.

Set Up Device Pool

Complete the following procedure to configure a device pool.

Procedure

Step 1 Choose **System** > **device pool**.

Step 2 Click **Add new**.

Step 3 Provide an appropriate device pool name in **Device Pool Name**.

Step 4 Select a corresponding Call manager group in **Cisco Unified Communications Manager group**.

Step 5 Select appropriate **Date/Time Group** and **Region**.

Step 6 Select an appropriate Media resource group list in **Media Resource Group List.**

Step 7 Click **Save**.

Set Up Unified Communications Manager Groups

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

Before you configure a Unified Communications Manager Group, you must configure the Unified Communications Managers that you want to assign as members to that group.

Procedure

Step 1 Login to the **Cisco Unified Communication Manager Administration** page, choose **System** > **Server**.

Step 2 Make sure that you configure both the Publisher and Subscriber.

a) Click **Add New**.
b) Select appropriate Server Type Eg: CUCM Voice/Video Select **Next**.
c) Enter the **Host Name/IP Address**.
d) Click **Save**.

Step 3 Choose **System** > **Cisco Unified CM**.

Step 4 Click **Find**.

Step 5 Make sure that you configured both the Publisher and Subscriber.

Step 6 Choose **System** > **Cisco Unified CM Group**.

Step 7 Add both Cisco Unified Communications Managers to the Default Unified Communications Manager Group. Select **Default** and from the Available Cisco unified communication managers select both Publisher and Subscriber to Selected Cisco Unified Communications Managers

Step 8 Click **Save**.

Set Up CTI Route Point

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

Procedure

Step 1 Choose **Device** > **CTI Route Point**.

Step 2 Click **Add New**.

Step 3 Use the wildcard string **XXXXX** to represent the digits of the dialed number configured on Unified CCE.

Note For example, the preconfigured dialed number in the Unified CCE for an agent phone is 10112.

Step 4 Select the appropriate device pool.

Step 5 Click **Save**.

Set Up Trunk

Complete the following procedure to configure a trunk for the Unified CVP Servers.

Procedure

Step 1 Choose **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 In the Device Name field, enter a name for the SIP trunk.

Step 5 In the Description field, enter a description for the SIP trunk.

a) Enter the SIP Trunk name in the Device Name field.
b) Select the appropriate Device Pool.

Step 6 Click **Next**.

Step 7 In the Trunk Configuration window, enter the appropriate settings:

a) Uncheck the **Media Termination Point** Required check box.
b) Enter the **Destination Address**.
c) Select the appropriate SIP Trunk Security Profile
d) From the **SIP Profile** drop-down list, choose **Standard SIP Profile**.
e) From the DTMF Signaling Method drop-down list, choose **RFC 2833**.

Step 8 Click **Save**.

Set Up Application User

Procedure

Step 1 Choose **User Management** > **Application User**.

Step 2 In the Application User Configuration window, click **Add New**.

Step 3 Enter the User ID that you entered in Set Up Enterprise Parameters , on page 434. Unified CCE defines the user ID as pguser.

Step 4 Enter a **cisco** in the Password field of your choice.

Note If you change this user ID or password in Unified CCE, you must also change the Unified Communications Manager application user configuration.

Note To change the JTAPI password on the CUCM configuration page:

a. Open the peripheral Gateway Setup in PG Machine.

b. Edit the CUCM PG.

c. Set the same password for the user as previously set in Step 4.

Step 5 Add the application user to the Standard CTI Enabled Group and Role:

a) Click **Add to Access Control Group**.
b) Select the **Standard CTI Enabled** group.
c) Select the **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** group.
d) Select the **Standard CTI Allow Control of Phones supporting Rollover Mode** group.
e) Click **Add Selected**.
f) Click **Save**.

Step 6 Associate the CTI route points and the phones with the application user.

Step 7 Click **Save**.

Set Up SIP Options

Procedure

Step 1 Login to CUCM administration page.

Step 2 Navigate to **Device** > **Device Settings** > **SIP Profile**.

Step 3 Click **Add New**.

Step 4 Enter **Name**.

Step 5 Check **Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"** check box, in **SIP OPTIONS Ping** panel.

Step 6 Click **Save**.

Note Once SIP profile is created, map newly added SIP profile to agent phones.

Set Up Route Pattern

Procedure

Step 1 Choose **Call Routing** > **Route Hunt** > **Route Pattern**.

Step 2 Add a route pattern for the Unified CVP routing clients as follows:

a) Click **Add New**.
b) In the **Route Pattern** field, enter `7777777777!`
c) In the **Gateway/Route List** field, choose **SIPTRK_to_CVP_1**.
d) Click **Save**.

Step 3 Add a route pattern for the Cisco Unified Communications Manager routing client.

a) Click **Add New**.
b) In the **Route Pattern** field, enter `8881111!`
c) In the **Gateway/Route List** field, choose **SIPTRK_to_CVP_1**.
d) Click **Save**.

Note These route patterns must match the network VRU label defined in Unified CCE.

Set Up Conference Bridge

Procedure

Step 1 Choose **Media Resources** > **Conference bridge**.

Step 2 Add a conference bridge for each ingress/VXML combination gateway in the deployment.

Step 3 In the Conference Bridge name field, enter a unique identifier for the conference bridge name that coincides with the configuration on the gateway.

Step 4 Click **Save**.

Step 5 Click **Apply Config**.

Set Up Media Termination Point

Procedure

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

Step 2 Add a media termination point for each ingress/VXML combo gateway in the deployment.

Step 3 In the Media Termination Point Name field, enter a media termination point name for each ingress/VXML combo gateway in the deployment.

Step 4 Click **Save**.

Step 5 Click **Apply Config**.

Set Up Transcoder

Procedure

Step 1 Choose **Media Resources** > **Transcoder**.

Step 2 Add a transcoder for each ingress/VXML combo gateway in the deployment.

Step 3 In the Device Name field, enter a unique identifier for the transcoder that coincides with the configuration on the gateway.

Step 4 Click **Save**.

Step 5 Click **Apply Config**.

Set Up Media Resource Group

Complete the following procedure to configure a media resource group for conference bridge, media termination point, and transcoder.

Procedure

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

Step 2 Add a Media Resource Group for Conference Bridges.

Step 3 Select all the hardware conference bridge resources configured for each ingress/VXML combination gateway in the deployment and add them to the group.

Step 4 Click **Save**.

Step 5 Choose **Media Resources** > **Media Resource Group**.

Step 6 Add a Media Resource Group for Media Termination Point.

Step 7 Select all the hardware media termination points configured for each ingress/VXML combination gateway in the deployment and add them to the group.

Step 8 Click **Save**.

Step 9 Choose **Media Resources** > **Media Resource Group**.

Step 10 Add a Media Resource Group for Transcoder.

Step 11 Select all the transcoders configured for each ingress/VXML combination gateway in the deployment and add them to the group.

Step 12 Click **Save**.

Set Up and Associate Media Resource Group List

Complete the following procedure to configure and associate a media resource group list. Add the media resource group list to the following devices and device pool.

Procedure

Step 1 Choose **Media Resources** > **Media Resource Group List**.

Step 2 Add a Media Resource Group list and associate all of the media resource groups.

Step 3 Click **Save**.

Step 4 Choose **System** > **Device Pool**.

Step 5 Click **Default**.

Step 6 From the Media Resource Group List drop-down list, choose the media resource group added in Step 2.

Step 7 Click **Save**.

Step 8 Click **Reset**.

Step 9 Choose **Device** > **CTI Route Point**.

Step 10 Click the configured CTI Route Point. For more information, see Set Up CTI Route Point , on page 429.

Step 11 From the Media Resource Group List drop-down list, choose the media resource group added in Step 2

Step 12 Click **Save**.

Step 13 Click **Reset**.

Step 14 Choose **Device** > **SIP Trunk**.

Step 15 Click the configured SIP Trunk for. For more information, see Set Up Trunk , on page 430.

Step 16 From the Media Resource Group List drop-down list, choose the media resource group added in Step 2

Step 17 Click **Save**.

Step 18 Click **Reset**.

Set Up Enterprise Parameters

Procedure

Step 1 Choose **System** > **Enterprise Parameter**.

Step 2 Configure the Cluster Fully Qualified Domain Name.

Example:

ccm.cce.icm

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

Set Up Service Parameters

Complete the following procedure to modify the maximum number of conference participants that the conference bridge support and maximum total number of call parties that the media termination point will support. This parameter change is required only for SCC deployment model.

Procedure

Step 1 Login to the CUCM Administration page.

Step 2 Under the System tab, Select **Service Parameter**.

Step 3 Select the CUCM server from the drop-down list.

Step 4 Select the service 'Cisco IP Voice Media Streaming App'.

Step 5 Under 'Conference Bridge (CFB) Parameters' modify the default value of 'Call Count' parameter(0-256).

Step 6 Under 'Media Termination Point (MTP) Parameters' modify the default value of 'Call Count' parameter(0-512).

Set up Recording Profile

Procedure

Step 1 Login to CUCM Administration page.

Step 2 Select **Device** > **Device Settings** > **Recording Profile**.

Step 3 Configure the recording profile name, and the recording destination address (enter the route pattern number you configured), and click **Save.**

Configuring Device

Procedure

Step 1 Choose the audio forking phone.

Step 2 Select the **Built In Bridge** configuration for this device and change the setting to **ON**.

Step 3 Access the **Directory Number Configuration** page for the line to be recorded.

Step 4 If you are using a recording partner, select either **Automatic Call Recording Enabled** or **Application Invoked Call Recording Enabled** from the **Recording Option** drop-down list, according to the recording partner recommendations. If you are not using a recording partner, select **Automatic Call Recording Enabled** .

Step 5 Select the recording profile created earlier in this procedure.

Disable iLBC, iSAC and g.722 for Recording Device

Procedure

Step 1 Login to CUCM administration page.

Step 2 Navigate to **System** > **Service parameters**

Step 3 Choose **Server** from the drop-down list.

Step 4 Choose **Service** from the drop-down list.
Displays **Service Parameter Configuration** page.

Step 5 In **Cluster-wide parameters (System - Location and Region)** panel, choose **Enable for All Devices Except Recording-Enabled Devices** for the below drop-down lists:

- **iLBC Codec Enabled**
- **iSAC Codec Enabled**
- **G.722 Codec Enabled**

Step 6 Click **Save**.

Set up Music on Hold Server Audio Source

Procedure

Step 1 Navigate to **Media Resources** > **Music On Hold Audio Source**.

Step 2 Select the default Sample Audio Source.

Step 3 Select **Initial Announcement** from drop-down list, it is optional.

Step 4 Click **Save**.

Note If you have to create new Audio Source then follow the below steps:

a) Click **Add New**.
b) Select **MOH Audio Stream Number** from drop-down list.
c) Choose **MOH Audio Source File** from the drop-down list.
d) Enter **MOH Source Name**.
e) Choose **Initial Announcement** from the drop-down list.
f) Click **Save**.

Set up Service Parameters for Music on Hold

Procedure

Step 1 Navigate to **System** > **Service Parameters**.

Step 2 Select **MOH Server**.

Step 3 Select the **Cisco IP Voice Media Streaming App** service.

Step 4 In **Supported MOH Codecs** field, select the required **Codec** and Click **Ok** in the pop-up window.

Step 5 Click **Save**.

Set up Phone Configuration for Music on Hold

Procedure

Step 1 Navigate to **Device** > **Phone**.

Step 2 Select the phone for which you want to configure MOH.

Step 3 For **User Hold MOH Audio Source** select the **Audio Source** that is added in the section **Add Music on Hold Server Audio Source**.

Step 4 For **Network Hold MOH Audio Source** select the **Audio Source** that is added in the section **Add Music on Hold Server Audio Source**.

Step 5 Click **Save and Apply Config** and reset the phone.

Setup Partition

Follow the below procedure for each sub customer.

Procedure

Step 1 Log in to **Cisco Unified Communications Administration Page**.

Step 2 Select **Call Routing** > **Class Of Control** > **Partition**.

Step 3 Click **Add New**.

Step 4 In **Name** field, enter the partition name.

Step 5 Click **Save**.

Setup Calling Search Space

Follow the below procedure for each sub customer.

Procedure

Step 1 Log in to **CUCM Administration Page**.

Step 2 Select **Call Routing** > **Class Of Control** > **Calling Space Search**

Step 3 Click **Add New**.

Step 4 In **Name** field, enter the calling search space name.

Step 5 Move the required partitions from **Available Partitions** to **Selected Partitions**.

Step 6 Click **Save**.

Associate CSS and Partition with Phones and Lines

Follow the below procedure for each sub customer.

Procedure

Step 1 Log in to **CUCM Administration page**.

Step 2 Select **Device** > **Phone** > **Find**.

Step 3 Select the phone from the list that you want to associate the partition and CSS.

Step 4 Select the required **Calling Search Space** from the drop-down list.

Step 5 From **SUBSCRIBE Calling Search Space** drop-down list, select the required Calling Search Space.

Step 6 Select the **Directory Number Line** from the list that you want to associate partition and CSS.

Step 7 Select the required **Route Partition** from the drop-down list.

Step 8 Select the required **Calling Search Space** from the drop-down list.

Step 9 Click **Apply Config**.

Step 10 Click **Reset** and click **Close**.

What to do next

Associate the required sub customer partitions with CSS, see Setup Calling Search Space, on page 437.

Associate CSS with Trunk

Procedure

Step 1 Log in to **CUCM Administration Page**.

Step 2 Select **Device** > **Trunk**.

Step 3 Select the trunk to which you want associate CSS.

Step 4 From **Calling Search Space** drop-down list, select the required CSS.

Note Select the CSS where all the sub customer partitions are associated.

Step 5 Click **Save**.

Step 6 Click **Reset** and click **Close**.

Note The route pattern which associated with trunk must be in default partition.

Provision Cisco Unified Communications Manager for Core Component Integrated Options

Configure Agent Greeting

Procedure

Step 1 Enable **Built-in-Bridge** for the local agent phones to support Agent Greeting.

Step 2 Click **System** > **Service parameters**.

Step 3 Select a Unified Communications Manager server from the **Server** drop-down list.

Step 4 Select Cisco CallManager(Active) from the **Service** drop-down list.

Step 5 Under Clusterwide Parameters (Device-Phone), select **On** for Built-in-Bridge Enable.

Step 6 Click **Save**.

Configure Mobile Agent

Complete the following procedure to configure CTI ports for Unified Mobile Agent.

Procedure

Step 1 In Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Click **Add a New Phone**.

Step 3 Select **CTI Port** from the **Phone Type** drop-down list.

Step 4 Click **Next**.

Step 5 In Device Name, enter a unique name for the local CTI Port pool name; click **OK** when finished.

Using the example naming convention format LCPxxxxFyyyy:

a) LCP identifies the CTI Port as a local device.
b) xxxx is the peripheral ID for the Unified Communications Manager PIM.
c) yyyy is the local CTI Port.

The name LCP5000F0000 would represent CTI Port: 0 in a local CTI Port pool for the Unified Communications Manager PIM with the peripheral ID 5000.

Step 6 In Description, enter text identifying the local CTI Port pool.

Step 7 Use the **Device Pool** drop-down list to choose the device pool to which you want network CTIPort pool assigned. (The device pool defines sets of common characteristics for devices.)

Step 8 Click **Save**.

Step 9 Highlight a record and select Add a New DN.

Step 10 Add a unique directory number for the CTI port you just created.

Step 11 When finished, click **Save** and **Close**.

Step 12 Repeat the preceding steps to configure the network CTI Port pool.

Step 13 In Device Name, enter a unique name for the local CTI Port pool name; click **OK** when finished.

Use the example naming convention format RCPxxxxFyyyy, where:

a) RCP identifies the CTI Port as a network device.

b) xxxx is the peripheral ID for the Unified Communications Manager PIM.
c) yyyy is the network CTI Port.

The name RCP5000F0000 would represent CTI Port: 0 in a network CTI Port pool for the Unified Communications Manager PIM with the peripheral ID 5000.

Step 14 In Description, enter text identifying the network CTI Port pool.

Step 15 Use the **Device Pool** drop-down list to choose the device pool to which you want network CTI Port pool assigned. (The device pool defines sets of common characteristics for devices.)

Step 16 Click **Save**.

Step 17 Highlight a record and select **Add a New DN**.

Step 18 Add a unique directory number for the CTI port you just created.

Step 19 When finished, click **Save** and **Close**.

Configure Local Trunk

Complete the following procedure to configure Unified Communications Manager for Local Trunk.

Procedure

Step 1 From Unified Communications Manager Administration choose **System** > **Location info** > **Location**.

Step 2 Click **Find** to list the locations and add new ones with appropriate bandwidth (8000).

Step 3 For the branch phones, configure each phone so that it is assigned the branch location for that phone.

a) Choose **Device > Phone**.
b) Click **Find** to list the phones.
c) Select a phone and set the Location field.

Step 4 Verify that the Cisco AXL Web Service is started and that an Application User is defined and has a role of Standard AXL API Access.

a) Select **Cisco Unified Serviceability** from the **Navigation** drop-down list and click **Go**.
b) Navigate to **Tools** > **Control Center** > **Feature Services** .
c) Start the Cisco AXL Web Service, if it is not started.
d) From Unified Communications Manager Administration, choose **User Management > Application User**. Verify you have a user with the role of Standard AXL API Access, or create a new one and add that user to a group that has the role of Standard AXL API Access.

Deploy SIP Trunk

Complete the following procedure to deploy the SIP trunk for local trunk:

Procedure

Step 1 Using Unified Communications Manager, create a SIP trunk toward the SIP proxy server and select the Phantom location.

Step 2 Create a SIP trunk for each ingress gateway and make the location of these ingress TDM-IP gateways the actual branch location.

Step 3 Create a route pattern pointing the Network VRU Label of the Unified Communications Manager routing client to the SIP trunk toward the SIP proxy.

The SIP proxy should route the Network VRU label of the Unified Communications Manager routing client to the Unified CVP Servers.

Step 4 For any IP-originated calls, associate the Unified Communications Manager route pattern with the SIP trunk.

Step 5 Using the Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile > Trunk Specific Configuration > Reroute Incoming Request to new Trunk based on > Call-Info header with the purpose equal to x-cisco-origIP**.

Step 6 Associate the new SIP profile with the SIP trunk and each ingress gateway.

Configure Outbound Dialer

Complete the following procedure to configure Unified Communications Manager:

Procedure

Step 1 Log in to the Unified Communications Manager administration page.

Step 2 Select **Devices** > **Trunk**.

Step 3 Create a SIP trunk to Outbound gateway.

Configure A-Law Codec

Complete the following procedure to configure Unified Communications Manager.

Procedure

Step 1 Click the **System**.

Step 2 Select **Service Parameters**.

Step 3 Select a Server.

Step 4 Select the service as **Cisco Call Manager(Active)**.

Step 5 Under Clusterwide Parameters (system-location and region), ensure the following:

- **G.711 A-law Codec Enabled** is **Enabled**.
- **G7.11 mu-law Codec Enabled** to **Disabled**.

Step 6 Click **Save**.

Create SIP Trunk between CUCM and CUBE (SP)

Create SIP Trunk Security Profile

Procedure

Step 1 Log In to CUCM Admin Portal.

Step 2 Navigate to **System->Security->Sip Trunk Security Profile.**

Step 3 Click on **Add New.**

Step 4 Provide the name for Sip Trunk Security Profile.

Step 5 In Incoming Transport Type field Select "TCP+UDP" from the drop down list.

Step 6 In Incoming Port Field Provide the Port number other than 5060 and 5090.

Note
- The port configured in step 6 should match with the "signaling peer port" that you configure in the CUBE(SP) for CUCM PUBLISHER adjacency
- A unique sip trunk security profile is required for mobile agent call flow for the each sub customer in SCC model

Step 7 Click On **Save**.

Create SIP Trunk

Procedure

Step 1 Log in to CUCM Admin Portal.

Step 2 Select **Device** > **Trunk**.

Step 3 Click **Add New**.

Step 4 In **Trunk Type** field, select the SIP trunk from the drop-down list, then click **Next**.

Step 5 Provide the name for Sip Trunk, select the device pool from the drop-down list and select **Media Resource Group List** from the drop-down list.

Step 6 In Sip Profile field, select the **Standard Sip Profile** from the drop down list. Check **Run On All Active Unified CM Nodes** check-box.

Step 7 Under SIP Information, provide the signaling-address and signaling-port details of the CUBE(SP) adjacency for the CUCM publisher for mobile agent call flow. See Add CUCM SUBSCRIBER Mobile Agent Call flow, on page 424.

Step 8 In **SIP Trunk Security Profile** field, select the profile which is created in the above procedure from the drop-down list.

Step 9 Retain rest all default value.

Step 10 Click **Save**.

Configure Music on Hold

Configure Unified Communication Manager

A Unified Communications Manager MoH server can generate a MoH stream from two types of sources, audio file and fixed source, either of which can be transmitted as unicast or multicast. There are two deployment modes:

1. An MoH server is deployed along with Unified CM on the same server for HCS for CC deployments with less than 1250 users in a CM Cluster
2. An MoH server is deployed as standalone node (TFTP/MoH Server) for HCS for CC deployments with more than 1250 users in a CM Cluster

- Configure Music on Hold Server Audio Source, on page 443
- Configure Service Parameters for Music on Hold , on page 443
- Modify Phone configuration for Music On Hold , on page 444

Configure Music on Hold Server Audio Source

Hold Server Audio Source is also known as MOH Track in UCDM.

Procedure

Step 1 In **Track Name** field, Enter the name for MOH Track.

Step 2 Enter the **Track ID**.

Step 3 Choose **MOH Server** from the drop down list.

Step 4 Click **Submit**.

Configure Service Parameters for Music on Hold

Procedure

Step 1 Navigate to **Network** > **PBX Devices**.

Step 2 Select **CUCM Cluster** and click on **Attributes** and search with the **Parameter Codec**.

Step 3 Set the value to **1** for the below listed parameters.

- **DefaultMOHCodec**
- **G711ALawCodecEnabled**
- **G711ULawCodecEnabled**

Step 4 Click **Modify**.

Modify Phone configuration for Music On Hold

Procedure

Step 1 Navigate to Location **Administration** > **Phone Management** and select the appropriate provider, reseller, customer, division and location.

Step 2 Click **Device Name**(Phone) that is added.

Step 3 In **Music On Hold** field, select the MOH Track that was configured in the above configuration.

Step 4 Click **Modify**

Base Configuration Parameters

Base Configuration Parameters for 2000 Agent Deployment

Unified CCE Instance Explorer

Name	Type	Network VRU
HCS for CC	Standard	CVP_Network_VRU
hcs	Standard	CVP_Network_VRU

Agent Desk Settings List

Name	Ring No Answer Time	Logout Non-activity Time	Maximum Wrap Up Time
Default_Agent_Desk_Settings	null	null	7200

PG Explorer

Peripheral Gateway	Type of PIM	Routing Client Name
Unified Communication Manager PG1	CUCM	CUCMPG1
Unified Voice Response (VRU) PG	VRU	CVPPG1A
	VRU	CVPPG1B
MR PG	MediaRouting	Multichannel
	MediaRouting	Outbound
	MediaRouting	Socialminer

Network VRU Explorer

Name	Type	Network VRU Label	Routing Client Name
CVP_Network_VRU	Type10	7777777777	CVPPG1A
		7777777777	CVPPG1B
		8881111000	CUCMPG1
		6661111000	Outbound
MR_Network_VRU	Type 2		

Network VRU Mapping

- All Unified CVP routing clients are mapped to **CVP_Network_VRU** of **Type10**. This is displayed in the **Advanced** tab of the PG Explorer.
- All Media Routing clients are mapped to **MR_Network_VRU** of **Type2**. This is displayed in the **Advanced** tab of the PG Explorer.

Network VRU Script List

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
VXML_Server	Type 10 CVP VRU	GS, Server, V	180	__	HCS for CC	Unchecked	Unchecked
VXML_Server_ Interruptible	Type 10 CVP VRU	GS, Server, V, interrupt	9000	__	HCS for CC	Checked	Unchecked
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS, Server, V , nointerrupt	9000	__	HCS for CC	Unchecked	Unchecked
AgentGreeting	Type 10 CVP VRU	PM, -a	180	none	HCS for CC	Unchecked	Unchecked
GreetingMenu _1_to_9	Type 10 CVP VRU	M, press _1_thru_9 _greeting, A	180	1-9	HCS for CC	Checked	Unchecked
Greeting SubMenu	Type 10 CVP VRU	M, press1-press2-press3,A	180	1-3	HCS for CC	Checked	Unchecked

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
Greeting _Not_Found	Type10 CVP VRU	PM, no _greeting _recorded, A	180	Y	HCS for CC	Checked	Unchecked
GreetingReview	Type10 CVP VRU	PM,-a,A	180	Y	HCS for CC	Checked	Unchecked
T10_GS_AUDIUM	Type 10 CVP VRU	GS,Server,V, FTP	180	,,,,,,,,,Y	HCS for CC	Checked	Unchecked
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	HCS for CC	Unchecked	Unchecked

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
VXML_Server	Type 10 CVP VRU	GS, Server, V	180	__	hcs	Unchecked	Unchecked
VXML_Server_ Interruptible	Type 10 CVP VRU	GS, Server, V, interrupt	9000	__	hcs	Checked	Unchecked
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS, Server, V , nointerrupt	9000	__	hcs	Unchecked	Unchecked
AgentGreeting	Type 10 CVP VRU	PM, -a	180	none	hcs	Unchecked	Unchecked
GreetingMenu _1_to_9	Type 10 CVP VRU	M, press _1_thru_9 _greeting, A	180	1-9	hcs	Checked	Unchecked
Greeting SubMenu	Type 10 CVP VRU	M, press1-press2-press3,A	180	1-3	hcs	Checked	Unchecked
Greeting _Not_Found	Type10 CVP VRU	PM, no _greeting _recorded, A	180	Y	hcs	Checked	Unchecked
GreetingReview	Type10 CVP VRU	PM,-a,A	180	Y	hcs	Checked	Unchecked

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
T10_GS_AUDIUM	Type 10 CVP VRU	GS,Server,V, FTP	180	,,,,,,,,,Y	hcs	Checked	Unchecked
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	hcs	Unchecked	Unchecked

Application Instance List

Application Instance	Name	Application Type	Permission Level	Application Key
Multichannel	MultiChannel	Other	Full read/write	cisco123
CCDM	CCDM	Cisco Voice	Full read/write	cisco123

Application Path List

Application Instance	Name	Peripheral Gateway	Application Path List members	
UQ.Desktop	5000.UQ.Desktop	CUCM_PG	**Peripheral**	**Media Routing Domain**
			CUCM_PG_1	SocialMiner_Task

Media Class List

Name	Description	Life	Start Timeout	Max Duration
Cisco_Chat	System provided media class for Cisco chat	1200	30	28800
Cisco_Task	System provided media class for Cisco Task	1200	30	28800
Cisco_Voice	Default value for Cisco Voice	0	0	0
CIM_BC	-	300	30	28800
ECE_Chat	-	300	30	28800
ECE_Email	-	300	30	28800
ECE_Outbound	-	300	30	28800

Media Routing Domain List

	Interruptible	Calls in Queue (Max)	Max per call type	Max time in queue
Cisco_BC	Unchecked	5000	-	-
ECE_Email	Checked	15000	-	-
ECE_Outbound	Checked	5000	-	-
ECE_Chat	Unchecked	5000	-	-
SocialMiner_Task	Unchecked	-	-	-
Cisco_Voice	Unchecked	As per your requirement	-	-

Note Set the **Max Per Call Type** and **Max Time in Queue** values as per your requirement.

Expanded Call Variable List

Note ECC variables will not be enabled by default. Use Unified CCE Configuration manager tool to enable the required ECC variables under the **Expanded Call Variable List**.

Name	Enabled	Persistent	Maximum Length	Description
user.CourtesyCallbackEnabled	FALSE	FALSE	1	Determines if Courtesy Callback is offered to a caller.
user.cvp_server_info	FALSE	FALSE	15	Used by Unified CVP to send the IP address of the Call Server sending the request to Unified CCE.
user.microapp.app_media_lib	FALSE	FALSE	210	Directory for all application-specific media files and grammar files. The **..** bypasses the user. When writing a URL path, microapp.app_media_lib and user.microapp.locale are the ECC variables.

Name	Enabled	Persistent	Maximum Length	Description
user.microapp.caller_input	FALSE	FALSE	210	Storage area for an ASR input that is collected from Get Speech. **Note** Get Speech results are written to the ECC variable. Results from Get Digits or Menu microapplications are written to the CED.
user.microapp.currency	FALSE	FALSE	6	Currency type.
user.microapp.error_code	FALSE	FALSE	2	Error status code returned from Unified CVP to Unified CCE when the Run Script Result is False.
user.microapp.FromExtVXML	FALSE	FALSE	60	This variable array returns information from the external VoiceXML file. Must be configured as array variables, not Scalar Variables, and array length set to 4.
user.microapp.input_type	FALSE	FALSE	1	Specifies the type of input that is allowed. Valid contents are: D(DTMF) and B (Both DTMF and Voice). B is the default. If you are not using an ASR, set this variable to D. If you are using an ASR, you can set this variable to either D or B.
user.microapp.locale	FALSE	FALSE	5	Combination of language and country that defines the grammar and prompt set to use.
user.microapp.metadata	FALSE	FALSE	62	Following the Menu (M), Get Data (GD) and Get Speech (GS) micro-applications, Unified CVP now returns information about the execution of that micro-application.
user.microapp.play_data	FALSE	FALSE	40	Default storage area for data for Play Data micro-applications.
user.microapp.sys_media_lib	FALSE	FALSE	10	Directory for all systems media files, such as individual digits, months, default error messages, and so forth.
user.microapp.ToExtVXML	FALSE	FALSE	60	This variable array sends information to the external VoiceXML file. Must be configured as Array variables, not Scalar Variables and array length set to 4.

Name	Enabled	Persistent	Maximum Length	Description
user.microapp.UseVXMLParams	FALSE	FALSE	1	Specifies the manner in which you pass the information to the external VoiceXML.
user.microapp.isPostCallSurvey	FALSE	FALSE	1	Used to determine if post call survey should be offered to a caller after the agent disconnects the call.
user.ece.activity.id	FALSE	FALSE	30	Needed for all types of WIM and EIM activities.
user.ece.customer.name	FALSE	FALSE	30	Needed for chat, callback, and delayed callback activities.
user.media.id	FALSE	FALSE	36	A number identifying a call to the Unified CCE Service, optionally, the H.323 Service.
user.microapp.grammar_choices	FALSE	FALSE	210	Specifies the ASR choices that a caller can input for the Get Speech micro-application.
user.microapp.inline_tts	FALSE	FALSE	210	Specifies the text for inline Text To Speech (TTS).
user.microapp.media_server	FALSE	FALSE	60	Root of the URL for all media files and external grammar files used in the script.
user.microapp.override_cli	FALSE	FALSE	200	Used by the system to override the CLI field on outgoing transfers.
user.microapp.pd_tts	FALSE	FALSE	1	Specifies whether Unifies Text To Speech or media files must be played to the caller.

System Information

- Expanded Call Context: Enabled
- Minimum Correlation number: 1001
- Maximum Correlation number: 9999
- Retain script versions:5

Agent Targeting Rule

Attribute	
Name	AgentExtensions
Peripheral	CUCM_PG_1

Attribute	
Rule Type	Agent Extension
Routing Client	All routing clients
Extension Range	000 - 999 0000 - 9999 00000 - 99999 000000 - 999999 0000000 - 9999999 00000000 - 99999999 000000000 - 999999999 0000000000 - 9999999999

Outbound Dialer

SIP Dialer Name	Enable	Unified CCE Pheripheral Name	Hangup Delay (1 - 10)	Port Throttle
SIP_DIALER1	Yes	CUCM_PG_1	1 sec	10.0
SIP_DIALER	Yes	CUCM_PG_1	1 sec	10.0

Base Configuration Parameters for 4000 Agent Deployment

Unified CCE Instance Explorer

Name	Type	Network VRU
HCS for CC	Standard	CVP_Network_VRU
hcs	Standard	CVP_Network_VRU

Agent Desk Settings List

Name	Ring No Answer Time	Logout Non-activity Time	Maximum Wrap Up Time
Default_Agent_Desk_Settings	null	null	7200

PG Explorer

Peripheral Gateway	Type of PIM	Routing Client Name
Unified Communication Manager PG1	CUCM	CUCMPG1
Unified Communication Manager PG2	CUCM	CUCMPG2

Peripheral Gateway	Type of PIM	Routing Client Name
Unified Voice Response (VRU) PG1	VRU	CVPRC01 and CVPRC02
Unified Voice Response (VRU) PG2	VRU	CVPRC03 and CVPRC04
Media Routing (MR) PG 1	MediaRouting	Multichannel1
	MediaRouting	Outbound1
	MediaRouting	SocialMiner1
Media Routing (MR) PG 2	MediaRouting	Multichannel2
	MediaRouting	Outbound2
	MediaRouting	SocialMiner2

Network VRU Explorer

Name	Type	Network VRU Label	Routing Client Name
CVP_Network_VRU	Type10	7777777777	CVPRC01
		7777777777	CVPRC02
		7777777777	CVPRC03
		7777777777	CVPRC04
		8881111000	CUCMPG1
		8881111000	CUCMPG2
		6661111000	Outbound1
		6661111000	Outbound2
MR_Network_VRU_Type2	Type 2	-	-

Network VRU Mapping

- All Unified CVP routing clients are mapped to **CVP_Network_VRU** of **Type10**. This is displayed in the **Advanced** tab of the PG Explorer.
- All Media Routing clients are mapped to **MR_Network_VRU_Type2** of **Type2**. This is displayed in the **Advanced** tab of the PG Explorer.

Network VRU Script List

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
VXML_Server	Type 10 CVP VRU	GS, Server, V	180	__	HCS for CC	Unchecked	Unchecked
VXML_Server_ Interruptible	Type 10 CVP VRU	GS, Server, V, interrupt	9000	__	HCS for CC	Checked	Unchecked
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS, Server, V , nointerrupt	9000	__	HCS for CC	Unchecked	Unchecked
AgentGreeting	Type 10 CVP VRU	PM, -a	180	none	HCS for CC	Unchecked	Unchecked
GreetingMenu _1_to_9	Type 10 CVP VRU	M, press _1_thru_9 _greeting, A	180	1-9	HCS for CC	Checked	Unchecked
Greeting SubMenu	Type 10 CVP VRU	M, press1-press2-press3,A	180	1-3	HCS for CC	Checked	Unchecked
Greeting _Not_Found	Type10 CVP VRU	PM, no _greeting _recorded, A	180	Y	HCS for CC	Checked	Unchecked
GreetingReview	Type10 CVP VRU	PM,-a,A	180	Y	HCS for CC	Checked	Unchecked
T10_GS_AUDIUM	Type 10 CVP VRU	GS,Server,V, FTP	180	,,,,,,,,,Y	HCS for CC	Checked	Unchecked
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	HCS for CC	Unchecked	Unchecked

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
VXML_Server	Type 10 CVP VRU	GS, Server, V	180	__	hcs	Unchecked	Unchecked
VXML_Server_ Interruptible	Type 10 CVP VRU	GS, Server, V, interrupt	9000	__	hcs	Checked	Unchecked

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS, Server, V , nointerrupt	9000	__	hcs	Unchecked	Unchecked
AgentGreeting	Type 10 CVP VRU	PM, -a	180	none	hcs	Unchecked	Unchecked
GreetingMenu _1_to_9	Type 10 CVP VRU	M, press _1_thru_9 _greeting, A	180	1-9	hcs	Checked	Unchecked
Greeting SubMenu	Type 10 CVP VRU	M, press1-press2-press3,A	180	1-3	hcs	Checked	Unchecked
Greeting _Not_Found	Type10 CVP VRU	PM, no _greeting _recorded, A	180	Y	hcs	Checked	Unchecked
GreetingReview	Type10 CVP VRU	PM,-a,A	180	Y	hcs	Checked	Unchecked
T10_GS_AUDIUM	Type 10 CVP VRU	GS,Server,V, FTP	180	,,,,,,,,,Y	hcs	Checked	Unchecked
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	hcs	Unchecked	Unchecked

Application Instance List

Application Instance	Name	Application Type	Permission Level	Application Key
Multichannel	MultiChannel	Other	Full read/write	cisco123
CCDM	CCDM	Cisco Voice	Full read/write	cisco123

Application Path List

Application Instance	Name	Peripheral Gateway	Application Path List	
			Peripheral	Media Routing Domain
UQ.Desktop	5000.UQ.Desktop	CUCM_PG1	CUCM_PG_1	SocialMiner_Task

Application Instance	Name	Peripheral Gateway	Application Path List	
UQ.Desktop	5001.UQ.Desktop	CUCM_PG2	CUCM_PG_2	SocialMiner_Task

Media Class List

Name	Description	Life	Start Timeout	Max Duration
Cisco_Chat	System provided media class for Cisco chat	1200	30	28800
Cisco_Task	System provided media class for Cisco Task	1200	30	28800
Cisco_Voice	Default value for Cisco Voice	0	0	0
CIM_BC	-	300	30	28800
ECE_Chat	-	300	30	28800
ECE_Email	-	300	30	28800
ECE_Outbound	-	300	30	28800

Media Routing Domain List

	Interruptible	Calls in Queue (Max)	Max per call type	Max time in queue
Cisco_BC	Unchecked	5000	-	-
ECE_Email	Checked	15000	-	-
ECE_Outbound	Checked	5000	-	-
ECE_Chat	Unchecked	5000	-	-
SocialMiner_Task	Unchecked	-	-	-
Cisco_Voice	Unchecked	As per your requirement	-	-

Note Set the **Max Per Call Type** and **Max Time in Queue** values as per your requirement.

Expanded Call Variable List

Note ECC variables will not be enabled by default. Use Unified CCE Configuration manager tool to enable the required ECC variables under the **Expanded Call Variable List**.

Name	Enabled	Persistent	Maximum Length	Description
user.CourtesyCallbackEnabled	FALSE	FALSE	1	Determines if Courtesy Callback is offered to a caller.
user.cvp_server_info	FALSE	FALSE	15	Used by Unified CVP to send the IP address of the Call Server sending the request to Unified CCE.
user.microapp.app_media_lib	FALSE	FALSE	210	Directory for all application-specific media files and grammar files. The **..** bypasses the user. When writing a URL path, microapp.app_media_lib and user.microapp.locale are the ECC variables.
user.microapp.caller_input	FALSE	FALSE	210	Storage area for an ASR input that is collected from Get Speech. **Note** Get Speech results are written to the ECC variable. Results from Get Digits or Menu microapplications are written to the CED.
user.microapp.currency	FALSE	FALSE	6	Currency type.
user.microapp.error_code	FALSE	FALSE	2	Error status code returned from Unified CVP to Unified CCE when the Run Script Result is False.
user.microapp.FromExtVXML	FALSE	FALSE	60	This variable array returns information from the external VoiceXML file. Must be configured as array variables, not Scalar Variables, and array length set to 4.
user.microapp.input_type	FALSE	FALSE	1	Specifies the type of input that is allowed. Valid contents are: D(DTMF) and B (Both DTMF and Voice). B is the default. If you are not using an ASR, set this variable to D. If you are using an ASR, you can set this variable to either D or B.
user.microapp.locale	FALSE	FALSE	5	Combination of language and country that defines the grammar and prompt set to use.

Name	Enabled	Persistent	Maximum Length	Description
user.microapp.metadata	FALSE	FALSE	62	Following the Menu (M), Get Data (GD) and Get Speech (GS) micro-applications, Unified CVP now returns information about the execution of that micro-application.
user.microapp.play_data	FALSE	FALSE	40	Default storage area for data for Play Data micro-applications.
user.microapp.sys_media_lib	FALSE	FALSE	10	Directory for all systems media files, such as individual digits, months, default error messages, and so forth.
user.microapp.ToExtVXML	FALSE	FALSE	60	This variable array sends information to the external VoiceXML file. Must be configured as Array variables, not Scalar Variables and array length set to 4.
user.microapp.UseVXMLParams	FALSE	FALSE	1	Specifies the manner in which you pass the information to the external VoiceXML.
user.microapp.isPostCallSurvey	FALSE	FALSE	1	Used to determine if post call survey should be offered to a caller after the agent disconnects the call.
user.ece.activity.id	FALSE	FALSE	30	Needed for all types of WIM and EIM activities.
user.ece.customer.name	FALSE	FALSE	30	Needed for chat, callback, and delayed callback activities.
user.media.id	FALSE	FALSE	36	A number identifying a call to the Unified CCE Service, optionally, the H.323 Service.
user.microapp.grammar_choices	FALSE	FALSE	210	Specifies the ASR choices that a caller can input for the Get Speech micro-application.
user.microapp.inline_tts	FALSE	FALSE	210	Specifies the text for inline Text To Speech (TTS).
user.microapp.media_server	FALSE	FALSE	60	Root of the URL for all media files and external grammar files used in the script.
user.microapp.override_cli	FALSE	FALSE	200	Used by the system to override the CLI field on outgoing transfers.
user.microapp.pd_tts	FALSE	FALSE	1	Specifies whether Unifies Text To Speech or media files must be played to the caller.

System Information

- Expanded Call Context: Enabled
- Minimum Correlation number: 1001
- Maximum Correlation number: 9999
- Retain script versions:5

Agent Targeting Rule

Attribute		
Name	AgentExtension1	AgentExtension2
Peripheral	CUCM_PG_1	CUCM_PG_2
Rule Type Agent Extension	Agent Extension	Agent Extension
Routing Client	All routing clients	All routing clients
Extension Range	000 - 999	000 - 999
	0000 - 9999	0000 - 9999
	00000 - 99999	00000 - 99999
	000000 - 999999	000000 - 999999
	0000000 - 9999999	0000000 - 9999999
	00000000 - 99999999	00000000 - 99999999
	000000000 - 999999999	000000000 - 999999999
	0000000000 - 9999999999	0000000000 - 9999999999

Outbound Dialer

SIP Dialer Name	Enable	Unified CCE Pheripheral Name	Hangup Delay (1 - 10)	Port Throttle
SIP_DIALER1	Yes	CUCM_PG_1	1 sec	10.0
SIP_DIALER2	Yes	CUCM_PG_2	1 sec	10.0

Base Configuration Parameters for 12000 Agent Deployment

Unified CCE Instance Explorer

Name	Type	Network VRU
HCS for CC	Standard	CVP_Network_VRU
hcs	Standard	CVP_Network_VRU

Agent Desk Settings List

Name	Ring No Answer Time	Logout Non-activity Time	Maximum Wrap Up Time
Default_Agent_Desk_Settings	null	null	7200

PG Explorer

Peripheral Gateway	Type of PIM	Routing Client Names
Unified CommunicationManager PG1	CUCM	CUCMPG1
Unified CommunicationManager PG2	CUCM	CUCMPG2
Unified CommunicationManager PG3	CUCM	CUCMPG3
Unified CommunicationManager PG4	CUCM	CUCMPG4
Unified CommunicationManager PG5	CUCM	CUCMPG5
Unified CommunicationManager PG6	CUCM	CUCMPG6
Unified Voice Response (VRU) PG1	VRU	CVPRC01 and CVPRC02
Unified Voice Response (VRU) PG2	VRU	CVPRC03 and CVPRC04
Unified Voice Response (VRU) PG3	VRU	CVPRC05 and CVPRC06
Unified Voice Response (VRU) PG4	VRU	CVPRC07 and CVPRC08
Unified Voice Response (VRU) PG5	VRU	CVPRC09 and CVPRC10
Unified Voice Response (VRU) PG6	VRU	CVPRC11 and CVPRC12
Media Routing (MR) PG 1	MediaRouting	Multichannel1
	MediaRouting	Outbound1
	MediaRouting	SocialMiner1

Peripheral Gateway	Type of PIM	Routing Client Names
Media Routing (MR) PG 2	MediaRouting	Multichannel2
	MediaRouting	Outbound2
	MediaRouting	SocialMiner2
Media Routing (MR) PG 3	MediaRouting	Multichannel3
	MediaRouting	Outbound3
	MediaRouting	SocialMiner3
Media Routing (MR) PG 4	MediaRouting	Multichannel4
	MediaRouting	Outbound4
	MediaRouting	SocialMiner4
Media Routing (MR) PG 5	MediaRouting	Multichannel5
	MediaRouting	Outbound5
	MediaRouting	SocialMiner5
Media Routing (MR) PG 6	MediaRouting	Multichannel6
	MediaRouting	Outbound6
	MediaRouting	SocialMiner6

Network VRU Explorer

Name	Type	Network VRU Label	Routing Client Name
CVP Network VRU	Type 10	7777777777	CVPRC01, CVPRC02 ... CVPRC12
		8881111000	CUCMPG1, CUCMPG2 ... CUCMPG6
		6661111000	Outbound1, Outbound2 ... Outbound6
MR_Network_VRU_Type2	Type 2	-	-

Network VRU Mapping

- All Unified CVP routing clients are mapped to **CVP_Network_VRU** of **Type10**. This is displayed in the **Advanced** tab of the PG Explorer.

- All Media Routing clients are mapped to **MR_Network_VRU_Type2** of **Type2**. This is displayed in the **Advanced** tab of the PG Explorer.

Network VRU Script List

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
VXML_Server	Type 10 CVP VRU	GS, Server, V	180	__	HCS for CC	Unchecked	Unchecked
VXML_Server_ Interruptible	Type 10 CVP VRU	GS, Server, V, interrupt	9000	__	HCS for CC	Checked	Unchecked
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS, Server, V , nointerrupt	9000	__	HCS for CC	Unchecked	Unchecked
AgentGreeting	Type 10 CVP VRU	PM, -a	180	none	HCS for CC	Unchecked	Unchecked
GreetingMenu _1_to_9	Type 10 CVP VRU	M, press _1_thru_9 _greeting, A	180	1-9	HCS for CC	Checked	Unchecked
Greeting SubMenu	Type 10 CVP VRU	M, press1-press2-press3,A	180	1-3	HCS for CC	Checked	Unchecked
Greeting _Not_Found	Type10 CVP VRU	PM, no _greeting _recorded, A	180	Y	HCS for CC	Checked	Unchecked
GreetingReview	Type10 CVP VRU	PM,-a,A	180	Y	HCS for CC	Checked	Unchecked
T10_GS_AUDIUM	Type 10 CVP VRU	GS,Server,V, FTP	180	,,,,,,,,,Y	HCS for CC	Checked	Unchecked
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	HCS for CC	Unchecked	Unchecked

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
VXML_Server	Type 10 CVP VRU	GS, Server, V	180	__	hcs	Unchecked	Unchecked
VXML_Server_ Interruptible	Type 10 CVP VRU	GS, Server, V, interrupt	9000	__	hcs	Checked	Unchecked
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS, Server, V , nointerrupt	9000	__	hcs	Unchecked	Unchecked
AgentGreeting	Type 10 CVP VRU	PM, -a	180	none	hcs	Unchecked	Unchecked
GreetingMenu _1_to_9	Type 10 CVP VRU	M, press _1_thru_9 _greeting, A	180	1-9	hcs	Checked	Unchecked
Greeting SubMenu	Type 10 CVP VRU	M, press1-press2-press3,A	180	1-3	hcs	Checked	Unchecked
Greeting _Not_Found	Type10 CVP VRU	PM, no _greeting _recorded, A	180	Y	hcs	Checked	Unchecked
GreetingReview	Type10 CVP VRU	PM,-a,A	180	Y	hcs	Checked	Unchecked
T10_GS_AUDIUM	Type 10 CVP VRU	GS,Server,V, FTP	180	,,,,,,,,,,Y	hcs	Checked	Unchecked
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	hcs	Unchecked	Unchecked

Application Instance List

Application Instance	Name	Application Type	Permission Level	Application Key
Multichannel	MultiChannel	Other	Full read/write	cisco123
CCDM	CCDM	Cisco Voice	Full read/write	cisco123

Application Path List

Application Instance	Name	Peripheral Gateway	Application Path List	
			Peripheral	Media Routing Domain
UQ.Desktop	5000.UQ.Desktop	CUCM_PG1	CUCM_PG_1	SocialMiner_Task
UQ.Desktop	5001.UQ.Desktop	CUCM_PG2	CUCM_PG_2	SocialMiner_Task
UQ.Desktop	5002.UQ.Desktop	CUCM_PG3	CUCM_PG_3	SocialMiner_Task
UQ.Desktop	5003.UQ.Desktop	CUCM_PG4	CUCM_PG_4	SocialMiner_Task
UQ.Desktop	5004.UQ.Desktop	CUCM_PG5	CUCM_PG_5	SocialMiner_Task
UQ.Desktop	5005.UQ.Desktop	CUCM_PG6	CUCM_PG_6	SocialMiner_Task

Media Class List

Name	Description	Life	Start Timeout	Max Duration
Cisco_Chat	System provided media class for Cisco chat	1200	30	28800
Cisco_Task	System provided media class for Cisco Task	1200	30	28800
Cisco_Voice	Default value for Cisco Voice	0	0	0
CIM_BC	-	300	30	28800
ECE_Chat	-	300	30	28800
ECE_Email	-	300	30	28800
ECE_Outbound	-	300	30	28800

Media Routing Domain List

	Interruptible	Calls in Queue (Max)	Max per call type	Max time in queue
Cisco_BC	Unchecked	5000	-	-
ECE_Email	Checked	15000	-	-
ECE_Outbound	Checked	5000	-	-
ECE_Chat	Unchecked	5000	-	-
SocialMiner_Task	Unchecked	-	-	-

	Interruptible	Calls in Queue (Max)	Max per call type	Max time in queue
Cisco_Voice	Unchecked	As per your requirement	-	-

Note Set the **Max Per Call Type** and **Max Time in Queue** values as per your requirement.

Expanded Call Variable List

Note ECC variables will not be enabled by default. Use Unified CCE Configuration manager tool to enable the required ECC variables under the **Expanded Call Variable List**.

Name	Enabled	Persistent	Maximum Length	Description
user.CourtesyCallbackEnabled	FALSE	FALSE	1	Determines if Courtesy Callback is offered to a caller.
user.cvp_server_info	FALSE	FALSE	15	Used by Unified CVP to send the IP address of the Call Server sending the request to Unified CCE.
user.microapp.app_media_lib	FALSE	FALSE	210	Directory for all application-specific media files and grammar files. The **..** bypasses the user. When writing a URL path, microapp.app_media_lib and user.microapp.locale are the ECC variables.
user.microapp.caller_input	FALSE	FALSE	210	Storage area for an ASR input that is collected from Get Speech. **Note** Get Speech results are written to the ECC variable. Results from Get Digits or Menu microapplications are written to the CED.
user.microapp.currency	FALSE	FALSE	6	Currency type.
user.microapp.error_code	FALSE	FALSE	2	Error status code returned from Unified CVP to Unified CCE when the Run Script Result is False.

Name	Enabled	Persistent	Maximum Length	Description
user.microapp.FromExtVXML	FALSE	FALSE	60	This variable array returns information from the external VoiceXML file. Must be configured as array variables, not Scalar Variables, and array length set to 4.
user.microapp.input_type	FALSE	FALSE	1	Specifies the type of input that is allowed. Valid contents are: D(DTMF) and B (Both DTMF and Voice). B is the default. If you are not using an ASR, set this variable to D. If you are using an ASR, you can set this variable to either D or B.
user.microapp.locale	FALSE	FALSE	5	Combination of language and country that defines the grammar and prompt set to use.
user.microapp.metadata	FALSE	FALSE	62	Following the Menu (M), Get Data (GD) and Get Speech (GS) micro-applications, Unified CVP now returns information about the execution of that micro-application.
user.microapp.play_data	FALSE	FALSE	40	Default storage area for data for Play Data micro-applications.
user.microapp.sys_media_lib	FALSE	FALSE	10	Directory for all systems media files, such as individual digits, months, default error messages, and so forth.
user.microapp.ToExtVXML	FALSE	FALSE	60	This variable array sends information to the external VoiceXML file. Must be configured as Array variables, not Scalar Variables and array length set to 4.
user.microapp.UseVXMLParams	FALSE	FALSE	1	Specifies the manner in which you pass the information to the external VoiceXML.
user.microapp.isPostCallSurvey	FALSE	FALSE	1	Used to determine if post call survey should be offered to a caller after the agent disconnects the call.
user.ece.activity.id	FALSE	FALSE	30	Needed for all types of WIM and EIM activities.
user.ece.customer.name	FALSE	FALSE	30	Needed for chat, callback, and delayed callback activities.

Name	Enabled	Persistent	Maximum Length	Description
user.media.id	FALSE	FALSE	36	A number identifying a call to the Unified CCE Service, optionally, the H.323 Service.
user.microapp.grammar_choices	FALSE	FALSE	210	Specifies the ASR choices that a caller can input for the Get Speech micro-application.
user.microapp.inline_tts	FALSE	FALSE	210	Specifies the text for inline Text To Speech (TTS).
user.microapp.media_server	FALSE	FALSE	60	Root of the URL for all media files and external grammar files used in the script.
user.microapp.override_cli	FALSE	FALSE	200	Used by the system to override the CLI field on outgoing transfers.
user.microapp.pd_tts	FALSE	FALSE	1	Specifies whether Unifies Text To Speech or media files must be played to the caller.

System Information

- Expanded Call Context: Enabled
- Minimum Correlation number: 1001
- Maximum Correlation number: 9999
- Retain script versions:5

Agent Targeting Rule

Attribute	
Name	AgentExtension1, AgentExtension2 … AgentExtension6
Peripheral	CUCM_PG_1, CUCM_PG_2 … CUCM_PG_6
Rule Type Agent Extension	Agent Extension
Routing Client	All routing clients

Attribute	
Extension Range	000 - 999 0000 - 9999 00000 - 99999 000000 - 999999 0000000 - 9999999 00000000 - 99999999 000000000 - 999999999 0000000000 - 9999999999

Outbound Dialer

SIP Dialer Name	Enable	Unified CCE Pheripheral Name	Hangup Delay (1 - 10)	Port Throttle
SIP_DIALER1	Yes	CUCM_PG_1	1 sec	10.0
SIP_DIALER2	Yes	CUCM_PG_2	1 sec	10.0
SIP_DIALER3	Yes	CUCM_PG_3	1 sec	10.0
SIP_DIALER4	Yes	CUCM_PG_4	1 sec	10.0
SIP_DIALER5	Yes	CUCM_PG_5	1 sec	10.0
SIP_DIALER6	Yes	CUCM_PG_6	1 sec	10.0

Base Configuration Parameters for 24000 Agent Deployment

Unified CCE Instance Explorer

Name	Type	Network VRU
HCS for CC	Standard	CVP_Network_VRU
hcs	Standard	CVP_Network_VRU

Agent Desk Settings List

Name	Ring No Answer Time	Logout Non-activity Time	Maximum Wrap Up Time
Default_Agent_Desk_Settings	null	null	7200

PG Explorer

Peripheral Gateway	Type of PIM	Routing Client Names
Unified CommunicationManager PG1	CUCM	CUCMPG1
Unified CommunicationManager PG2	CUCM	CUCMPG2
Unified CommunicationManager PG3	CUCM	CUCMPG3
Unified CommunicationManager PG4	CUCM	CUCMPG4
Unified CommunicationManager PG5	CUCM	CUCMPG5
Unified CommunicationManager PG6	CUCM	CUCMPG6
Unified CommunicationManager PG7	CUCM	CUCMPG7
Unified CommunicationManager PG8	CUCM	CUCMPG8
Unified CommunicationManager PG9	CUCM	CUCMPG9
Unified CommunicationManager PG10	CUCM	CUCMPG10
Unified CommunicationManager PG11	CUCM	CUCMPG11
Unified CommunicationManager PG12	CUCM	CUCMPG12
Unified Voice Response (VRU) PG1	VRU	CVPRC01 and CVPRC02
Unified Voice Response (VRU) PG2	VRU	CVPRC03 and CVPRC04
Unified Voice Response (VRU) PG3	VRU	CVPRC05 and CVPRC06
Unified Voice Response (VRU) PG4	VRU	CVPRC07 and CVPRC08
Unified Voice Response (VRU) PG5	VRU	CVPRC09 and CVPRC10

Peripheral Gateway	Type of PIM	Routing Client Names
Unified Voice Response (VRU) PG6	VRU	CVPRC11 and CVPRC12
Unified Voice Response (VRU) PG7	VRU	CVPRC13 and CVPRC15
Unified Voice Response (VRU) PG8	VRU	CVPRC15 and CVPRC16
Unified Voice Response (VRU) PG9	VRU	CVPRC17 and CVPRC18
Unified Voice Response (VRU) PG10	VRU	CVPRC19 and CVPRC20
Unified Voice Response (VRU) PG11	VRU	CVPRC21 and CVPRC22
Unified Voice Response (VRU) PG12	VRU	CVPRC23 and CVPRC24
Media Routing (MR) PG 1	MediaRouting	Multichannel1
	MediaRouting	Outbound1
	MediaRouting	SocialMiner1
Media Routing (MR) PG 2	MediaRouting	Multichannel2
	MediaRouting	Outbound2
	MediaRouting	SocialMiner2
Media Routing (MR) PG 3	MediaRouting	Multichannel3
	MediaRouting	Outbound3
	MediaRouting	SocialMiner3
Media Routing (MR) PG 4	MediaRouting	Multichannel4
	MediaRouting	Outbound4
	MediaRouting	SocialMiner4
Media Routing (MR) PG 5	MediaRouting	Multichannel5
	MediaRouting	Outbound5
	MediaRouting	SocialMiner5

Peripheral Gateway	Type of PIM	Routing Client Names
Media Routing (MR) PG 6	MediaRouting	Multichannel6
	MediaRouting	Outbound6
	MediaRouting	SocialMiner6
Media Routing (MR) PG 7	MediaRouting	Multichannel7
	MediaRouting	Outbound7
	MediaRouting	SocialMiner7
Media Routing (MR) PG 8	MediaRouting	Multichannel8
	MediaRouting	Outbound8
	MediaRouting	SocialMiner8
Media Routing (MR) PG 9	MediaRouting	Multichannel9
	MediaRouting	SocialMiner9
	MediaRouting	Outbound9
Media Routing (MR) PG 10	MediaRouting	Multichannel10
	MediaRouting	Outbound10
	MediaRouting	SocialMiner10
Media Routing (MR) PG 11	MediaRouting	Multichannel11
	MediaRouting	Outbound11
	MediaRouting	SocialMiner11
Media Routing (MR) PG 12	MediaRouting	Multichannel12
	MediaRouting	Outbound12
	MediaRouting	SocialMiner12

Network VRU Explorer

Name	Type	Network VRU Label	Routing Client Name
CVP Network VRU	Type 10	7777777777	CVPRC01, CVPRC02 ... CVPRC24
		8881111000	CUCMPG1, CUCMPG2 ... CUCMPG12

Name	Type	Network VRU Label	Routing Client Name
		6661111000	Outbound1, Outbound2 ... Outbound12
MR_Network_VRU_Type2	Type 2	-	-

Network VRU Mapping

- All Unified CVP routing clients are mapped to **CVP_Network_VRU** of **Type10**. This is displayed in the **Advanced** tab of the PG Explorer.
- All Media Routing clients are mapped to **MR_Network_VRU_Type2** of **Type2**. This is displayed in the **Advanced** tab of the PG Explorer.

Network VRU Script List

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
Greeting SubMenu	Type 10 CVP VRU	M, press1-press2-press3,A	180	1-3	HCS for CC	Checked	Unchecked
Greeting _Not_Found	Type10 CVP VRU	PM, no _greeting _recorded, A	180	Y	HCS for CC	Checked	Unchecked
GreetingReview	Type10 CVP VRU	PM,-a,A	180	Y	HCS for CC	Checked	Unchecked
T10_GS_AUDIUM	Type 10 CVP VRU	GS,Server,V, FTP	180	,,,,,,,,,,Y	HCS for CC	Checked	Unchecked
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	HCS for CC	Unchecked	Unchecked
VXML_Server	Type 10 CVP VRU	GS, Server, V	180	__	HCS for CC	Unchecked	Unchecked
VXML_Server_ Interruptible	Type 10 CVP VRU	GS, Server, V, interrupt	9000	__	HCS for CC	Checked	Unchecked
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS, Server, V , nointerrupt	9000	__	HCS for CC	Unchecked	Unchecked
AgentGreeting	Type 10 CVP VRU	PM, -a	180	none	HCS for CC	Unchecked	Unchecked

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
GreetingMenu _1_to_9	Type 10 CVP VRU	M, press _1_thru_9 _greeting, A	180	1-9	HCS for CC	Checked	Unchecked

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
Greeting SubMenu	Type 10 CVP VRU	M, press1-press2-press3,A	180	1-3	hcs	Checked	Unchecked
Greeting _Not_Found	Type10 CVP VRU	PM, no _greeting _recorded, A	180	Y	hcs	Checked	Unchecked
GreetingReview	Type10 CVP VRU	PM,-a,A	180	Y	hcs	Checked	Unchecked
T10_GS_AUDIUM	Type 10 CVP VRU	GS,Server,V, FTP	180	,,,,,,,,,,Y	hcs	Checked	Unchecked
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	hcs	Unchecked	Unchecked
VXML_Server	Type 10 CVP VRU	GS, Server, V	180	__	hcs	Unchecked	Unchecked
VXML_Server_ Interruptible	Type 10 CVP VRU	GS, Server, V, interrupt	9000	__	hcs	Checked	Unchecked
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS, Server, V , nointerrupt	9000	__	hcs	Unchecked	Unchecked
AgentGreeting	Type 10 CVP VRU	PM, -a	180	none	hcs	Unchecked	Unchecked
GreetingMenu _1_to_9	Type 10 CVP VRU	M, press _1_thru_9 _greeting, A	180	1-9	hcs	Checked	Unchecked

Application Instance List

Application Instance	Name	Application Type	Permission Level	Application Key
Multichannel	MultiChannel	Other	Full read/write	cisco123
CCDM	CCDM	Cisco Voice	Full read/write	cisco123

Application Path List

Application Instance	Name	Peripheral Gateway	Application Path List	
			Peripheral	Media Routing Domain
UQ.Desktop	5000.UQ.Desktop	CUCM_PG1	CUCM_PG_1	SocialMiner_Task
UQ.Desktop	5001.UQ.Desktop	CUCM_PG2	CUCM_PG_2	SocialMiner_Task
UQ.Desktop	5002.UQ.Desktop	CUCM_PG3	CUCM_PG_3	SocialMiner_Task
UQ.Desktop	5003.UQ.Desktop	CUCM_PG4	CUCM_PG_4	SocialMiner_Task
UQ.Desktop	5004.UQ.Desktop	CUCM_PG5	CUCM_PG_5	SocialMiner_Task
UQ.Desktop	5005.UQ.Desktop	CUCM_PG6	CUCM_PG_6	SocialMiner_Task
UQ.Desktop	5006.UQ.Desktop	CUCM_PG7	CUCM_PG_7	SocialMiner_Task
UQ.Desktop	5007.UQ.Desktop	CUCM_PG8	CUCM_PG_8	SocialMiner_Task
UQ.Desktop	5008.UQ.Desktop	CUCM_PG9	CUCM_PG_9	SocialMiner_Task
UQ.Desktop	5009.UQ.Desktop	CUCM_PG10	CUCM_PG_10	SocialMiner_Task
UQ.Desktop	5010.UQ.Desktop	CUCM_PG11	CUCM_PG_11	SocialMiner_Task
UQ.Desktop	5011.UQ.Desktop	CUCM_PG12	CUCM_PG_12	SocialMiner_Task

Expanded Call Variable List

Note ECC variables will not be enabled by default. Use Unified CCE Configuration manager tool to enable the required ECC variables under the **Expanded Call Variable List**.

Name	Enabled	Persistent	Maximum Length	Description
user.CourtesyCallbackEnabled	FALSE	FALSE	1	Determines if Courtesy Callback is offered to a caller.
user.cvp_server_info	FALSE	FALSE	15	Used by Unified CVP to send the IP address of the Call Server sending the request to Unified CCE.

Name	Enabled	Persistent	Maximum Length	Description
user.microapp.app_media_lib	FALSE	FALSE	210	Directory for all application-specific media files and grammar files. The .. bypasses the user. When writing a URL path, microapp.app_media_lib and user.microapp.locale are the ECC variables.
user.microapp.caller_input	FALSE	FALSE	210	Storage area for an ASR input that is collected from Get Speech. Note Get Speech results are written to the ECC variable. Results from Get Digits or Menu microapplications are written to the CED.
user.microapp.currency	FALSE	FALSE	6	Currency type.
user.microapp.error_code	FALSE	FALSE	2	Error status code returned from Unified CVP to Unified CCE when the Run Script Result is False.
user.microapp.FromExtVXML	FALSE	FALSE	60	This variable array returns information from the external VoiceXML file. Must be configured as array variables, not Scalar Variables, and array length set to 4.
user.microapp.input_type	FALSE	FALSE	1	Specifies the type of input that is allowed. Valid contents are: D(DTMF) and B (Both DTMF and Voice). B is the default. If you are not using an ASR, set this variable to D. If you are using an ASR, you can set this variable to either D or B.
user.microapp.locale	FALSE	FALSE	5	Combination of language and country that defines the grammar and prompt set to use.
user.microapp.metadata	FALSE	FALSE	62	Following the Menu (M), Get Data (GD) and Get Speech (GS) micro-applications, Unified CVP now returns information about the execution of that micro-application.
user.microapp.play_data	FALSE	FALSE	40	Default storage area for data for Play Data micro-applications.
user.microapp.inline_tts	FALSE	FALSE	210	Specifies the text for inline Text To Speech (TTS).

Name	Enabled	Persistent	Maximum Length	Description
user.microapp.media_server	FALSE	FALSE	60	Root of the URL for all media files and external grammar files used in the script.
user.microapp.override_cli	FALSE	FALSE	200	Used by the system to override the CLI field on outgoing transfers.
user.microapp.pd_tts	FALSE	FALSE	1	Specifies whether Unifies Text To Speech or media files must be played to the caller.
user.ece.activity.id	FALSE	FALSE	30	Needed for all types of WIM and EIM activities.
user.ece.customer.name	FALSE	FALSE	30	Needed for chat, callback, and delayed callback activities.
user.media.id	FALSE	FALSE	36	A number identifying a call to the Unified CCE Service, optionally, the H.323 Service.
user.microapp.grammar_choices	FALSE	FALSE	210	Specifies the ASR choices that a caller can input for the Get Speech micro-application.

Media Class List

Name	Description	Life	Start Timeout	Max Duration
Cisco_Chat	System provided media class for Cisco chat	1200	30	28800
Cisco_Task	System provided media class for Cisco Task	1200	30	28800
Cisco_Voice	Default value for Cisco Voice	0	0	0
CIM_BC	-	300	30	28800
ECE_Chat	-	300	30	28800
ECE_Email	-	300	30	28800
ECE_Outbound	-	300	30	28800

Media Routing Domain List

	Interruptible	Calls in Queue (Max)	Max per call type	Max time in queue
Cisco_BC	Unchecked	5000	-	-
ECE_Email	Checked	15000	-	-

	Interruptible	Calls in Queue (Max)	Max per call type	Max time in queue
ECE_Outbound	Checked	5000	-	-
ECE_Chat	Unchecked	5000	-	-
SocialMiner_Task	Unchecked	-	-	-
Cisco_Voice	Unchecked	As per your requirement	-	-

Note Set the **Max Per Call Type** and **Max Time in Queue** values as per your requirement.

System Information

- Expanded Call Context: Enabled
- Minimum Correlation number: 1001
- Maximum Correlation number: 9999
- Retain script versions:5

Agent Targeting Rule

Attribute	
Name	AgentExtension1, AgentExtension2 … AgentExtension6
Peripheral	CUCM_PG_1, CUCM_PG_2 … CUCM_PG_12
Rule Type Agent Extension	Agent Extension
Routing Client	All routing clients
Extension Range	000 - 999 0000 - 9999 00000 - 99999 000000 - 999999 0000000 - 9999999 00000000 - 99999999 000000000 - 999999999 0000000000 - 9999999999

Outbound Dialer

SIP Dialer Name	Enable	Unified CCE Pheripheral Name	Hangup Delay (1 - 10)	Port Throttle
SIP_DIALER1	Yes	CUCM_PG_1	1 sec	10.0
SIP_DIALER2	Yes	CUCM_PG_2	1 sec	10.0
SIP_DIALER3	Yes	CUCM_PG_3	1 sec	10.0
SIP_DIALER4	Yes	CUCM_PG_4	1 sec	10.0
SIP_DIALER5	Yes	CUCM_PG_5	1 sec	10.0
SIP_DIALER6	Yes	CUCM_PG_6	1 sec	10.0
SIP_DIALER7	Yes	CUCM_PG_7	1 sec	10.0
SIP_DIALER8	Yes	CUCM_PG_8	1 sec	10.0
SIP_DIALER9	Yes	CUCM_PG_9	1 sec	10.0
SIP_DIALER10	Yes	CUCM_PG_10	1 sec	10.0
SIP_DIALER11	Yes	CUCM_PG_11	1 sec	10.0
SIP_DIALER12	Yes	CUCM_PG_12	1 sec	10.0

Base Configuration Parameters for Small Contact Center Agent Deployment

Unified CCE Instance Explorer

Name	Type	Network VRU
HCS for CC	Standard	CVP_Network_VRU
hcs	Standard	CVP_Network_VRU

Agent Desk Settings List

Name	Ring No Answer Time	Logout Non-activity Time	Maximum Wrap Up Time
Default_Agent_Desk_Settings	null	null	7200

PG Explorer

Peripheral Gateway	Type of PIM	Routing client Name
Unified Communication Manager PG1	CUCM	CUCMPG1

Peripheral Gateway	Type of PIM	Routing client Name
Unified Voice Response (VRU) PG	VRU	CVPRC01
	VRU	CVPRC02
	VRU	CVPRC03
	VRU	CVPRC04

Network VRU Explorer

Name	Type	Network VRU Label	Routing Client Name
CVP Network VRU	Type 10	7777777777	CVPRC01
		7777777777	CVPRC02
		7777777777	CVPRC03
		7777777777	CVPRC04
		8881111000	CUCMPG1
MR_Network_VRU	Type 2	-	-

Network VRU Mapping

All Unified CVP routing clients are mapped to **CVP_Network_VRU** of **Type10**. This is displayed in the **Advanced** tab of the PG Explorer.

Network VRU Script List

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
VXML_Server	Type 10 CVP VRU	GS, Server, V	180	__	HCS for CC	Unchecked	Unchecked
VXML_Server_ Interruptible	Type 10 CVP VRU	GS, Server, V, interrupt	9000	__	HCS for CC	Checked	Unchecked
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS, Server, V , nointerrupt	9000	__	HCS for CC	Unchecked	Unchecked
AgentGreeting	Type 10 CVP VRU	PM, -a	180	none	HCS for CC	Unchecked	Unchecked
GreetingMenu _1_to_9	Type 10 CVP VRU	M, press _1_thru_9 _greeting, A	180	1-9	HCS for CC	Checked	Unchecked

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
Greeting SubMenu	Type 10 CVP VRU	M, press1-press2-press3,A	180	1-3	HCS for CC	Checked	Unchecked
Greeting _Not_Found	Type10 CVP VRU	PM, no _greeting _recorded, A	180	Y	HCS for CC	Checked	Unchecked
GreetingReview	Type10 CVP VRU	PM,-a,A	180	Y	HCS for CC	Checked	Unchecked
T10_GS_AUDIUM	Type 10 CVP VRU	GS,Server,V, FTP	180	,,,,,,,,,Y	HCS for CC	Checked	Unchecked
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	HCS for CC	Unchecked	Unchecked

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
VXML_Server	Type 10 CVP VRU	GS, Server, V	180	__	hcs	Unchecked	Unchecked
VXML_Server_ Interruptible	Type 10 CVP VRU	GS, Server, V, interrupt	9000	__	hcs	Checked	Unchecked
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS, Server, V , nointerrupt	9000	__	hcs	Unchecked	Unchecked
AgentGreeting	Type 10 CVP VRU	PM, -a	180	none	hcs	Unchecked	Unchecked
GreetingMenu _1_to_9	Type 10 CVP VRU	M, press _1_thru_9 _greeting, A	180	1-9	hcs	Checked	Unchecked
Greeting SubMenu	Type 10 CVP VRU	M, press1-press2-press3,A	180	1-3	hcs	Checked	Unchecked

Name	Network VRU	VRU Script Name	Time out (Sec)	Configuration Parameter	Customer	Interruptible	Override
Greeting _Not_Found	Type10 CVP VRU	PM, no _greeting _recorded, A	180	Y	hcs	Checked	Unchecked
GreetingReview	Type10 CVP VRU	PM,-a,A	180	Y	hcs	Checked	Unchecked
T10_GS_AUDIUM	Type 10 CVP VRU	GS,Server,V, FTP	180	,,,,,,,,,Y	hcs	Checked	Unchecked
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	hcs	Unchecked	Unchecked

Application Instance List

Application Instance	Name	Application Type	Permission Level	Application Key
Multichannel	MultiChannel	Other	Full read/write	cisco123
CCDM	CCDM	Cisco Voice	Full read/write	cisco123

Application Path List

Application Instance	Name	Peripheral Gateway	Application Path List members	
UQ.Desktop	5000.UQ.Desktop	CUCM_PG	**Peripheral**	**Media Routing Domain**
			CUCM_PG_1	SocialMiner_Task

Media Class List

Name	Description	Life	Start Timeout	Max Duration
Cisco_Chat	System provided media class for Cisco chat	1200	30	28800
Cisco_Task	System provided media class for Cisco Task	1200	30	28800
Cisco_Voice	Default value for Cisco Voice	0	0	0
CIM_BC	-	300	30	28800
ECE_Chat	-	300	30	28800

Name	Description	Life	Start Timeout	Max Duration
ECE_Email	-	300	30	28800
ECE_Outbound	-	300	30	28800

Media Routing Domain List

	Interruptible	Calls in Queue (Max)	Max per call type	Max time in queue
Cisco_BC	Unchecked	5000	-	-
ECE_Email	Checked	15000	-	-
ECE_Outbound	Checked	5000	-	-
ECE_Chat	Unchecked	5000	-	-
SocialMiner_Task	Unchecked	-	-	-
Cisco_Voice	Unchecked	As per your requirement	-	-

Note Set the **Max Per Call Type** and **Max Time in Queue** values as per your requirement.

Expanded Call Variable List

Note ECC variables will not be enabled by default. Use Unified CCE Configuration manager tool to enable the required ECC variables under the **Expanded Call Variable List**.

Name	Enabled	Persistent	Maximum Length	Description
user.CourtesyCallbackEnabled	FALSE	FALSE	1	Determines if Courtesy Callback is offered to a caller.
user.cvp_server_info	FALSE	FALSE	15	Used by Unified CVP to send the IP address of the Call Server sending the request to Unified CCE.
user.microapp.app_media_lib	FALSE	FALSE	210	Directory for all application-specific media files and grammar files. The **..** bypasses the user. When writing a URL path, microapp.app_media_lib and user.microapp.locale are the ECC variables.

Name	Enabled	Persistent	Maximum Length	Description
user.microapp.caller_input	FALSE	FALSE	210	Storage area for an ASR input that is collected from Get Speech. **Note** Get Speech results are written to the ECC variable. Results from Get Digits or Menu microapplications are written to the CED.
user.microapp.currency	FALSE	FALSE	6	Currency type.
user.microapp.error_code	FALSE	FALSE	2	Error status code returned from Unified CVP to Unified CCE when the Run Script Result is False.
user.microapp.FromExtVXML	FALSE	FALSE	60	This variable array returns information from the external VoiceXML file. Must be configured as array variables, not Scalar Variables, and array length set to 4.
user.microapp.input_type	FALSE	FALSE	1	Specifies the type of input that is allowed. Valid contents are: D(DTMF) and B (Both DTMF and Voice). B is the default. If you are not using an ASR, set this variable to D. If you are using an ASR, you can set this variable to either D or B.
user.microapp.locale	FALSE	FALSE	5	Combination of language and country that defines the grammar and prompt set to use.
user.microapp.metadata	FALSE	FALSE	62	Following the Menu (M), Get Data (GD) and Get Speech (GS) micro-applications, Unified CVP now returns information about the execution of that micro-application.
user.microapp.play_data	FALSE	FALSE	40	Default storage area for data for Play Data micro-applications.
user.microapp.sys_media_lib	FALSE	FALSE	10	Directory for all systems media files, such as individual digits, months, default error messages, and so forth.
user.microapp.ToExtVXML	FALSE	FALSE	60	This variable array sends information to the external VoiceXML file. Must be configured as Array variables, not Scalar Variables and array length set to 4.

Name	Enabled	Persistent	Maximum Length	Description
user.microapp.UseVXMLParams	FALSE	FALSE	1	Specifies the manner in which you pass the information to the external VoiceXML.
user.microapp.isPostCallSurvey	FALSE	FALSE	1	Used to determine if post call survey should be offered to a caller after the agent disconnects the call.
user.ece.activity.id	FALSE	FALSE	30	Needed for all types of WIM and EIM activities.
user.ece.customer.name	FALSE	FALSE	30	Needed for chat, callback, and delayed callback activities.
user.media.id	FALSE	FALSE	36	A number identifying a call to the Unified CCE Service, optionally, the H.323 Service.
user.microapp.grammar_choices	FALSE	FALSE	210	Specifies the ASR choices that a caller can input for the Get Speech micro-application.
user.microapp.inline_tts	FALSE	FALSE	210	Specifies the text for inline Text To Speech (TTS).
user.microapp.media_server	FALSE	FALSE	60	Root of the URL for all media files and external grammar files used in the script.
user.microapp.override_cli	FALSE	FALSE	200	Used by the system to override the CLI field on outgoing transfers.
user.microapp.pd_tts	FALSE	FALSE	1	Specifies whether Unifies Text To Speech or media files must be played to the caller.

System Information

- Expanded Call Context: Enabled
- Minimum Correlation number: 1001
- Maximum Correlation number: 9999
- Retain script versions:5

Agent Targeting Rule

Attribute	
Name	AgentExtensions
Peripheral	CUCM_PG_1

Attribute	
Rule Type	Agent Extension
Routing Client	All routing clients
Extension Range	000 - 999 0000 - 9999 00000 - 99999 000000 - 999999 0000000 - 9999999 00000000 - 99999999 000000000 - 999999999 0000000000 - 9999999999

IOPS values for Unified Communication Manager

The IOPS values for Unified Communication Manager are based on the BHCA values. These values may differs for the following scenarios:

- Software upgrades during business hours generate 800 to 1200 IOPS in addition to steady state IOPS.
- CDR/CMR using CDR Analysis and Reporting (CAR):
  - A Unified Communications Manager that sends CDR/CMR to the external billing server does not incur any additional IOPS.
  - CAR continuous loading results in around 300 IOPS average on the system.
  - Scheduled uploads are around 250 IOPS for Publisher VM only.
- Trace collection is 100 IOPS (occurs on all VMs for which tracing is enabled).
- Nightly backup (usually Publisher VM only) is 50 IOPS.

Mount ISO Files

Upload ISO image to data store:

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

Mount the ISO image:

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

Set Up NTP and Time Configuration at the Customer Site

Any domain controllers at the customer site must be configured to use NTP servers. The two ESXi host servers must point to the same NTP servers as the domain controllers. Additionally, you must review time configuration settings on the ESXi servers.

Procedure

Step 1 To add an NTP server to the domain controller:

a) Locate the Microsoft instructions on how to configure an authoritative time server in Windows Server.

Public NTP servers are available on the Internet if you do not have one.

b) Note down the IP address or domain name of the NTP server that you add.

Step 2 To point the ESXi core servers to the domain controller NTP servers:

a) For each core server, click the **Configuration** tab.
b) Choose **Time Configuration** > **Properties...** > **Options**.

This opens a panel with two sections: General and NTP Settings.

c) Click NTP Settings. Then click **Add.**
d) Enter the IP address of the primary domain controller. Click **OK**. Click **Restart.**

Step 3 To set the startup policy for the NTP server(s):

a) Navigate to **Time Configuration** . Then select **Properties**.
b) Check NTP Client Enabled.
c) Click **Options**.
d) Select **Start**. Click **OK.**

Step 4 To review the time settings for the host servers:

a) Click the **Configuration** tab.
b) In the Software panel, select **Time Configuration**, which shows the Date & Time and the NTP Servers.

Step 5 To adjust the Date & Time if they are incorrect:

a) Click **Properties...**
This opens the Time Configuration dialog box.

b) Change the Time and Date fields. Then click **OK**.

CCDM Logging and MaxSizeRollBackups

This section refers to the CCDM Logging and MaxSizeRollBackups:

Logging

Unified CCDM provides an extensive logging framework for each of the components of the system to aid troubleshooting in the event of a problem.

Logging trace levels are stored in the registry for each separate component and may be set to one of the four following values:

Logging Level	Name	Description
0	ERROR	This is the lowest level of logging. It will only log information relating to exceptions that occurred in the application.
1	WARN	Warn provides ERROR level logging plus warnings raised for potential system issues.
2	INFO	Info is the default logging level. It provides ERROR and WARN as well as standard diagnostic information.
3	DEBUG	Debug is the highest level of logging. It provides detailed information of every operation that is performed. Debug logging has an adverse effect on performance, its usage should be kept to a minimum.

Set Logging Level Using the Unified System CLI in the CCDM Server

Complete the following procedure to set logging level using the Unified System CLI in the CCDM server.

Procedure

Step 1 Navigate to **Start** > **All Programs** > **Domain Manager** > **Unified System CLI**.

Step 2 Enter the username (wsmadmin) and password for the wsmadmin user

Step 3 Enter the instance name (optional) and click **Enter**.

Step 4 Enter a debug level , for example debug level 0.

Note The value can be any logging level given in the table above.

MaxSizeRollBackups

MaxSizeRollBackups setting defines the number of log files per day to store before deleting them and creating a new one. This feature protects against a high volume of exceptions filling the disk in a short period of time.

MaxSizeRollBackups parameter is present in the configuration file for Application Server, Web, Data, Import Server services. Partitioning service, Provisioning service

Install and Configure Jabber for Windows

Install and Configure Jabber Client

You can run the installation program manually to install a single instance of the client and specify connection settings in the **Manual setup and sign-in** window.

Procedure

Step 1	Launch CiscoJabberSetup.msi. The installation program opens a window to guide you through the installation process.
Step 2	Select **Accept and Install** to begin the installation.
Step 3	Check **Launch Cisco Jabber** and select **Finish**.
Step 4	Select **Manual setup and sign-in**.
Step 5	In **Select your Account Type** window check **Cisco Communication Manager (Phone capabilities only)**.
Step 6	In the Login server select: use the following servers and enter the details of **TFTP server**, **CTI server** and **CUCM server** . Click **Save**
Step 7	Enter the **User Name**(the end user created in CUCM for jabber phone) and **Password** and sign in.

Configure Jabber Using UCDM

Add End User

Procedure

Step 1	Log in as Provider / Customer Admin.
Step 2	Navigate to **Location Administration** > **End Users**.
Step 3	Choose a **Location** from the drop-down list.
Step 4	Click **Add**.
Step 5	Enter **Username**, **Password**, **Lastname** and then, choose a **Role** from drop-down list.

Step 6 Fill rest of the form with **User Details** and click **Next**.

Step 7 Enter **Phone Pin** for the user.

Step 8 Select **Feature Group**.

Step 9 Select **Access Profile**, **Security Profile**, and **Feature Display Policy**.

Step 10 Click **Add**.

Migrate Agents and Supervisors to Single Sign-On Accounts

Important Be aware that this release does not provide support for disabling SSO once it is enabled.

Customers electing global hybrid mode to incrementally add SSO-enabled users may subsequently move to global enablement, or global enablement may be configured directly. However, the transition of hybrid mode to global off, of per-agent disablement while in hybrid mode, or of switching global on to global off is not supported at this time.

Customers who attempt to disable SSO after enabling it may experience user account inconsistencies, such as cleared (pre-SSO) passwords, invalid passwords, and Cisco Unified Intelligence Center reporting issues for supervisor accounts introduced after SSO was enabled. For this reason, be sure to back up Logger databases using the Microsoft SQL Server Backup and Restore utility.

Contact the Cisco TAC for questions or assistance.

If you are enabling SSO in an existing deployment, you can set the SSO state to hybrid to support a mix of SSO and non-SSO users. In hybrid mode, you can enable agents and supervisors selectively for SSO making it possible for you to transition your system to SSO in phases.

Use the procedures in this section to migrate groups of agents and supervisors to SSO accounts using the SSO Migration content file in the Unified CCE Administration Bulk Jobs tool. You use the Administration Bulk Jobs tool to download a content file containing records for agents and supervisors who have not migrated to SSO accounts. You modify the content file locally to specify SSO usernames for the existing agents and supervisors. Using the Administration Bulk Jobs tool again, you upload the content file to update the agents and supervisors usernames; the users are also automatically enabled for SSO.

The content file returns the first 12,000 agents and supervisors who have not been migrated to SSO accounts. After you run the bulk job to update users from that group of records, you can download the SSO Migration content file again to update additional agent and supervisor records.

If you do not want to migrate a user, delete the row for that user.

For instructions on how to setup SSO for Agent or Supervisor login, see the Configure the Cisco Identity Service, on page 301.

Important While the Finesse agent is logged in, changing the login name prevents the agent from answering or placing calls. In this situation, the agent can still change between *ready* and *not_ready* state. This affects all active agents, independent of whether SSO is enabled or disabled. Should you need to modify a login name, do so only after the corresponding agent is logged out. Note too that SSO migration (moving a non-SSO agent to be SSO-enabled, by either hybrid mode or global SSO mode) should not be done when the agent is logged in.

Procedure

Step 1 In Unified CCE Administration, navigate to **Manage** > **Bulk Jobs**.

Step 2 Download the SSO Migration bulk job content file.

a) Click **Templates.**

The **Download Templates** popup window opens.

b) Click the **Download** icon for the SSO Migration template.

c) Click **OK** to close the **Download Templates** popup window.

Step 3 Enter the SSO usernames in the SSO Migration content file.

a) Open the template in Microsoft Excel. Update the **newUserName** field for the agents and supervisors whom you want to migrate to SSO accounts.

The content file for the SSO migration bulk job contains these fields:

Field	Required?	Description
userName	Yes	The user's non-SSO username.
firstName	No	The user's first name.
lastName	No	The user's last name.
newUserName	No	The user's new SSO username. Enter up to 255 ASCII characters. If you want to enable a user for SSO, but keep the current username, leave **newUserName** blank, or copy the value of **userName** into **newUserName**.

b) Save the populated file locally.

Step 4 Create a bulk job to update the usernames in the database.

a) Click **New** to open the **New Bulk Job** window.

b) Enter an optional **Description** for the job.

c) In the **Content File** field, browse to the SSO Migration content file you completed.

The content file is validated before the bulk job is created.

d) Click **Save**.

The new bulk job appears in the list of bulk jobs. Optionally, click the bulk job to review the details and status for the bulk job. You can also download the log file for a bulk job.

When the bulk job completes, the agents and supervisors are enabled for SSO and their usernames are updated. You can open an individual user's record to see the changes.

Step 5 Repeat this procedure, if needed, to migrate additional agents and supervisors to SSO usernames.

What to do next

After all of the agents and supervisors in your deployment are migrated to SSO accounts, you can enable SSO globally in your deployment.

Globally Disable Single Sign-On

Follow these steps if you need to globally disable single sign-on from either SSO or Hybrid mode.

Important If you later want to migrate agents or supervisors from SSO-enabled to non-SSO:

- If you change a Cisco Unified Intelligence Center supervisor who was created as SSO-enabled to non-SSO, a new, non-SSO user account is created for the supervisor after the next user synchronization. The older, SSO-enabled supervisor account (in the format SSO\<loginname>) still exists in Cisco Unified Intelligence Center, however, and you must delete it. You must reconfigure the new, non-SSO supervisor user account (that matches the supervisor's SAM account name in Active Directory) in Cisco Unified Intelligence Center Administration Console to set up the supervisor's reports and permissions.

Procedure

Step 1 If the system is in **SSO** mode, change the SSO mode to **Hybrid** in the Unified CCE Administration **Single Sign-On** tool.

Step 2 Disable agents for SSO, and assign the agents new passwords. This step allows the agents to sign into Finesse.

Step 3 Disable supervisors for SSO. This step allows the supervisors to sign in to Unified CCE Administration to reskill agents.

Step 4 After you have updated all of the agent and supervisor records, change the SSO mode to **Non-SSO**.

Java Upgrades

In 12.5(1), after the initial release, CCE transitioned from Oracle to OpenJDK for the Java runtime environment. Newer installs and upgrades with 12.5(1a) base installer run with OpenJDK JRE while the older installs and upgrades with 12.5(1) base run with Oracle JRE. Existing 12.5(1) deployments will transition to OpenJDK with 12.5(1) ES55, which in turn is a mandatory prerequisite for receiving further maintenance patches on CCE.

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

Before updating the Java Runtime Environment (JRE):

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

Important Use JAVA_HOME if you are employing Oracle JRE.

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

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

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

- You can apply Java updates for the latest 32-bit Java 8 minor version.

  For the most current Java support information, see the Contact Center Enterprise Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

  You can download and install the Oracle Java updates from the Oracle website and the OpenJDK Java updates from the OpenLogic website.
- Modify the Windows CCE_JAVA_HOME environment variable to point to the new OpenJDK Java Runtime Environment (JRE) location if it has changed.

After updating the OpenJDK Java Runtime Environment (JRE):

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

Important Use JAVA_HOME if you are employing Oracle JRE.

- Import the certificates for all the components that you previously exported from the truststore before you updated the JRE.

  The command to import certificates is *keytool -import -keystore <JRE path>\lib\security\cacerts -file <filepath>.cer -alias <alias>*.
- Enter the truststore password when prompted.
- Enter 'yes' when prompted to trust the certificate.

Upgrade OpenJDKUtility

The Cisco Upgrade OpenJDKUtility:

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

Before using the tool:

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

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

Upgrade Tomcat Utility

Use the optional Cisco Upgrade Tomcat Utility to:

- Upgrade Tomcat to version 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.

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:

  <ICM install directory>:\icm\tomcat\logs
  <ICM install directory>:\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**

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**

Step 3 When prompted, enter **yes** to continue with the reversion.

Step 4 Repeat these steps for all unified CCE component VMs.

INDEX