# Installing and Configuring Guide for Cisco HCS for CC 11.0(1)

**First Published:** January 25, 2016

**Last Modified:** May 18, 2016

**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



## Purpose

This document provides the overview, design, installation and configuration of Cisco Hosted Collaboration Solutions for Contact Center. It provides all technical specifications and requirements, a list of procedures you must perform to install and configure this solution, and a configuration example.

## Audience

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

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

# Change History

| Change | See | Date |
|---|---|---|
| Outbound consideration updated for Small Contact Center deployment model | | April 2016 |
| Call by Call connection mode is supported | Connection Modes, on page 130 | |
| Specification Based Hardware support section is updated | Specification-Based Hardware Support, on page 48 | |
| Initial Publication Release | | January 2016 |

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

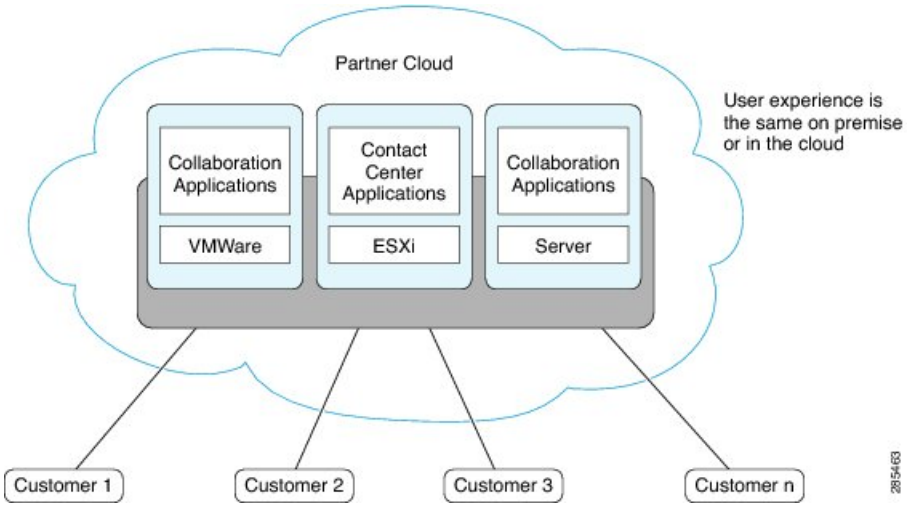
CHAPTER 1

# Cisco HCS for Contact Center

# Cisco HCS for Contact Center Topology

The following figure shows the high-level solution topology for Cisco HCS for Contact Center.

***Figure 1: Cisco HCS for Contact Center***




Cisco HCS for Contact Center service delivers Cisco Unified Contact Center Enterprise (Unified CCE) on a pair of duplexed Unified Computing System (UCS) Table 2: B200 M4 Blades, referred to as Side A and Side B. Cisco HCS for Contact Center offers the same shared management (service fulfillment and assurance) and aggregation (carrier trunks) that is common for all customer instances and used for other Cisco HCS services.

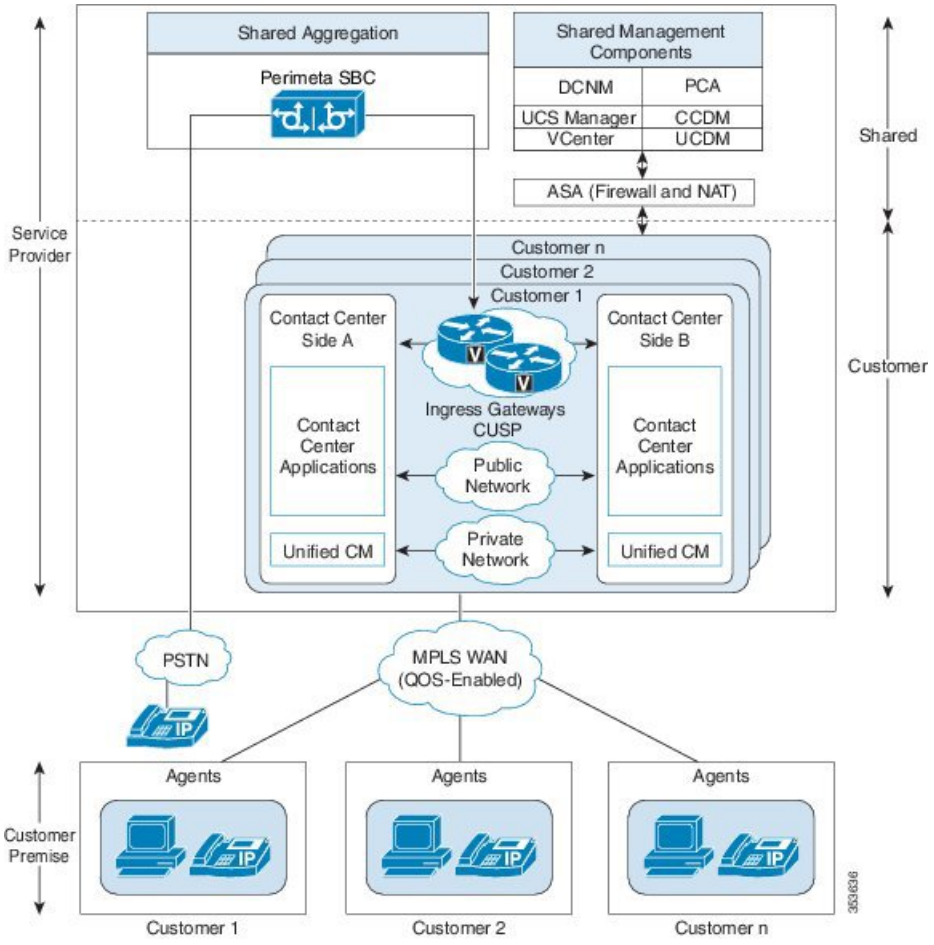
Cisco HCS for Contact Center is deployed in a virtualized environment, using OVA templates that are downloaded from Cisco Systems.

For an illustration of the topology see the following illustration.

The Contact Center aggregation layer and the shared management layer combines Cisco HCS components with the multiple network connections and route requests to the dedicated customer instances. Shared

aggregation consists of PGW and Perimeta SBC and shared management consists of UCDM, CCDM, Cisco Prime Collaboration Assurance (PCA), DCNM, UCS Manager, vCenter, and ASA (Firewall/NAT).

***Figure 2: Cisco for HCS Contact Center Topology***




# Cisco HCS for Contact Center Options and Feature Support

***Table 1: Core Components and Functionality included for HCS for Contact Center***

| Component | Functionality |
|---|---|
| Contact Center Domain Manager (CCDM) | Day 2 web configuration and WebServices API |
| Cisco Unified Contact Center Enterprise (UCCE) | Voice ACD |
| Cisco Unified Customer Voice Portal (Unified CVP) | Self Service, IVR, and rich VXML scripting |
| Cisco Unified Intelligence Center (CUIC) | Reporting |
| Cisco Unified Communications Manager (CUCM) | PBX, Call Control, and back-office phones |

| Component | Functionality |
|---|---|
| Cisco Finesse (Finesse) | Web 2.0 Agent Desktop |
| Unified Communications Domain Manager (UCDM) | Provision Unified Communications Domain Manager |

HCS for Contact Center offers the following features and options that are pre-sized within core components.

- Core component Integrated options:
  - Courtesy Callback
  - Agent Greeting
  - Whisper Announcement
  - Database Integration
  - Mobile Agent
  - Outbound Dialer
  - Post Call Survey
  - Precision Routing
  - A-law codec
  - CM Based Silent Monitoring
  - Back-office phone support
  - Finesse IP Phone Agent
- Optional Cisco components:
  - AW-HDS-DDS

    **Note** AW-HDS-DDS is a optional component for both 500 agent deployment and 1000 agent deployment.

  - Span-based monitoring
  - Unified WIM and EIM

    **Note** Supports Email, Chat and Web Call Back.

  - Cisco RSM
  - Cisco MediaSense
  - Cisco Unified SIP Proxy
  - Avaya PG

- Remote Expert Mobile
- Cisco Virtualized Voice Browser

- Optional third-party components:
  - Wallboard
  - Workforce Management
  - Recording
  - Speech-ASR/TTS
  - Cisco Solution Plus

- Remote Deployment options:
  - Global Deployments
  - Local Trunks
  - Remote Office Options

At this time, the following solution options and features are not supported in HCS for Contact Center

**Note**

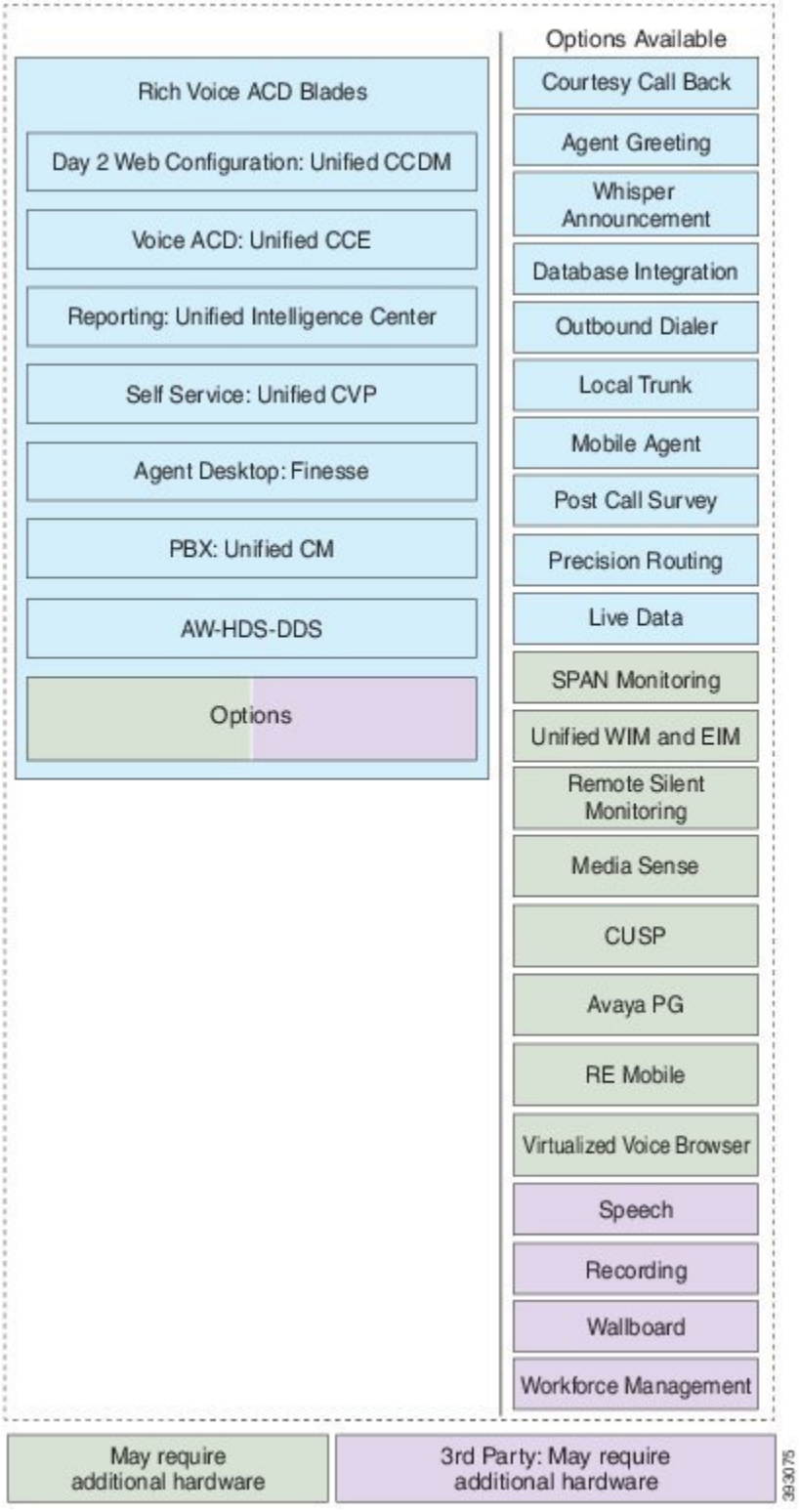
1. The following list is not exhaustive list. As a rule, if an option or feature is not mentioned in this document, it is not supported in this deployment.
2. Non-Contact Center UC applications such as Cisco Unity Connection or third party applications such as CRM and recording - may be deployed on external servers, if the hardware, co-residency, and support requirements are met for each application residing on that server. Refer to the respective external application's documentation.

- Cisco Agent Desktop
- Cisco Agent Desktop Browser Edition
- Cisco Intelligent Contact Management (ICM) to ICM Gateway
- Cisco Unified IP IVR
- CVP models other than comprehensive type 10
- H.323 or MGCP signaling
- ICM Application Gateway
- IP Phone Agent (CAD based)
- Parent Child
- SCCP Agent phones
- TDM (3rd party legacy ACD integration) PG, except Avaya PG

The following figure shows the list of features and options supported for HCS for Contact Center Release.

In several instances, configuration and capacity limits in this document supersede the information in **Cisco Unified Contact Center Enterprise Design Guide** and **Unified Cisco Voice Portal Design Guide**.

***Figure 3: HCS Contact Center Options and Feature Support***


Rich Voice ACD Blades
Day 2 Web Configuration: Unified CCDM
Voice ACD: Unified CCE
Reporting: Unified Intelligence Center
Self Service: Unified CVP
Agent Desktop: Finesse
PBX: Unified CM
AW-HDS-DDS
Options
Options Available
Courtesy Call Back
Agent Greeting
Whisper Announcement
Database Integration
Outbound Dialer
Local Trunk
Mobile Agent
Post Call Survey
Precision Routing
Live Data
SPAN Monitoring
Unified WIM and EIM
Remote Silent Monitoring
Media Sense
CUSP
Avaya PG
RE Mobile
Virtualized Voice Browser
Speech
Recording
Wallboard
Workforce Management
May require additional hardware
3rd Party: May require additional hardware
393075

# Shared Management and Aggregation

This section describes the following shared management components and aggregations:



## Unified Contact Center Domain Manager

Cisco Unified Contact Center Domain Manager (Unified CCDM) is a browser-based management application that is designed for use by Contact Center/system administrators, business users, and supervisors. It is a dense, multi-tenanted provisioning platform that overlays the Contact Center equipment. The Contact Center equipment consists of configuration items, generally known as resources, such as agents or skill groups, and events that are logged when the resources are used by the equipment, such as call record statistics. CCDM also manages CVP Day 2 operations ( Media files and VXML applications ).

Unified CCDM partitions the resources in the equipment using a familiar folder paradigm. These folders are then secured using a sophisticated security structure that allows administrators to specify which users can perform which actions within the specified folders. Unified CCDM supplies a number of tools that operate on the configuration and statistics data and allow users to modify both the Contact Center and Unified CCDM itself. The tools are all inherently multi-tenanted and the following tools are currently supported:

- Information Notices tool provides a *Message of the Day"*functionality
- Resource Manager tool enables users to create and modify resources such as agents or call types and organize them into a hierarchical folder structure
- Security Manager tool enables administrators to set up and manage security permissions

Unified CCDM focuses on supplying multi-tenancy functionality, playing to the business plans of hosts and large enterprises by enabling distributed or disparate Contact Center equipment to be partitioned:

- Unified CCDM abstracts and virtualizes the underlying Contact Center equipment, thereby allowing centralized deployment and decentralized control, which in turn gives economies of scale while supporting multi-level user command and control.
- Unified CCDM allows the powerful and flexible native provisioning operations to be abstracted into simple, high-level tasks that enable business users to rapidly add and maintain Contact Center services across the virtualized enterprise (or portion thereof).
- Unified CCDM users can see only the resources in the platform that they are entitled to see, thereby giving true multi-tenancy.
- Unified CCDM users can only manipulate resources visible to them, by using the tools and features they are authorized to use, thereby giving role-based task control.

The advantages of CCDM are :

- Provides Northbound APIs (SOAP and REST).
- Can be used at the shared management level across multiple customer instances.
- OVAs are sized for 50000 active and 300000 configured agents across multiple customer instances.

Unified CCDM maintains a complete data model of the Contact Center equipment to which it is connected. This data model is periodically synchronized with the equipment. In addition to the configuration information such as agent and skill groups, Unified CCDM records the events logged by the equipment, such as call records, for management information and reporting.

Unified CCDM provisions multiple Contact Center customer instances. It also provides the northbound REST and SOAP interfaces for multiple instances from a shared Unified CCDM.

Install the Unified CCDM servers on a Service Provider Management AD domain and create a trust relationship with the Unified CCDM domain and each customer instance domain.

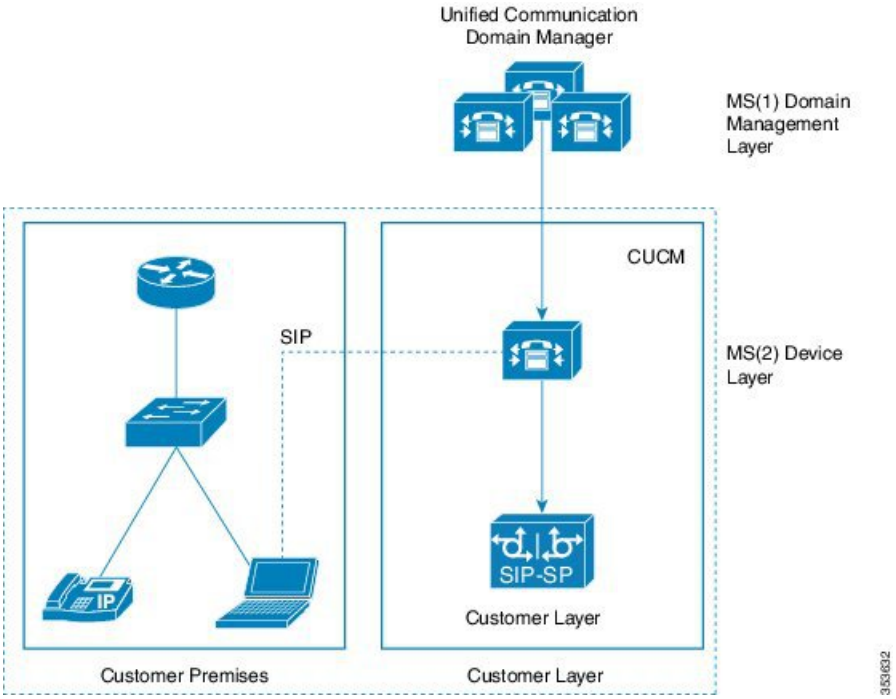
Refer to the sections Install and Configure Unified CCDM, on page 195 and Provision Unified CCE Using Unified CCDM, on page 501 for Installing and provisioning Unified CCDM information respectively.

# Unified Communication Domain Manager

In HCS, Unified Communications Domain Manager provisions Unified Communications (UC) applications and devices, such as Cisco Unified Communications Manager (Unified Communications Manager).

Unified Communications Domain Manager is a multi-tenant application, so you can use the Unified Communications Domain Manager server to provision all HCS customers. HCS supports multinode Unified Communications Domain Manager instance per HCS installation.

***Figure 4: Unified Communication Domain Manager***



For more information about Unified Communication Domain Manager, see Install and Configure Unified Communication Domain Manager, on page 221.

# ASA NAT and Firewall

Cisco Adaptive Security Appliance (ASA) Firewall partitions a single security appliance into multiple virtual devices known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Each context keeps customer traffic separate and secure, and also makes configuration easier. All customer traffic is first sent to the firewall before forwarding to the computer resources.

For more information about ASA NAT and Firewall, see Install and Configure ASA Firewall and NAT, on page 227 and Firewall Hardening Considerations, on page 191.

# Cisco Prime Collaboration - Assurance

Cisco Prime Collaboration Assurance is a comprehensive video and voice assurance and management system with a set of monitoring, troubleshooting, and reporting capabilities that help ensure end users receive a consistent, high-quality video and voice collaboration experience. You can deploy Prime Collaboration in either Managed Service Provider (MSP) mode. The following are the key features of Cisco Prime Collaboration.

- Voice and Video Unified Dashboard
- Device Inventory Management
- Voice and Video Endpoint Monitoring
- Diagnostics
- Fault Management
- Reports
- Live Contact Center topology with link status, device status, device performance, device 360.
- Contact Center device discovery
- Contact Center devices real time performance monitoring.
- Events and Alarms along with root cause analysis.
- Contact Center device Dashboards - Pre-canned and custom
- Threshold, Syslog, Correlation and System Rules - Pre-canned and custom
- Multi-tenancy and logged-in agent licensing information.

For more information about Cisco Prime Collaboration - Assurance, see Cisco Prime Collaboration Assurance Integration for Small Contact Center Deployment Model, on page 498 and Install and Configure Prime Collaboration Assurance, on page 239.

# Perimeta SBC

**Perimeta Session Border Controller (SBC)** is a Metaswitch's family of carrier-class Session Border Controller (SBC) products which is a session-aware device designed for **Communications over IP** ,it protects a network from malicious traffic and excessive call load - as well as providing other session-based services such as protocol interworking. Perimeta SBC is an advanced Session Border Controller based on Metaswitch's field-proven SBC technology.

Perimeta SBC facilitates in SIP trunk aggregation and distribution of SIP calls to individual customer instances. It streamlines the SIP traffic ALG functionality in small contact center deployment.

Perimeta SBC works to solve the Communications over IP network problems by ensuring the following:

- **Security**: Perimeta SBC filters out malicious traffic before it reaches the network, accepting only valid SIP signaling traffic. If a call is accepted into the network, Perimeta SBC opens dynamic pinholes for the media, and ensures that only traffic conforming to the parameters negotiated in the call setup request flows through those pinholes.
- **Quality of Service**: Perimeta SBC processes every SIP signaling request to decide whether the network can provide the requested service, given current loading patterns.
- **Accessibility**: Perimeta SBC detects when it is contacted by a device behind a NAT, caches the details of the NAT pinholes created by that device and invokes standard protocol mechanisms to ensure that the pinhole remains open and hence that the device is available for incoming calls.

# Core Solution Components

This section describes the following core solution components:

- Unified CCE, on page 11
- Unified CVP, on page 14
- Unified Communication Manager, on page 15
- Unified Intelligence Center, on page 17
- Cisco Finesse, on page 18
- CUBE-Enterprise, on page 18

# Unified CCE

Unified Contact Center Enterprise (Unified CCE) is the software application that provides the contact center features, including agent state management, agent selection, call routing and queue control, IVR control, CTI Desktop screen pops, and contact center reporting. The Unified CCE runs on Cisco Unified Communications on Cisco Unified Computing System (Cisco Unified Communications on Cisco UCS) virtualized servers or exact equivalents unless otherwise specified. There are following major components of a Unified CCE deployment:

- Router
- Logger

- Peripheral Gateway (PG)
- Administration & Data Server
- Live Data Server

## Router

The Router is the brain of Unified CCE. It is capable of running user defined scripts to make decisions on what should happen with calls, and it has the ability to figure out how to get a call from one place to another. Routers are "duplex" entities, whereby two separate, distributed instances (identified as Side A and Side B) use the MDS to keep in lock-step with its other side, ensuring that any outage of one side guarantees that the system continues operating without failures or impairments - the opposite side assumes sole responsibility for making routing decisions. All data as well as call control messaging is shared between sides to ensure that both sides have the same data by which to make (the same) routing decisions. Both router sides are "in service" concurrently.

## Logger

The Logger is used by Unified CCE to store historical data and configuration data about the call center. It is the place where historical data is first stored, and from which it is later distributed. The Logger uses a synchronization process that is a little different than the Router. The messages coming to the Logger are only sent from the corresponding Router. Side A Router only sends messages to the Side A Logger. Side B Router only sends messages to the Side B Logger. Because the routers are running in lock-step, it is guaranteed that while messages are flowing they are the same messages. The Loggers also distribute historical data to HDS and configuration and real time data to the Administration & Data Servers through MDS.

## Peripheral Gateway

The PG is the component that talks to the telephony devices through their own proprietary CTI interface in a Unified CCE system. These devices can be ACDs, IVR devices or an IP PBX. The PG normalizes whatever protocol the telephony device speaks, and keeps track of the state of agents and calls that are on that device. The PG sends this status to the Router, as well as forwards requests requiring customer logic to the Router. The component of the PG that does the normalization is called a Peripheral Interface Manager (PIM). This component is responsible for actually talking to the peripheral and translating whatever proprietary language it speaks into the normalized one that the OPC and the rest of the PG understands. Co-resident with the PG is the CTI Gateway (CG - CTI Server component) and the CTI Object Server (CTI OS)

There are several groups that PGs fall into. The first classification of PG includes those that talk to an ACD or Unified CM that has agents on it. It talks a proprietary CTI protocol to the switch, and maintains the state of agents and calls in queue on the device. The second classification of PG is a VRU or Media Routing (MR) PG. These PGs expose an interface that is client-neutral. In the case of the VRU PG, this interface is tailored to voice calls; in the case of the MR PG, it is more generic task routing that is exposed. The third classification of PG is the group PG (Generic PG). This PG allows multiple PIMs of different types to reside inside of the same PG.

## Administration & Data Server

The Administration & Data Server is the main interface to the Unified ICM/CC configuration. On the Administration & Data Server resides a database which contains a copy of the configuration information

contained in the Logger. A Distributor process, which receives updates from the central controller, writes to the database to keep everything in sync. Multiple clients read the configuration from the database and send update messages to the central controller's DB Agent process. The two main clients in the Administration & Data Server are the configuration tools which are used to provide a GUI to update the configuration, and the Configuration Management Server (CMS) process which is used to provide the Configuration API (ConAPI). The Administration & Data Server does not have a dependent twin but rather provides fault tolerance in numbers (N+1 model).

The Administration & Data Servers are classified into the following roles in HCS-CC based on the system configuration and the call load that it can handle:

**Administration Server (Configuration and Real-Time Reporting):**

This role is similar to the former Distributor AW model which provides the capability for configuration changes as well as real-time reporting. The real-time reporting is supported using Cisco Unified Intelligent Center (Reporting client). No historical reporting is supported

**Administration Server, Historical Data Server, and Detail Data Server (AW-HDS-DDS):**

This Administration & Data Server deployment role is similar to the existing Distributor AW with HDS model which provides the capability for configuration changes as well as both real-time and historical reporting. The real-time and historical reporting is supported using Cisco Unified Intelligence Center (Unified Intelligence Center Reporting client). Call detail and call variable data are supported for custom reporting data extraction to feed historical data.

**Administration Server And Historical Data Server (AW-HDS):**

This Administration & Data Server deployment role provides the capability for configuration changes as well as both real-time and historical reporting. Real-time and historical reporting are supported using Cisco Unified Intelligence Center Reporting user. The following features are disabled and not supported:

- Call Detail, Call Variable, and Agent State Trace data
- Custom reporting data extraction

**Historical Data Server and Detail Data Server (HDS-DDS):**

The HDS-DDS deployment model is used specifically for data extraction and for custom reports for call detail (TCD and RCD) only. The following features are disabled and not supported:

- Real-time data reporting
- Ability to make configuration changes

This deployment role is limited to one per Logger side.

## Nomenclature Table

| | |
|---|---|
| CCE Call Server | Router and PG |
| CCE Data Server | Logger and AW |
| CCE Rogger | Router and Logger running on same VM |
| CCE Central Controller | Router and Logger |

# Unified CVP

Cisco Unified Customer Voice Portal combines open-standards support for speech with intelligent application development and industry-best call control to deliver personalized self-service to callers-either as a standalone interactive-voice-response (IVR) system or transparently integrated with a contact center. The following topics describe the Cisco Unified Customer Voice Portal (CVP) product components.

- Call Server
- VXML Server
- Media Server
- Unified CVP Reporting Server
- Unified CVP Operations Console Server
- CVP Server includes CVP Call Server, VXML Server, Media Server

## Call Server

The Call Server component provides the following independent services, which all run on the same Windows 2012 R2 server:

- **SIP service**: This service communicates with the Unified CVP solution components such as the SIP Proxy Server, Ingress Gateway, Unified CM SIP trunks, and SIP phones. The SIP service implements a Back-to-Back User Agent (B2BUA). This B2BUA accepts SIP invites from ingress voice gateways and typically directs those new calls to an available Voice XML gateway port. After completing call setup, the Unified CVP B2BUA acts as an active intermediary for any subsequent call control. While the Unified CVP SIP signaling is routed through this service, this service does not touch the RTP traffic. Integrated into this B2BUA is the ability to interact with the Cisco Unified ICM via the ICM Service. This integration provides the ability for the SIP Service to query the Unified ICM for routing instruction and service control. This integration also allows Unified ICM to initiate subsequent call control to do things such as requesting that a caller be transferred from queue to an agent or transferred from one agent to another agent.
- **ICM service**: This service is responsible for all communication between Unified CVP components and Unified ICM. It sends and receives messages on behalf of the SIP Service and the IVR Service.
- **IVR service**: This service creates the Voice XML pages that implement the Unified CVP Micro applications based on Run VRU Script instructions received from Unified ICM. The IVR Service functions as the VRU leg (in Unified ICM Enterprise parlance), and calls must be transferred to it from the SIP Service in order to execute Micro applications. The Voice XML pages created by this module are sent to the Voice XML gateway to be executed.

## VXML Server

The VXML Server executes advanced IVR applications by exchanging VoiceXML pages with the VoiceXML gateway's built-in voice browser. Like almost all other Unified CVP product components, it runs within a Java 2 Enterprise Edition (J2EE) application server environment such as Tomcat and many customers add their own custom-built or off-the-shelf J2EE components to interact with back-end hosts and services. The VXML Server applications are written using Cisco Unified Call Studio and are deployed to the VXML Server

for execution. The applications are invoked on an as-needed basis by a special Micro application which must be executed from within the Unified CCE routing script.

### Media Server

The Media Server component is a simple Web Server, such as Microsoft IIS or Apache, which can provide prerecorded audio files, external VoiceXML documents, or external ASR grammars to the gateway. Some of these files can be stored in local flash memory on the gateways. However, in practice, most installations use a centralized media server to simplify distribution of prerecorded customer prompt updates. Media Server functionality can also include a caching engine. The gateways themselves, however, can also do prompt caching when configured for caching. Typical Media Servers used are Microsoft IIS and Apache, both of which are HTTP-based.

### Unified CVP Reporting Server

The Unified CVP Reporting Server is a Windows 2012 R2 server that hosts an IBM Informix Dynamic Server (IDS) database management system. The Reporting Server provides consolidated historical reporting for a distributed self-service deployment. The database schema is prescribed by the Unified CVP product, but the schema is fully published so that customers can develop custom reports based on it. The Reporting Server receives reporting data from the IVR Service, the SIP Service (if used), and the Unified CVP VXML Server (VXML Server). The Reporting Server depends on the Unified CVP Call Server (Call Server) to receive call records.

The Reporting Server does not itself perform database administrative and maintenance activities such as backups or purging. However, Unified CVP provides access to such maintenance tasks through the Unified CVP Operations Console Server.

### Unified CVP Operations Console Server

The Unified CVP Operations Console Server is a Windows 2012 R2 server that provides an Operations Console for the browser-based administration and configuration for all Unified CVP product components, and it offers shortcuts into the administration and configuration interfaces of other Unified CVP solution components. The Operations Console is a required component in all Unified CVP deployments.

The Operations Console must be run on a separate machine from other Unified CVP devices.

The Operations Console is, in effect, a dashboard from which an entire Unified CVP deployment can be managed.

The Operations Console Server is not a redundant component. As such, you cannot duplicate the Operations Console Server within a deployment. Back up the configuration database regularly or when a change is made, because the Operations Console Server is an essential component, and cannot be duplicated within a deployment.

## Unified Communication Manager


- Call Processing Nodes, on page 16
- TFTP and Music on Hold Nodes, on page 17

## Call Processing Nodes

Cisco Unified Communications Manager (formerly named as Cisco Unified Call Manager) serves as the software-based call-processing component of the Cisco Unified Communications family of products. A wide range of Cisco Media Convergence Servers provides high-availability server platforms for Cisco Unified Communications Manager call processing, services, and applications.

The Cisco Unified Communications Manager system extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Cisco Unified Communications Manager provides signaling and call control services to Cisco integrated telephony applications as well as third-party applications. Cisco Unified Communications Manager performs the following primary functions:

- Call processing
- Signaling and device control
- Dial plan administration
- Phone feature administration
- Directory services
- Operations, administration, maintenance, and provisioning (OAM&P)
- Programming interface to external voice-processing applications such as Cisco IP Communicator, Cisco Unified Customer Voice Portal (CVP).

The Cisco Unified Communications Manager system includes a suite of integrated voice applications that perform voice-conferencing and manual attendant console functions. This suite of voice applications means that no need exists for special-purpose voice-processing hardware. Supplementary and enhanced services such as hold, transfer, forward, conference, multiple line appearances, automatic route selection, speed dial, last-number redial, and other features extend to IP phones and gateways. Because Cisco Unified Communications Manager is a software application, enhancing its capabilities in production environments requires only upgrading software on the server platform, thereby avoiding expensive hardware upgrade costs.

Distribution of Cisco Unified Communications Manager and all Cisco Unified IP Phones, gateways, and applications across an IP network provides a distributed, virtual telephony network. This architecture improves system availability and scalability. Call admission control ensures that voice quality of service (QoS) is maintained across constricted WAN link and automatically diverts calls to alternate public switched telephone network (PSTN) routes when WAN bandwidth is not available.

A web-browse-able interface to the configuration database provides the capability for remote device and system configuration. This interface also provides access to HTML-based online help for users and administrators.

Cisco Unified Communications Manager, designed to work like an appliance, refers to the following functions:

- Cisco Unified Communications Manager servers can get pre-installed with software to ease customer and partner deployment and automatically search for updates and notify administrators when key security fixes and software upgrades are available for their system. This process comprises Electronic Software Upgrade Notification.
- You can upgrade Cisco Unified Communications Manager servers while they continue to process calls, so upgrades take place with minimal downtime.

- Cisco Unified Communications Manager supports the Asian and Middle Eastern markets by providing support for Unicode on higher resolution phone displays.
- Cisco Unified Communications Manager provides Fault, Configuration, Accounting, Performance, and Security (FCAPS).

### TFTP and Music on Hold Nodes

A TFTP subscriber or server node performs two main functions as part of the Unified CM cluster:

- The serving of files for services, includes configuration files for devices such as phones and gateways, binary files for the upgrade of phones as well as some gateways, and various security files
- Generation of configuration and security files, which are usually signed and in some cases encrypted before being available for download
- The Cisco TFTP service that provides this functionality can be enabled on any server in the cluster. However, in a cluster with more than 1250 users, other services might be impacted by configuration changes that can cause the TFTP service to regenerate configuration files. Therefore, Cisco recommends that you dedicate a specific subscriber node to the TFTP service and MOH feature for a cluster with more than 1250 users or any features that cause frequent configuration changes
- Cisco recommends that you use the same hardware platform for the TFTP subscribers as used for the call processing subscribers
- 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

## Unified Intelligence Center

Cisco Unified IC offers both a web-based reporting application and an administration interface. The reporting application runs on the Members. The administration application runs on the Controller. Unified IC reporting features include multi-user support, customized reports, security, multiple display formats, web accessibility, and Web 2.0-like mashup support to display data from multiple sources on a single dashboard. These features make Unified IC a valuable tool in the Information Technology arsenal of any organization and position it as a drop-in replacement or solution for most reporting requirements. Cisco Unified IC reporting capabilities include

- Web 2.0 based dashboard mashups
- powerful grid presentations of reports with sorting and grouping
- chart and gauge presentations of reports
- association of multiple report displays with the same report definition
- custom filters
- custom thresholds to alert on the data
- pre-installed stock report templates for Unified CCE data
- ability to report data from JDBC compatible data sources

### Live Data Reporting System

Live Data Reporting System is a data reporting framework that processes real-time events with fast refresh rates and high availability. The Live Data Reporting System continuously pushes real-time updates to Unified Intelligence Center reporting clients as the event occur.

Two other data flows, the Real Time and Historical Data flows, are used to support existing stock and custom reports via the Administrative Workstation (AW) database. In the Real Time data flow, the Router on the Central Controller pushes all real-time updates every 10 seconds to the AW Distributors which write the data to tables in the AW database. Unified Intelligence Center queries the database periodically to retrieve the data stored in the AW database and presents it to clients, such as reports and dashboards. In contrast, Live Data continuously publishes only changed data directly to Unified Intelligence Center without the delay of controller write/reads to the database.

## Cisco Finesse

Cisco Finesse is the next-generation agent and supervisor desktop for Cisco Unified Contact Center Enterprise, providing benefits across a variety of communities that interact with your customer service organization. It is designed to improve collaboration by enhancing the customer and customer service representative experience.

The Cisco Finesse agent and supervisor desktop for Cisco Unified Contact Center Enterprise integrates traditional contact center functions into a thin-client desktop. A critical characteristic is that every desktop is 100-percent browser-based and implemented through a Web 2.0 interface. No client-side installations are required. This reduces the total cost of ownership (TCO).

Cisco Finesse also provides a Web 2.0 software development kit (SDK) and gadgets to enable developers to quickly get started with implementing in your environment.

## CUBE-Enterprise

The Cisco Unified Border Element is a special Cisco IOS software image that provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking. Cisco Unified Border Element Enterprise provides the feature set to support the transition to SIP trunking. Cisco session border controller (SBC), the Cisco Unified Border Element, provides these important services between the enterprise and service provider networks:

- **Interworking**: The capability to interconnect different signaling methods and variants.
- **Demarcation**: The capability to act as a distinct demarcation point between two networks.
- **Security**: The capability to intelligently allow or disallow real-time traffic between networks.

# Core Component Integrated Options

This section describes the following core component integrated options:

- Courtesy Callback, on page 19
- Agent Greeting, on page 19

# Courtesy Callback

Courtesy Callback limits the time a caller waits on the phone for an agent to answer. Instead of listening to queue music, callers have the option to have their calls returned when an agent becomes available.

Each call has a calculated Estimated Wait Time (EWT). When a callers' EWT approaches zero, the script initiates a call back to the caller. Upon retrieving the caller on the phone again, the caller is placed back into the queue in the order in which they first entered. Therefore, their call is transferred to an agent. For more information about Courtesy Callback, see Courtesy Callback Considerations, on page 126 and Configure Courtesy Callback, on page 592.

# Agent Greeting

You can play a configurable, automated agent greeting to callers, standardizing the caller experience. The greeting helps keep the agent voices fresh because they do not have to repeat the same greeting on every call. The Agent Greeting feature lets you record a message that plays automatically to callers when they connect to you. The greeting message can welcome the caller, identify the agent, and include other useful contextual information. With Agent Greeting, each caller receives a clear, well-paced, and language-appropriate introduction.

The process of recording a greeting is similar to recording a message for your voice mail. Depending on how your call center is set up, you can record different greetings that play for different types of callers (for example, an English greeting for English speakers or an Italian greeting for Italian speakers).

By default, greeting play is enabled when you log in to your agent desktop, but you can turn it off and on as necessary.

Agent Greeting is available to agents and supervisors who use IP Phones with Built-in-Bridge (BiB) that are controlled by the Unified CCE and Unified CM. These agents are typically located within a contact center. This feature is subject to certain functional limitations. For more information about the Agent Greeting phone requirements and limitations, see Agent Greeting Design Considerations, on page 129.

To deploy the Agent Greeting feature, you must configure Unified CVP, Unified CCE, and Unifed CCM. For more information about these configurations, see Configure Agent Greeting, on page 602.

# Whisper Announcement

Customers can play a configurable announcement to an agent right before the caller is connected, providing information about the type of call being delivered (for example, sales or tech support) and other guidance. Agents get information about the caller through their headset, speeding problem handling and improving first-call resolution.

Whisper Announcement plays a brief, prerecorded message to an agent just before the agent connects with each caller. The content of the announcement can contain information about the caller that helps prepare the agent to handle the call. You can enable Whisper Announcement and specify the announcements to play in your Unified CCE call routing scripts. For more information about these scripts, see Configure Whisper Announcement, on page 613.

Whisper Announcement is subject to certain limitations. For more information about Whisper Announcement, see Whisper Announcement Considerations, on page 129.

# Database Integration

Database Integration provides the option to integrate with an external database and to create, or update, or retrieve the operations on a database table. For more information, see Configure Database Integration, on page 614.

# Mobile Agent

Mobile Agent enables an agent using any PSTN phone and a broadband VPN connection (for agent desktop communications) to function just like a Unified CCE agent sitting in a formal call center and using a Cisco IP Phone monitored and controlled by Cisco Unified Communications Manager (Unified CM) JTAPI.

For more information about Mobile Agent, see Mobile Agent Considerations, on page 130 and Configure Unified Mobile Agent, on page 619

# Outbound Dialer

The Cisco Outbound Dialer application provides outbound dialing functionality along with the existing inbound capabilities of the Cisco Unified Contact Center Enterprise. This application enables the contact center to dial customer contacts and direct contacted customers to agents or IVRs. With Cisco Outbound Dialer, you can configure a contact center for automated outbound activities.

**Note** HCS for Contact Center supports SIP dialer.

For more information about Outbound Dialer, see Outbound Dialer Considerations, on page 133 and Configure Outbound, on page 623

# Post Call Survey

A Post Call Survey takes place after normal call treatment typically to determine whether a customer was satisfied with their call center experience. This feature enables you to configure a call flow that, after the agent disconnects from the caller, optionally sends the call to a Dialed Number Identification Service (DNIS) configured for a Post Call Survey.

The caller can be prompted during IVR treatment as to whether they want to participate in a Post Call Survey. If they choose to do so, they are automatically transferred to the Post Call Survey after the normal call flow completes, for example, after the agent ends the conversation.

For more information about post call survey, see Post Call Survey Considerations, on page 136 and Configure Post Call Survey, on page 641.

# Precision Routing

Precision Routing is a feature available with Cisco Unified Contact Center Enterprise (Unified CCE). Precision Routing enhances and can replace traditional routing. Traditional routing looks at all of the skills to which an agent belongs and defines the hierarchy of skills to map business needs. However, traditional routing is restricted by its single dimensional nature. Precision Routing provides multidimensional routing with simple configuration, scripting, and reporting. Agents are represented through multiple attributes with proficiencies so that the capabilities of each agent are accurately exposed, bringing more value to the business.

You can use a combination of attributes to create multidimensional precision queues. Using Unified CCE scripting, you can dynamically map the precision queues to direct a call to the agent that best matches the precise needs of the caller.

For more information about Precision Routing, see Configure Precision Routing, on page 515

# A-law Codec

By default, HCS for Contact Center applications will accept incoming calls using Mu-Law codecs. However a-law codec is supported by changing the default values in Unified CVP, Unified Communications Manager and VXML/Ingress Gateways.

For more information about A-law codec, see a-Law Codec Support Considerations, on page 137 and Configure a-Law Codec, on page 642

# CM based Silent Monitoring

Unified Communications Manager accomplishes silent monitoring with a call between the supervisor (monitoring) device and the agent (monitored) device. The agent phone mixes and sends the agent's conversation to the supervisor phone, where it is played out to the supervisor.

Unified CCE supports the Silent Monitoring functionality available in Unified Communications Manager. Unified Communications Manager Silent Monitoring supports only one silent monitoring session and one recording session for the same agent phone.

**Note** Unified Communications Manager Silent Monitoring does not support mobile agents.

## Back-office Phone support

Back-Office Agents have all of the functionality of the formal contact center agents. They also may be able to receive calls routed by the system or transferred from the formal contact center agents. See Back-Office Phone Support Considerations, on page 137.

## Finesse IP Phone Agent

With Finesse IP Phone Agent, you can access Finesse features on your Cisco IP phones as an alternative to accessing Finesse through your browser. For more information about Cisco Finesse IP Phone Agent, see Finesse IP Phone Agent Considerations, on page 138.

# Optional Cisco Components

This section describes the following optional Cisco components:



## AW-HDS-DDS

Administration & Data Servers have several roles: Administration, Real-Time Data Server, Historical Data Server, and Detail Data Server. The AW-HDS-DDS Server is a combination of Administration Server, Real-Time and Historical Data Server, and Detail Data Server all in one. The Logger database retention period is 400 days of historical data and 40 days of detailed TCD and RCD records. If you require longer retention periods, optionally add a single AW-HDS-DDS server to the deployment. For more information about AW-HDS-DDS, see Configure Unified CCE AW-HDS-DDS, on page 409.

**Note** AW-HDS-DDS is optional component for 500 and 1000 agent deployment only.

# SPAN-Based Monitoring

You can silently monitor the mobile agents through CTI OS based silent monitoring. In some cases, you must deploy a standalone silent monitor server. This silent monitor server gains access to mobile agent voice traffic through a SPAN port that you must configure to send all traffic to and from the agent gateway to the silent monitor server. The silent monitor server then filters and forwards voice traffic for the selected agent to the supervisor's silent monitor server. For more information about SPAN-Based Monitoring, see SPAN-Based Monitoring, on page 651.

# Cisco Unified WIM and EIM

Cisco Unified E-Mail Interaction Manager (Unified EIM) enables organizations to intelligently route and process inbound emails, webform inquiries, faxes, and letters. Cisco Unified Web Interaction Manager (Unified WIM) provides agents with a comprehensive set of tools for serving customers in real time. It enables call center agents to provide immediate personalized service to customers through text chat messaging and page-push abilities. Agents can also use Unified WIM to assist customers using web chat.

Following are the Cisco Unified WIM and EIM supported features.

- Email, on page 23
- Chat Feature, on page 23
- Web Callback and Delayed Callback, on page 24
- Unified WIM and EIM Considerations, on page 139

For more information about Installation and Configuration Cisco Unified E-mail and Web Interface Management, see Cisco Unified Email and Web Interface Management Documentation Guide.

## Cisco Unified WIM and EIM Features

### Email

Email is supported by Unified WIM and EIM to create a communication channel between a customer and an agent. There are various steps involved in efficiently responding to emails from customers. Emails are first retrieved into the system and routed to appropriate users or queues. Once a response is created, it is processed through the system and sent to the customer.

For information on how to configure emails, See Cisco Unified Email and Web Interface Management Documentation Guide.

### Chat Feature

It is an activity created for a chat session between a customer and an agent. A chat is a real time interaction between an agent and a customer during which they exchange text messages. As part of a chat, agents can also push web pages to customers. Based on how chat activities are routed to agents, they can be categorized as Standalone chats and Integrated chats. An integrated chat is routed to an integrated queue, and a message is sent to Unified CCE. Unified CCE processes the activity and assigns the chat to an available IPTA (ICM Picks the Agent) agent.

### Web Callback and Delayed Callback

*Web Callback*

The Web Callback feature allows the user to request a callback by submitting a form on a website. Unified WIM processes the submitted information and connects the user with an agent. In the Unified CCE integration, the Unified WIM sends a message to Unified CCE requesting Unified CCE to route the callback request to an agent. Unified CCEsends a message to Unified WIM with a message for Cisco Media Blender. Call Router supports the Web Callback for sending notification to the peripheral interface manager (PIM), and Media Blender receives the message.

*Delayed Callback*

The Delayed Callback feature in the Unified CCE integration is similar to the Web Callback feature, but when the Unified WIM receives the delayed callback request, it adds the request in the Delayed Callback table. Unified WIM sends the HTML page to the caller, indicating that the caller will receive a callback within a specified time. When the specified time arrives, Unified WIM moves the request to the Unified CCE queue for routing to Unified CCE. The call is then processed the same way as for Web Callback. For more information, see Unified WIM and EIM Considerations, on page 139.

# Cisco Remote Silent Monitoring

The Cisco Remote Silent Monitoring (RSM) application allows for real-time phone-based monitoring of agents in the Cisco Unified Contact Center Enterprise (Unified CCE) environment. The RSM platform is installed on a Windows operating system as a single server instance, and a separate call flow script is hosted on the Unified CVP (VRU) platform.

When a supervisor dials into the VRU node using a VoIP or a plain old telephone service (POTS) phone:

- The incoming call is routed to the Unified CCE call flow script, then sent to a VXML call flow script.
- The script requests services and data from the RSM server, according to the caller's input to system prompts.
- The script parses a response and provides data and voice streams to the caller.

The RSM system prompts allow for the selection of Random, Newest, or Problem call monitoring modes. Callers can also select the specific agents they want to monitor based on the Agent ID (or Peripheral ID) of the agent, or they can select from a list of currently active agents. For more information about Cisco Remote Silent Monitoring, see Configure Cisco RSM, on page 656 and Cisco RSM Considerations, on page 147.

## RSM Services

The RSM server runs two application instances, VLEngine (see VLEngine, on page 24) and Phone Sim (see PhoneSim, on page 25), which together provide RSM services to callers. The VLEngine tracks the environment state and handles most of the requests from the call flow script (that is the login authentication, agent listing, permissions required to monitor a call). The PhoneSim service manages the simulated phones.

### VLEngine

VLEngine runs on the Tomcat application server software, which provides servlet hosting. So, when a supervisor who is dialed into RSM interacts with the system,the call flow script makes HTTP requests for

dynamic content from VLEngine servlets and then parses the output. Requests for static content, such as audio prompts, are also made to the VLEngine in certain cases (for example, for the Unified CVP VXML script, through the use of its VXML VoiceBrowser step).

VLEngine monitors all Unified CCE events using CTI or CTI OS, keeping dynamic, real-time track of those agents currently handling calls, as well as the skill-group membership of those agents. So, for example, if an agent was previously not on a call when the caller first dialed in, but is now handling a call, that agent's status is updated so the agent can now be monitored.

### PhoneSim

PhoneSim device entries look and function exactly like hardware VoIP phones in the Unified Communications Manager environment and they are managed and controlled by the RSM server. It functions as a supervisor's VoIP phone, and provides supervisor dial-in functionality. So, when a supervisor sends a request through RSM to monitor an agent, the system identifies that it is streaming the monitored agent's call data directly to the supervisor's VoIP phone. In reality, the call is streamed to the PhoneSim service, which proxies it to the VRU node for playback to the dialed-in supervisor.

For more information about the RSM requirements and limitations. See Cisco RSM Bandwidth, Latency and QOS Considerations, on page 149 ,Cisco RSM High Availability, on page 147, Cisco RSM Capabilities, on page 149.

For more information about the RSM configuration. See Configure Cisco RSM, on page 656

## Cisco MediaSense

Cisco MediaSense is the media-capture platform for Cisco Unified Communications. It can be used to record calls in Cisco contact centers. MediaSense can be used by compliance recording companies whose regulatory environment requires all sessions to be recorded and maintained. These recordings can later be used by a compliance auditor or a contact center supervisor to resolve customer issues or for training purposes. The recordings can also be used by speech analytics servers or transcription engines.

MediaSense uses Unified Communications Manager (Unified CM) to provide user-authentication services. It uses Web 2.0 application programming interfaces (APIs) to expose its functionality to third-party customers to enable them to create custom applications. For more information about Cisco MediaSense, see Cisco MediaSense, on page 672 and Cisco MediaSense Considerations, on page 150.

## Cisco Unified SIP Proxy

The Cisco ® Unified SIP Proxy (USP) is a high-performance, highly available Session Initiation Protocol (SIP) server for centralized routing and SIP signaling normalization. By forwarding requests between call-control domains, the Cisco Unified SIP Proxy provides the means for routing sessions within enterprise and service provider networks. The application aggregates SIP elements and applies highly developed routing rules. These rules enhance control, management, and flexibility of SIP networks. For more information on Cisco Unified SIP Proxy, see Cisco Unified SIP Proxy , on page 688

## Avaya PG

Cisco Unified Intelligent Contact Management (Unified ICM) Peripheral Gateway (PG) supports Avaya Automatic Call Distributor (ACD). Avaya PG is the component that communicates to the Avaya ACD device

that has agents on it. Avaya PG supports ACD using CVLAN (Call Visor LAN) Service, running on Avaya Application Enablement Services (AES). CVLAN is an Avaya software option that allows the Unified ICM PG to communicate with the Avaya ACD. CVLAN also allows the PG to perform Post-Routing, station monitoring, and third-party call control. For more information about Avaya PG, see Avaya PG Considerations , on page 153 and Avaya PG, on page 705.

**Note** Avaya PG is an optional cisco component supported for 4000 and 12000 agent deployments only. Each Avaya PG is counted towards the total number of supported PGs.

## Remote Expert Mobile

Callers outside the enterprise's network engage in web-based video chats or expert assist sessions with agents. Unregistered callers can make calls using standard browsers on PC or Mac computers, or tablets and smart-phones. Remote Expert Application Server and Media Broker components provide expert assist functionality, including co-browsing, screen sharing, remote control, annotation, content and URL push, and assisted form completion.

For more information about the Remote Expert Mobile deployment, see, Cisco Contact Center Solutions and Unified Communications Manager Solution Configuration Guide for Remote Expert Mobile.

## Cisco Virtualized Voice Browser

Cisco Virtualized Voice Browser (Cisco VVB) provides a platform for interpreting VoiceXML documents. When a new call arrives at the contact center, the VVB allocates a VXML port that represents the VoIP endpoint. Cisco VVB sends HTTP requests to Cisco Unified Customer Voice Portal (Unified CVP) VXML server. In response to HTTP request, the Unified CVP VXML server executes the request and sends dynamically generated VXML document. For more information about Cisco VVB, see Cisco Virtualized Voice Browser Considerations, on page 154 and Cisco Virtualized Voice Browser, on page 711.

# Optional Third-Party Components

This section describes the following optional third-party components:

# Speech - ASR/TTS

Automatic Speech Recognition (ASR) allows callers to speak words or phrases to choose menu options. For example, after a caller dials, an Automated Attendant receives a welcome message, and is asked for the name of the caller, the caller can say a name and then be connected to that person.

Text-to-Speech (TTS) converts plain text (UNICODE) into speech. For example, VXML gateways either retrieves and plays back the pre-recorded audio files referenced in the VXML document or it streams media from text-to-speech (TTS) server.

# Recording

The Recording option provides network-based, recording, playback, live streaming, and storage of media for compliance, quality management, and agent coaching including audio and video, with rich recording metadata. The platform provides an efficient, cost-effective foundation for capturing, preserving, and mining conversations for business intelligence.

# Wallboard

Wallboard provides the user with the ability to monitor, in real time, the service being provided to customers and display information on customer service metrics such as number of calls waiting, waiting call length, and Service levels.

# Workforce Management

Workforce Management (WFM) is a browser application that can be accessed by any user (agent, supervisor, scheduler, and administrator) who has the Internet Explorer browser. WFM does not use a thick client (which would require installation programs) and therefore, is ideally suited to a highly-distributed workforce environment.

WFM allows the scheduling of multiple Contact Service Queue (CSQs) and sites. A single WFM implementation may be used worldwide. It also allows the managing of key performance indicators and real-time adherence to schedules.

# Cisco Solutions Plus

HCS-CC supports the following applications:

- OnQ Campaign Management Solution
- B+S CRM Connector for SAP, Siebel or Salesforce
- eGain Solutions Plus
- Nuance for CVP
- Nice Interaction Management Solution for Cisco MediaSense
- Calabrio Recording Applications for Cisco MediaSense

- Exony Solutions Plus VIM

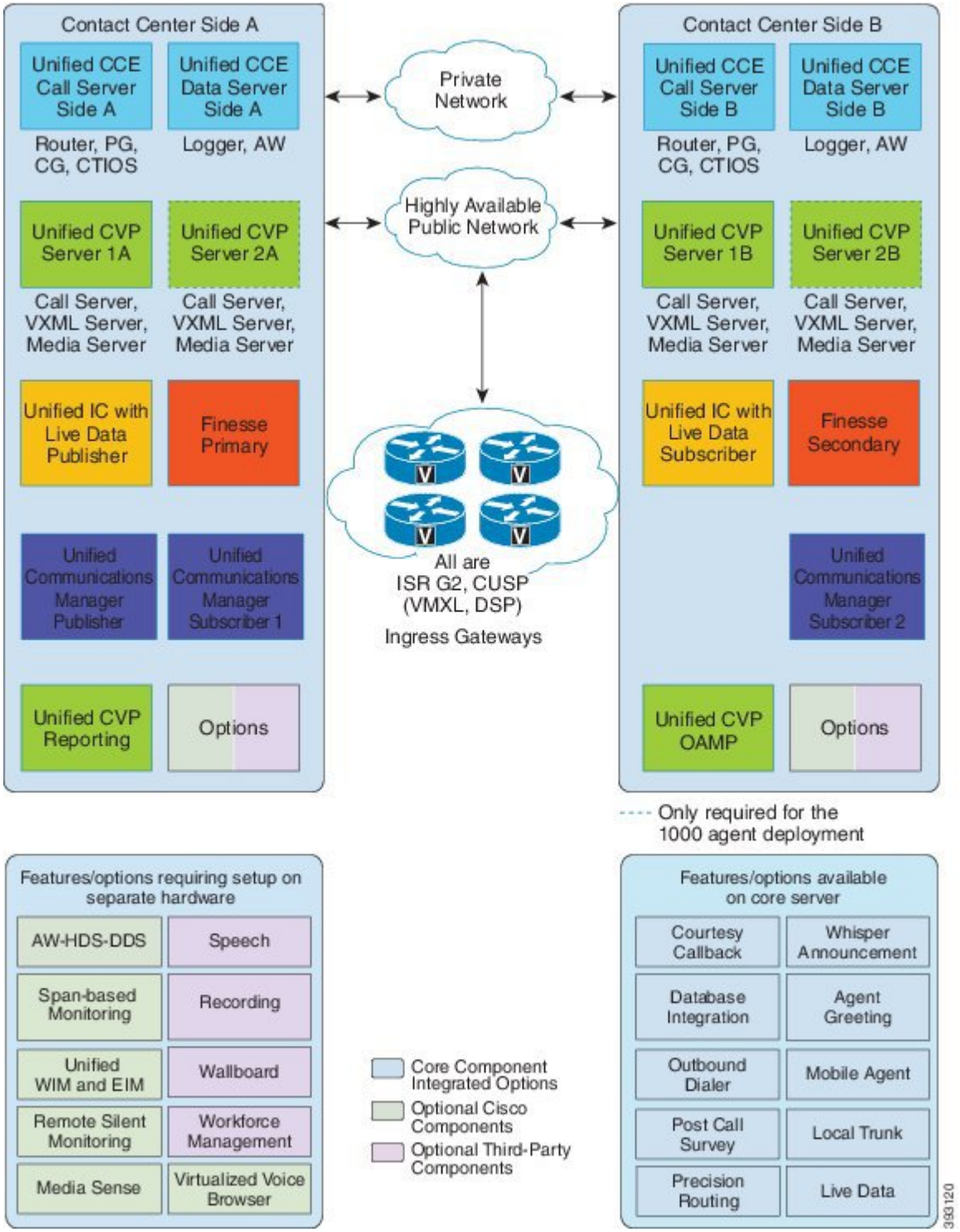
# Deployment Models

This section describes the following deployment models:

# 500 Agent Deployment

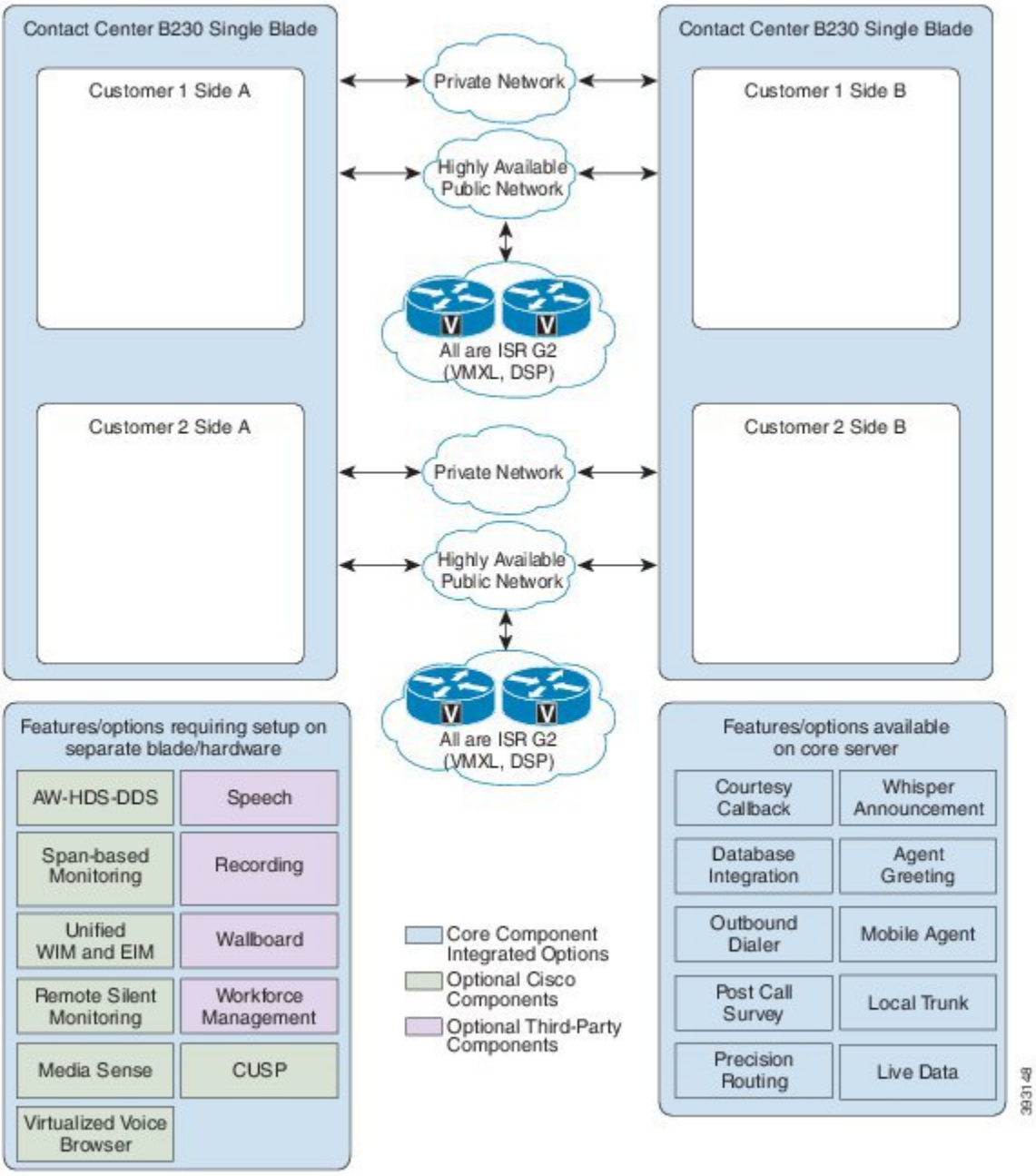
The following figure shows the 500 or 1000 agent deployment with the high density B200 M4 Blades). Use the guidelines for http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware to add additional VM for options.

***Figure 5: 500 Agent or 1000 Agent Deployment Model***


Contact Center Side A
Unified CCE Call Server Side A
Unified CCE Data Server Side A
Router, PG, CG, CTIOS
Logger, AW
Unified CVP Server 1A
Unified CVP Server 2A
Call Server, VXML Server, Media Server
Call Server, VXML Server, Media Server
Unified IC with Live Data Publisher
Finesse Primary
Unified Communications Manager Publisher
Unified Communications Manager Subscriber 1
Unified CVP Reporting
Options
Private Network
Highly Available Public Network
All are ISR G2, CUSP (VMXL, DSP)
Ingress Gateways
Contact Center Side B
Unified CCE Call Server Side B
Unified CCE Data Server Side B
Router, PG, CG, CTIOS
Logger, AW
Unified CVP Server 1B
Unified CVP Server 2B
Call Server, VXML Server, Media Server
Call Server, VXML Server, Media Server
Unified IC with Live Data Subscriber
Finesse Secondary
Unified Communications Manager Subscriber 2
Unified CVP OAMP
Options
Only required for the 1000 agent deployment
Features/options requiring setup on separate hardware
AW-HDS-DDS
Speech
Span-based Monitoring
Recording
Unified WIM and EIM
Wallboard
Remote Silent Monitoring
Workforce Management
Media Sense
Virtualized Voice Browser
Core Component Integrated Options
Optional Cisco Components
Optional Third-Party Components
Features/options available on core server
Courtesy Callback
Whisper Announcement
Database Integration
Agent Greeting
Outbound Dialer
Mobile Agent
Post Call Survey
Local Trunk
Precision Routing
Live Data
393120

The following figure shows the 500 or less agent deployment model allowing a single blade to be shared for two customer instances.

***Figure 6: 500 or Less Agent Deployment Model with Single Blade Shared by Two Customers***



# 1000 Agent Deployment

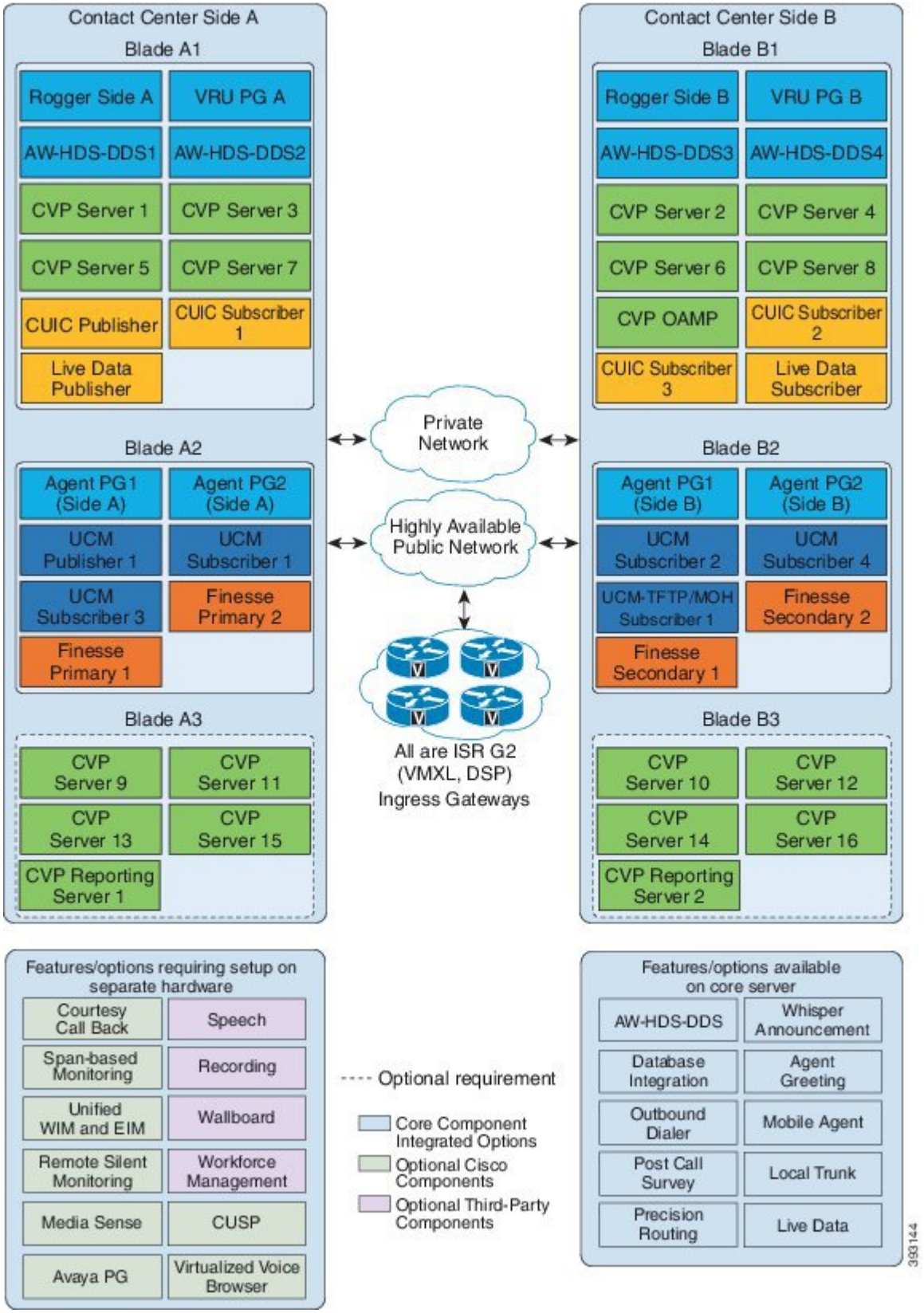
Deployment Models, on page 28 shows the 1000 agent deployment with the high density B200 M4 blades. Use the guidelines for specification-based hardware to add additional VMs for options. For more information about available options, see Deployment Models, on page 28.

# 4000 Agent Deployment

The following figure shows the 4000 agent deployment model with three pairs of high density Tested Reference Configurations. The third pair of blade is optional for both CCB and CVP Reporting server. Also, the third pair of blade is required when the sum of calls at agents and the IVR exceeds 3600. Use the guidelines for specification-based hardware to add additional VMs for options. For more information about available options, see Deployment Models, on page 28.

**Note** The below blade placement is an optimized version for B200 M4 servers only(Tested Reference Configurations.) For any other Specification-based hardware including B230 M2 Blades, the blade placement needs to be designed as per the available vCPU and reservations of the Blades.

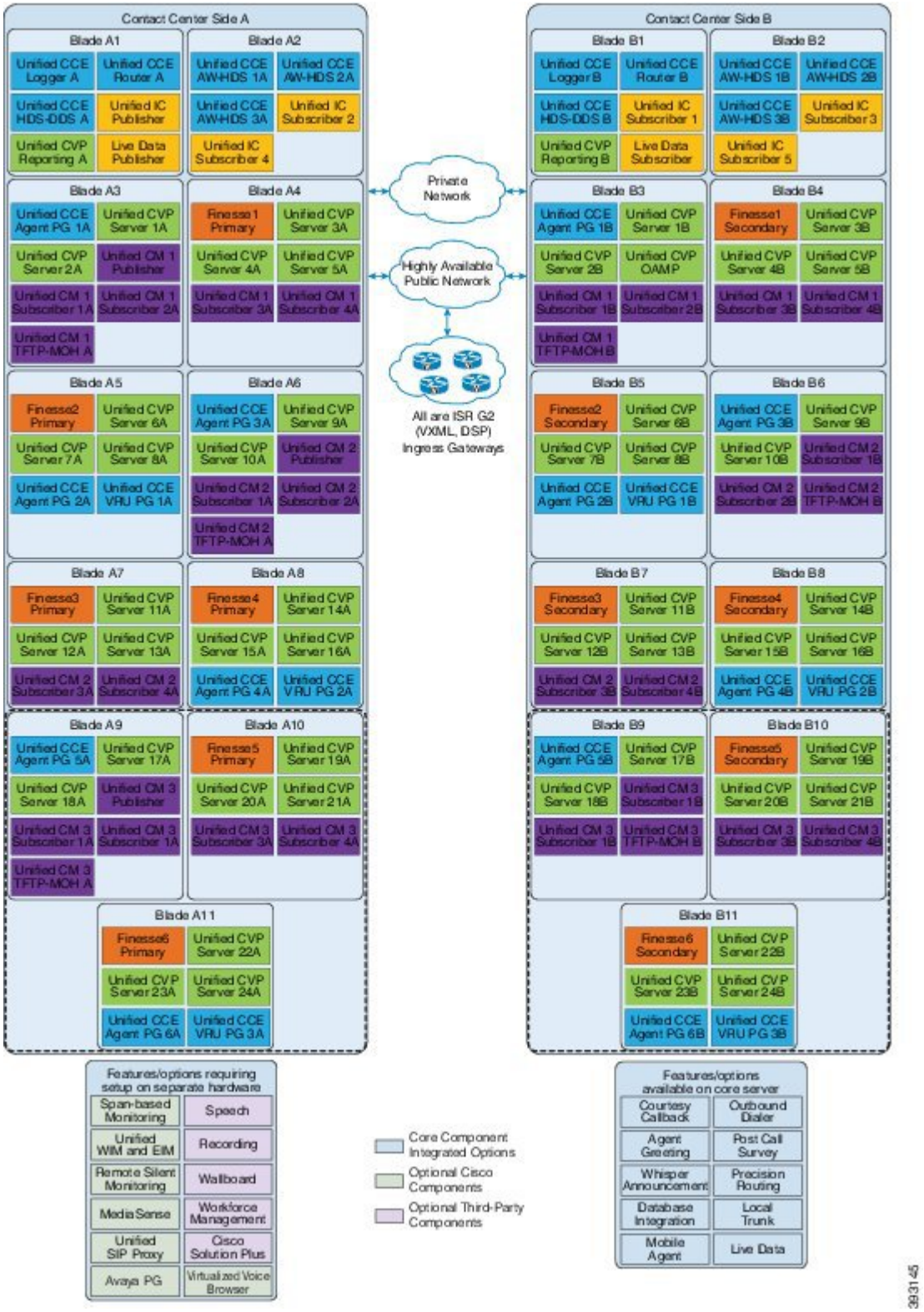
***Figure 7: 4000 Agent Deployment Model***


Contact Center Side A
Blade A1
Rogger Side A
VRU PG A
AW-HDS-DDS1
AW-HDS-DDS2
CVP Server 1
CVP Server 3
CVP Server 5
CVP Server 7
CUIC Publisher
CUIC Subscriber 1
Live Data Publisher
Blade A2
Agent PG1 (Side A)
Agent PG2 (Side A)
UCM Publisher 1
UCM Subscriber 1
UCM Subscriber 3
Finesse Primary 2
Finesse Primary 1
Blade A3
CVP Server 9
CVP Server 11
CVP Server 13
CVP Server 15
CVP Reporting Server 1
Contact Center Side B
Blade B1
Rogger Side B
VRU PG B
AW-HDS-DDS3
AW-HDS-DDS4
CVP Server 2
CVP Server 4
CVP Server 6
CVP Server 8
CVP OAMP
CUIC Subscriber 2
CUIC Subscriber 3
Live Data Subscriber
Blade B2
Agent PG1 (Side B)
Agent PG2 (Side B)
UCM Subscriber 2
UCM Subscriber 4
UCM-TFTP/MOH Subscriber 1
Finesse Secondary 2
Finesse Secondary 1
Blade B3
CVP Server 10
CVP Server 12
CVP Server 14
CVP Server 16
CVP Reporting Server 2
Private Network
Highly Available Public Network
All are ISR G2 (VMXL, DSP) Ingress Gateways
Features/options requiring setup on separate hardware
Courtesy Call Back
Speech
Span-based Monitoring
Recording
Unified WIM and EIM
Wallboard
Remote Silent Monitoring
Workforce Management
Media Sense
CUSP
Avaya PG
Virtualized Voice Browser
Optional requirement
Core Component Integrated Options
Optional Cisco Components
Optional Third-Party Components
Features/options available on core server
AW-HDS-DDS
Whisper Announcement
Database Integration
Agent Greeting
Outbound Dialer
Mobile Agent
Post Call Survey
Local Trunk
Precision Routing
Live Data
393144

# 12000 Agent Deployment Model

The following figure shows the 12000 agent deployment model with eleven pairs of high density Tested Reference Configurations. Use the guidelines for specification-based hardware to add additional VMs for options. For more information about available options, see Deployment Models, on page 28.

***Figure 8: 12000 Agent Deployment Model***


Contact Center Side A
Blade A1
Unified CCE Logger A
Unified CCE Router A
Unified CCE HDS-DDS A
Unified IC Publisher
Unified CVP Reporting A
Live Data Publisher
Blade A2
Unified CCE AW-HDS 1A
Unified CCE AW-HDS 2A
Unified CCE AW-HDS 3A
Unified IC Subscriber 2
Unified IC Subscriber 4
Blade A3
Unified CCE Agent PG 1A
Unified CVP Server 1A
Unified CVP Server 2A
Unified CM 1 Publisher
Unified CM 1 Subscriber 1A
Unified CM 1 Subscriber 2A
Unified CM 1 TFTP-MOH A
Blade A4
Finesse1 Primary
Unified CVP Server 3A
Unified CVP Server 4A
Unified CVP Server 5A
Unified CM 1 Subscriber 3A
Unified CM 1 Subscriber 4A
Blade A5
Finesse2 Primary
Unified CVP Server 6A
Unified CVP Server 7A
Unified CVP Server 8A
Unified CCE Agent PG 2A
Unified CCE VRU PG 1A
Blade A6
Unified CCE Agent PG 3A
Unified CVP Server 9A
Unified CVP Server 10A
Unified CM 2 Publisher
Unified CM 2 Subscriber 1A
Unified CM 2 Subscriber 2A
Unified CM 2 TFTP-MOH A
Blade A7
Finesse3 Primary
Unified CVP Server 11A
Unified CVP Server 12A
Unified CVP Server 13A
Unified CM 2 Subscriber 3A
Unified CM 2 Subscriber 4A
Blade A8
Finesse4 Primary
Unified CVP Server 14A
Unified CVP Server 15A
Unified CVP Server 16A
Unified CCE Agent PG 4A
Unified CCE VRU PG 2A
Blade A9
Unified CCE Agent PG 5A
Unified CVP Server 17A
Unified CVP Server 18A
Unified CM 3 Publisher
Unified CM 3 Subscriber 1A
Unified CM 3 Subscriber 1A
Unified CM 3 TFTP-MOH A
Blade A10
Finesse5 Primary
Unified CVP Server 19A
Unified CVP Server 20A
Unified CVP Server 21A
Unified CM 3 Subscriber 3A
Unified CM 3 Subscriber 4A
Blade A11
Finesse6 Primary
Unified CVP Server 22A
Unified CVP Server 23A
Unified CVP Server 24A
Unified CCE Agent PG 6A
Unified CCE VRU PG 3A
Private Network
Highly Available Public Network
All are ISR G2 (VXML, DSP) Ingress Gateways
Contact Center Side B
Blade B1
Unified CCE Logger B
Unified CCE Router B
Unified CCE HDS-DDS B
Unified IC Subscriber 1
Unified CVP Reporting B
Live Data Subscriber
Blade B2
Unified CCE AW-HDS 1B
Unified CCE AW-HDS 2B
Unified CCE AW-HDS 3B
Unified IC Subscriber 3
Unified IC Subscriber 5
Blade B3
Unified CCE Agent PG 1B
Unified CVP Server 1B
Unified CVP Server 2B
Unified CVP OAMP
Unified CM 1 Subscriber 1B
Unified CM 1 Subscriber 2B
Unified CM 1 TFTP-MOH B
Blade B4
Finesse1 Secondary
Unified CVP Server 3B
Unified CVP Server 4B
Unified CVP Server 5B
Unified CM 1 Subscriber 3B
Unified CM 1 Subscriber 4B
Blade B5
Finesse2 Secondary
Unified CVP Server 6B
Unified CVP Server 7B
Unified CVP Server 8B
Unified CCE Agent PG 2B
Unified CCE VRU PG 1B
Blade B6
Unified CCE Agent PG 3B
Unified CVP Server 9B
Unified CVP Server 10B
Unified CM 2 Subscriber 1B
Unified CM 2 Subscriber 2B
Unified CM 2 TFTP-MOH B
Blade B7
Finesse3 Secondary
Unified CVP Server 11B
Unified CVP Server 12B
Unified CVP Server 13B
Unified CM 2 Subscriber 3B
Unified CM 2 Subscriber 4B
Blade B8
Finesse4 Secondary
Unified CVP Server 14B
Unified CVP Server 15B
Unified CVP Server 16B
Unified CCE Agent PG 4B
Unified CCE VRU PG 2B
Blade B9
Unified CCE Agent PG 5B
Unified CVP Server 17B
Unified CVP Server 18B
Unified CM 3 Subscriber 1B
Unified CM 3 Subscriber 1B
Unified CM 3 TFTP-MOH B
Blade B10
Finesse5 Secondary
Unified CVP Server 19B
Unified CVP Server 20B
Unified CVP Server 21B
Unified CM 3 Subscriber 3B
Unified CM 3 Subscriber 4B
Blade B11
Finesse6 Secondary
Unified CVP Server 22B
Unified CVP Server 23B
Unified CVP Server 24B
Unified CCE Agent PG 6B
Unified CCE VRU PG 3B
Features/options requiring setup on separate hardware
Span-based Monitoring
Speech
Unified WIM and EIM
Recording
Remote Silent Monitoring
Whiteboard
MediaSense
Workforce Management
Unified SIP Proxy
Cisco Solution Plus
Avaya PG
Virtualized Voice Browser
Core Component Integrated Options
Optional Cisco Components
Optional Third-Party Components
Features/options available on core server
Courtesy Callback
Outbound Dialer
Agent Greeting
Post Call Survey
Whisper Announcement
Precision Routing
Database Integration
Local Trunk
Mobile Agent
Live Data
393145

**Note** Blade A9-A11 and B9-B11 are required for the following cases:

1. If the required number of active agents are greater than 8000
2. If the sum of total calls at agents and IVR are greater than 14400

# Small Contact Center Deployment

This deployment model uses shared Contact Center core components with two options based on the placement of peripheral components. Dedicated sub customer Unified CM and Peripheral gateways deployment supports up to 500 agents. In Shared Unified CM and Peripheral Gateway deployment sub customers can deploy on their shared infrastructure within the contact center core.

- **Dedicated components sub-customer option –** Dedicated Cisco Unified CM, Peripheral Gateway and Finesse sized for either 100 or 500 agents.
- **Shared components sub-customer option –** Shared Cisco Unified CM, Peripheral Gateway and Finesse support up to 2000 agents across 100 Department enabled sub-customers.

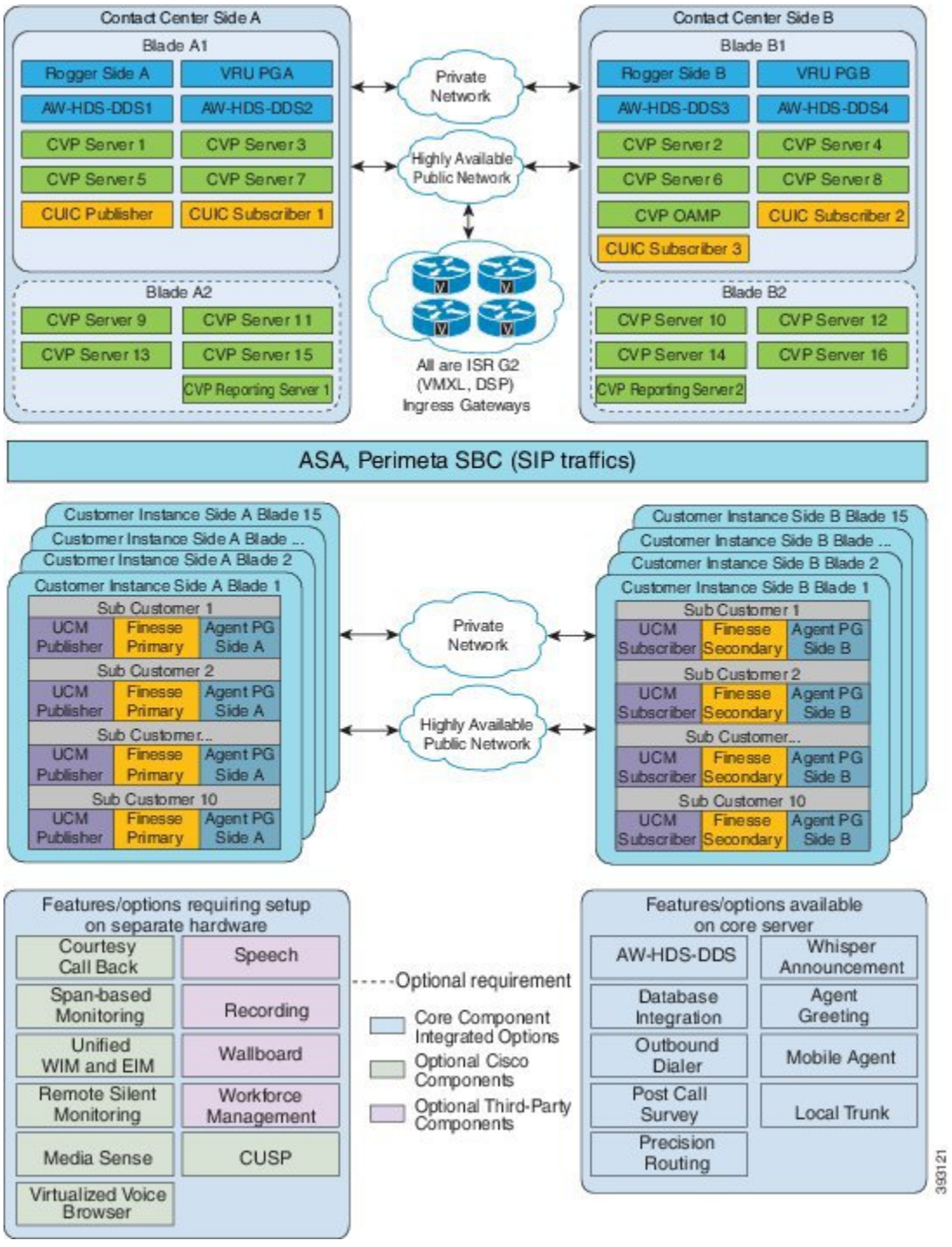
Sub customer can avail any one of the option in their infrastructure.

The following figure shows the less than 100 agent deployment model with two pairs of high density Table 2: B200 M4 Blades, on page 48. The second pair of blades is optional for both CCB and CVP Reporting server but is required when the total calls at agents and the IVR exceeds 3600. Use the guidelines for specification-based hardware to add additional VMs for options. For more information about available options, see Deployment Models, on page 28.

**Note**

- For Cisco Finesse installation, you can use a local DNS server or shared DNS. For more information see, Create DNS Server for Finesse in Small Contact Center Deployment, on page 436..
- The blade placement below is an optimized version for UCSB200 M4 servers only (Tested Reference Configuration). For any other Specification-based hardware including B230 M2 Blades, the blade placement needs to be designed as per the available vCPU and reservations of the Blades.

***Figure 9: Small Contact Center Deployment Model for 100 Agents***


Contact Center Side A
Blade A1
Rogger Side A
VRU PG A
AW-HDS-DDS1
AW-HDS-DDS2
CVP Server 1
CVP Server 3
CVP Server 5
CVP Server 7
CUIC Publisher
CUIC Subscriber 1
Blade A2
CVP Server 9
CVP Server 11
CVP Server 13
CVP Server 15
CVP Reporting Server 1
Private Network
Highly Available Public Network
All are ISR G2 (VMXL, DSP) Ingress Gateways
Contact Center Side B
Blade B1
Rogger Side B
VRU PG B
AW-HDS-DDS3
AW-HDS-DDS4
CVP Server 2
CVP Server 4
CVP Server 6
CVP Server 8
CVP OAMP
CUIC Subscriber 2
CUIC Subscriber 3
Blade B2
CVP Server 10
CVP Server 12
CVP Server 14
CVP Server 16
CVP Reporting Server 2
ASA, Perimeta SBC (SIP traffics)
Customer Instance Side A Blade 15
Customer Instance Side A Blade ...
Customer Instance Side A Blade 2
Customer Instance Side A Blade 1
Sub Customer 1
UCM Publisher
Finesse Primary
Agent PG Side A
Sub Customer 2
Sub Customer...
Sub Customer 10
Private Network
Highly Available Public Network
Customer Instance Side B Blade 15
Customer Instance Side B Blade ...
Customer Instance Side B Blade 2
Customer Instance Side B Blade 1
Sub Customer 1
UCM Subscriber
Finesse Secondary
Agent PG Side B
Sub Customer 2
Sub Customer...
Sub Customer 10
Features/options requiring setup on separate hardware
Courtesy Call Back
Speech
Span-based Monitoring
Recording
Unified WIM and EIM
Wallboard
Remote Silent Monitoring
Workforce Management
Media Sense
CUSP
Virtualized Voice Browser
Optional requirement
Core Component Integrated Options
Optional Cisco Components
Optional Third-Party Components
Features/options available on core server
AW-HDS-DDS
Whisper Announcement
Database Integration
Agent Greeting
Outbound Dialer
Mobile Agent
Post Call Survey
Local Trunk
Precision Routing
393121

**Note** Small Contact Center 100 agent deployment model with dedicated components sub-customer option does not support Live Data Reporting System.

***Figure 10: Small Contact Center Deployment Model for 500 Agents***

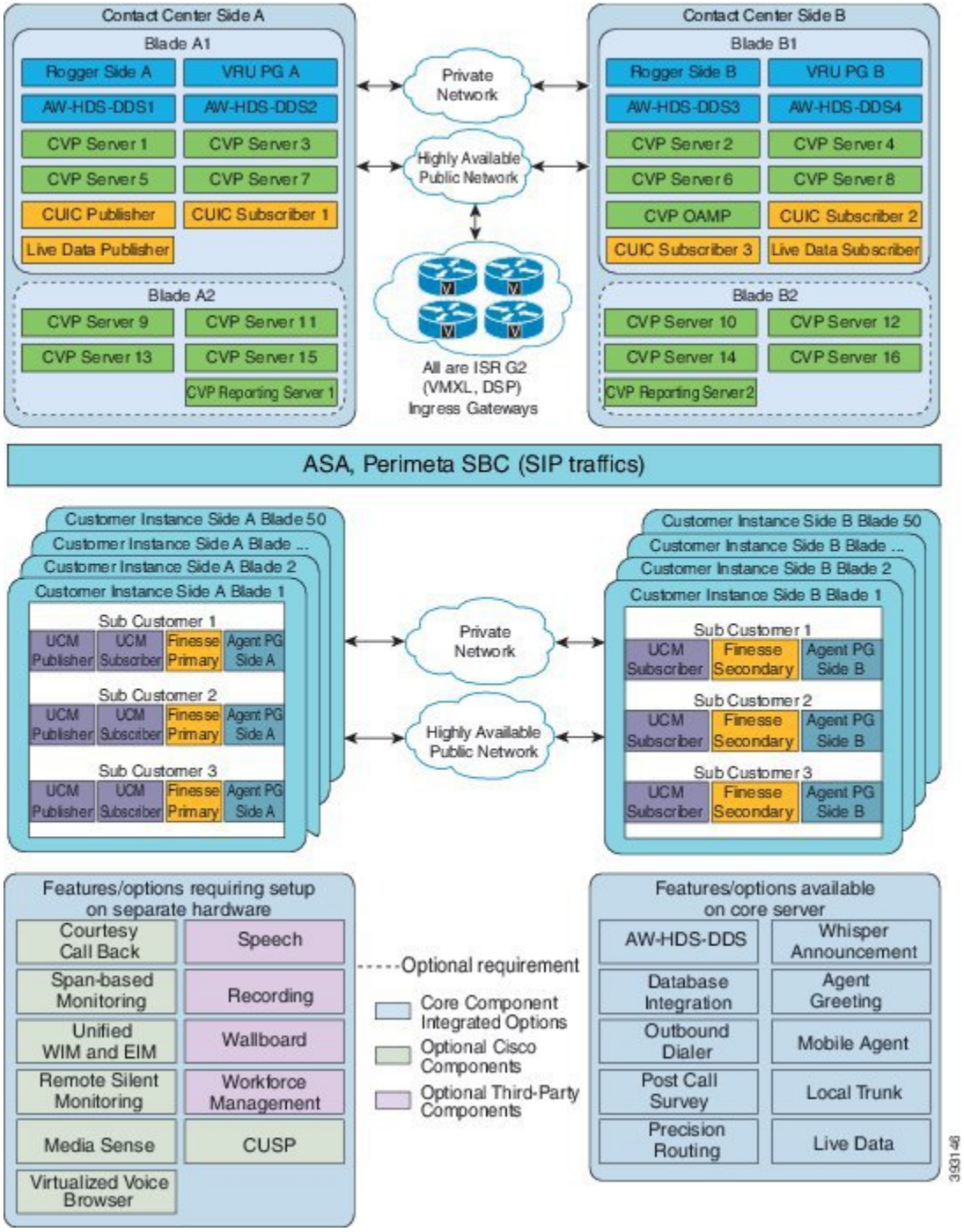
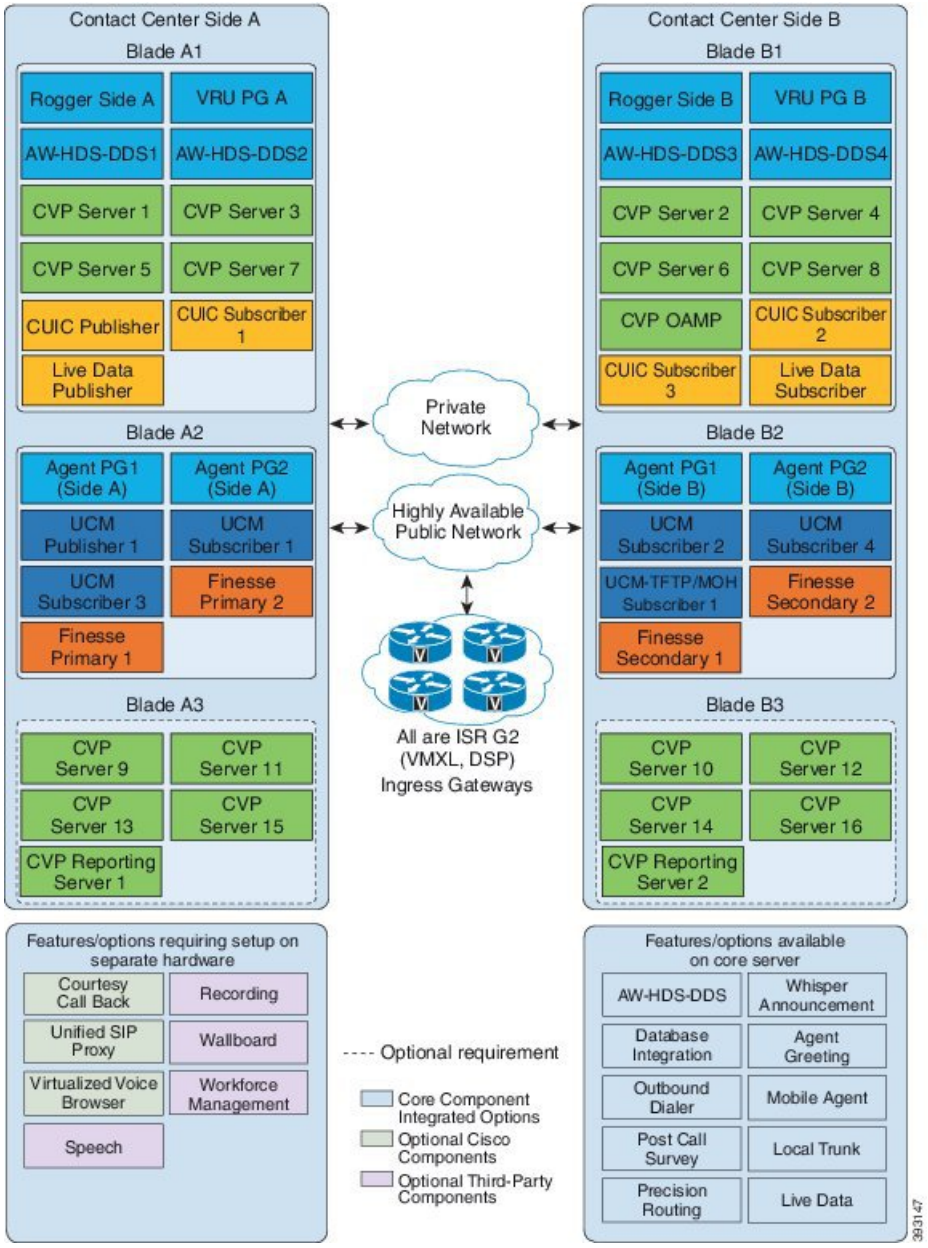



*Figure 11: Small Contact Center Deployment Model for Shared Component Sub Customer Option*




# Remote Deployment options

HCS for Contact Center provides the following remote deployment options.

- Global Deployments, on page 43
- Local Trunk, on page 44
- Remote Office Options, on page 44

# Global Deployments

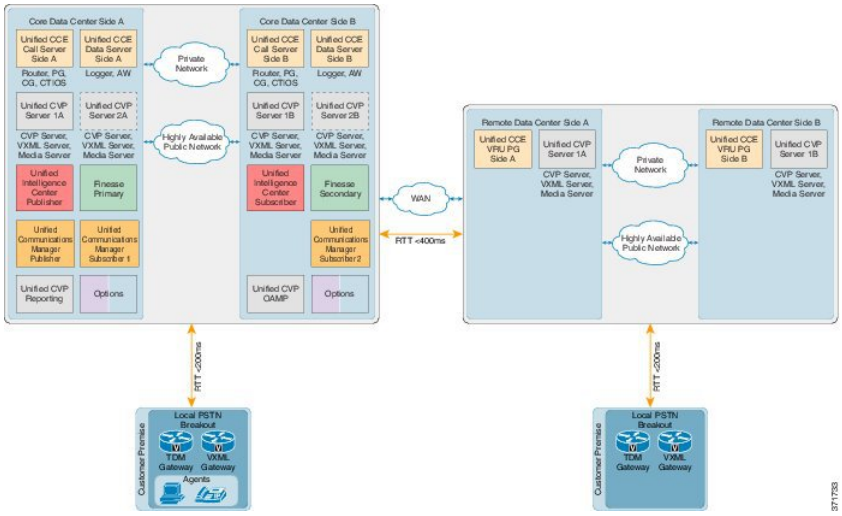
Global deployments enables the Service Providers to deploy a Single contact center available world-wide with a Centralized data center and global access. This helps in reduced deployment costs by eliminating multiple customer instances. The HCS-Unified Communications Manager can be located in a centralized/remote data center or customer premise and the Remote components can be deployed either on B-series blades or Cseries servers. The following Global deployment topologies are supported


- Remote CVP Deployment, on page 43
- Remote CVP and UCM Deployment, on page 43


## Remote CVP Deployment

The topology shown in the below illustration shows a simple example of Remote CVP deployment, that requires additional Unified CVP servers with Unified CCE VRU PG Servers at remote Data centers. The maximum RTT with central controller over the WAN is restricted upto 400ms.

***Figure 12: Remote CVP Deployment Topology***

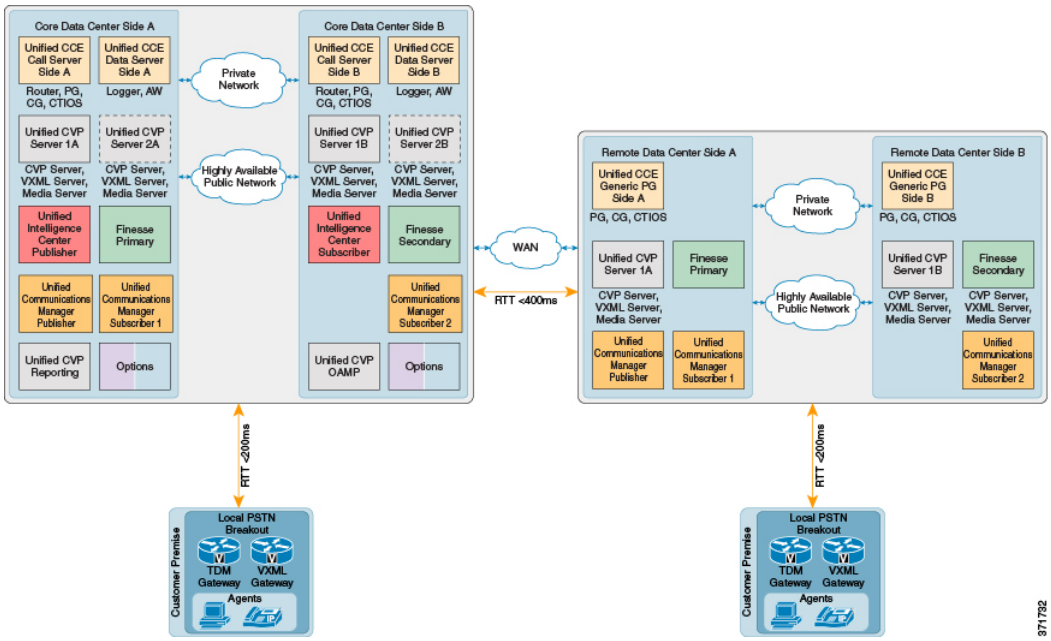



## Remote CVP and UCM Deployment

The topology shown in the below illustration shows a simple example of Remote CVP deployment, that requires additional Unified CVP and Unified Communication Manager servers with Unified CCE Generic

PG Servers at remote Data centers. The maximum RTT with central controller over the WAN is restricted upto 400ms.

***Figure 13: Remote CVP and CUCM Deployment Topology***




# Local Trunk

The HCS for Contact Center has two options for local trunks at the customer premise:

- Cisco Unified Border Element—Enterprise at the customer premise
- TDM gateway at the customer premise

**Note** Transcoding resources are not deterministically picked from the local customer premise gateway.

For more information, refer Local Trunk Design Considerations, on page 163.

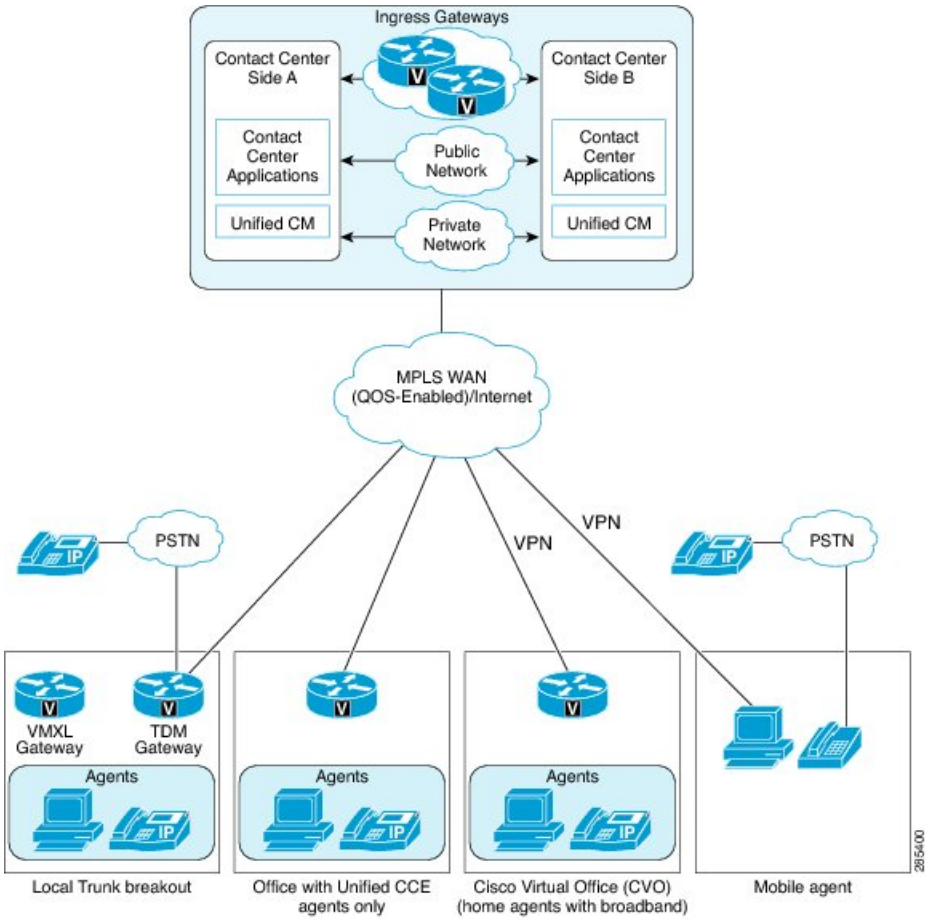
# Remote Office Options

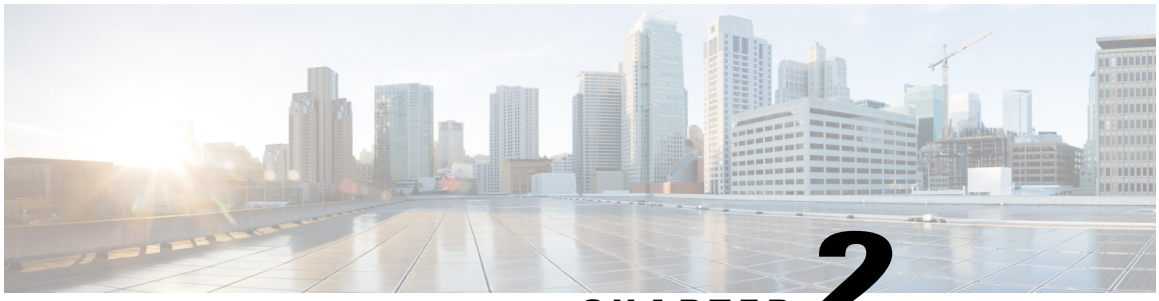
Remote office options include:

- Local trunk breakout
- Office only with Unified CCE agents
- Cisco Virtual Office

- Mobile Agent

***Figure 14: Remote Office Options***





CHAPTER 2

# Prerequisites



# Hardware Requirements

HCS for Contact Center Release supports Tested Reference Configurations (see Tested Reference Configurations, on page 47) and Specification-Based Hardware (see Specification-Based Hardware Support, on page 48)

HCS for Contact Center supports the following configurations:



## Tested Reference Configurations

This section lists the specifications for the UCSB200 M4 Blade server. At the *source* system, the service provider uses one core server for the golden template environment. The customer *destination* system must run in a duplexed environment using a pair of core Unified Computing System (UCS) UCSB200 M4 blade servers known as Side A and Side B.

*Table 2: B200 M4 Blades*

| Server Model | Cisco UCS B200 M4 Tested Reference Configuration (TRC) blade server |
|---|---|
| CPU Type | Intel(R) Xeon(R) 2.60 GHz E5-2660 v3/105W 10C/25MB Cache |
| CPU Cores | Two 10-core CPUs |
| Memory | 16 X [16GB DDR3-1866-MHz-RDIMM/PC-3-14900/dual rank/x4/1.5v] |
| Disks | Diskless |
| Virtual Interface | Cisco UCS VIC 1240 modular LOM for M4 blade servers |
| Part Number | UCS-UC-B200M4 |

# Specification-Based Hardware Support

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

*Table 3: Hardware Requirements*

| Server | Component | Description |
|---|---|---|
| Cisco UCS B2XX Blade Server, such as<br>• Cisco UCS-B200M2-VCS1 Blade Server<br>• Cisco UCS-B200M4 Blade Server<br>• Cisco UCS-B230M2-VCDL1 Blade Server | CPU Type | You must use the processors that meet the requirements of full UC performance. For more information about CPU types, see http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#CPU.C2.A0Table_1_-_Allowed_Specs-based_CPUs |
| | Memory | 128 GB minimum |
| | Virtual Interface Card | All Cisco Virtual Interface Cards (VICs) are supported. |

**Note** For specification-based hardware, total CPU reservations must be within 65 percent of the available host CPU and total memory reservations must be within 80% of the available host memory.

## Additional Hardware Specification

The following table lists the additional hardware specification for HCS for Contact Center.

| Server | Components | Description |
|---|---|---|
| Cisco Unified Border Element Enterprise Gateway | CUBE-E | ISR G2 with a combination of TDM and VXML.<br>29*xx*, 39*xx* series routers. |
| Cisco UCS C240 M3/M4 Rack Server | Perimeta SBC | Install on C-Series rack server |
| Cisco Unified SIP Proxy | CUSP | Services Module with Services Ready Engine |
| Adaptive Security Appliance | ASA | Cisco ASA 55*xx* series<br>For small contact center it should be 5585 or 5580. |

# Software Requirement

The following table contains the software requirements for core Cisco components of Cisco HCS for Contact Center.

| Components | Major Release Version |
|---|---|
| Unified Contact Center Enterprise | 11.0(2) ES1 or later MR |
| Unified CVP | 11.0(1) or later MR |
| Cisco Finesse | 11.0(1) or later MR |
| Unified Intelligence Center | 11.0(1) or later MR |
| Live Data Reporting System | 11.0(1) or later MR |
| Unified CCDM | 11.0(1) or later MR |
| Unified Communication Manager | 10.5(2) ES43 or later MR |
| Unified Communications Domain Manager | 10.6 or later MR |

| Components | Major Release Version |
|---|---|
| Cisco IOS Gateways | 15.5(3)T or later MR |

**Note**

- You can use UCDM 8.1.6 or later MR version for HCS-CC instances that are upgraded from previous releases.
- Cisco Virtualized Voice Browser requires CVP 11.0(1) ES8 or later MR version to be installed on all CVP servers.

For Nexus, ASA, and Perimeta SBC supported release version, see http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html compatibility matrix document.

The following table contains the software requirements for optional Cisco components of Cisco HCS for Contact Center.

| Component | Major Release Version |
|---|---|
| Unified WIM and EIM | 11.0(1) or later MR |
| Cisco RSM | 11.0(1) or later MR |
| Cisco MediaSense | 11.0(1) or later MR |
| Avaya PG | 10.5(2) or later releases |
| Cisco Virtualized Voice Browser | 11.0(1) or later |

# Automation Software

**Note** Automation software is required for golden templates only.

| Software | Version | Download | Notes |
|---|---|---|---|
| GoldenTemplateTool zip file | 11.0(1) | https://communities.cisco.com/docs/DOC-58859 | Download and extract the *GoldenTemplateTool* .zip file to run the automation tool. See Automated Cloning and OS Customization, on page 300. |
| PowerCLI | 5.5, 32-bit | http://downloads.vmware.com/ | Use PowerCLI to run the automation script. |
| OVF Tool | 32-bit | https://my.vmware.com/group/vmware/ | downloadGroup=OVFTOOL350&productId=353 |

| Software | Version | Download | Notes |
|---|---|---|---|
| WinImage | 8.5 , 32-bit | See http://winimage.com/download.htm.<br>**Note** WinImage is shareware. If you choose to not purchase a licensed copy, you will see pop-ups when you run this tool. Clicking **No** at the pop-ups will allow you to proceed. | WinImage creates a floppy image (.flp file) from the platformConfig.xml file. This file contains parameters for customizing VOS primary and secondary nodes. |

# Third-Party Software

| Software | Version | Notes |
|---|---|---|
| Microsoft Windows Server 2012 R2 Standard Edition | Service Pack 1 | Used for Windows based Virtual Machines. |
| Microsoft SQL Server 2014 x64 Standard Edition | Service Pack 1 | Used for Unified CCE, CCDM, and WIM databases |
| vCenter Server | 5.1, 5.5 or 6.0 | Required for deploying virtual machines. |
| ESXi Server | 5.1, 5.5 or 6.0 | Required for deploying virtual machines. |
| vSphere Client | 5.1, 5.5 or 6.0 | Required for managing a virtualize infrastructure. |
| Java Development Kit (JDK) | Version 1.7 | — |
| Microsoft Excel | Release 2003 or later | Required to complete GT Tool Automation Spreadsheet. |
| **Anti-Virus:** | | |
| Symantec Endpoint Protection | 12.1 | Required for all applications that run on the Windows platform.<br>For more information, see Install Antivirus Software, on page 253. |
| Trend Micro Server Protect version | 5.8 | |
| McAfee VirusScan Enterprise | 8.8i | |

| Software | Version | Notes |
|---|---|---|
| **Browser:** | | |
| Internet Explorer | 9.0 or later | Required for Contact Center Provisioning and Web Administration. |
| Firefox | 24 or later | |

# Required Software Licenses

Following information contains the number of software licenses required to deploy a single instance of Cisco Hosted Collaboration Solution for Contact Center:

***Table 4: License Requirement for Shared Components***

| Development Type | Software Type | Total Number of Licenses |
|---|---|---|
| Unified CCDM (dual-tier) | Microsoft Windows Server 2012 R2 Standard Edition | 4 |
| | Microsoft Windows SQL Server 2014 x64 Standard Edition | 2 |

***Table 5: License Requirement for Core Components***

| Development Type | Software Type | Components | Total Number of Licenses | Total Number of Licenses |
|---|---|---|---|---|
| 500 Agent | Microsoft Windows Server 2012 R2 Standard Edition | Unified CCE<br>Unified CVP | 4<br>4 | 8 |
| | Microsoft Windows SQL Server 2014 x64 Standard Edition | Unified CCE | 2 | 2 |
| 1000 Agent | Microsoft Windows Server 2012 R2 Standard Edition | Unified CCE<br>Unified CVP | 4<br>6 | 10 |
| | Microsoft Windows SQL Server 2014 x64 Standard Edition | Unified CCE | 2 | 2 |

| Development Type | Software Type | Components | Total Number of Licenses | Total Number of Licenses |
|---|---|---|---|---|
| 4000 Agent | Microsoft Windows Server 2012 R2 Standard Edition | Unified CCE<br>Unified CVP | 12<br>19 | 31 |
| | Microsoft Windows SQL Server 2014 x64 Standard Edition | Unified CCE | 6 | 6 |
| 12000 Agent | Microsoft Windows Server 2012 R2 Standard Edition | Unified CCE<br>Unified CVP | 30<br>51 | 81 |
| | Microsoft Windows SQL Server 2014 x64 Standard Edition | Unified CCE | 10 | 10 |
| SCC (Core Components) | Microsoft Windows Server 2012 R2 Standard Edition | Unified CCE<br>Unified CVP | 8<br>19 | 27 |
| | Microsoft Windows SQL Server 2014 x64 Standard Edition | Unified CCE | 6 | 6 |
| SCC (Per sub customer) | Microsoft Windows Server 2012 R2 Standard Edition | Unified CCE | 2 | 2 |

**Note** You can use same 4000 agent deployment model licenses for shared component sub-customer option of Small Contact Center deployment model.

***Table 6: License Requirement for Optional Components***

| Development Type | Software Type | Total Number of Licenses |
|---|---|---|
| Cisco RSM | Microsoft Windows Server 2012 R2 Standard Edition | 1 |

# Open Virtualization Format Files

Open Virtualization Format files (OVAs) are required for golden templates. HCS for Contact Center uses the OVAs that define the basic structure of the corresponding VMs that are created - including 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.

The following OVA files are packaged into HCS-CC 11.0.1-OVA.zip file. Download and extract this file and save the OVAs to your local drive. You can browse to them for vcenter:


- Hosted Collaboration Solution for Contact Center OVA, on page 54
- Unified Communications Manager OVA, on page 56
- Unified Intelligence Center OVA, on page 56
- Live Data Reporting System OVA, on page 56
- Cisco Finesse OVA, on page 57
- Cisco Remote Silent Monitoring OVA, on page 57
- Cisco MediaSense OVA, on page 57
- Avaya PG OVA, on page 57
- Cisco Virtualized Voice Browser OVA, on page 58


## Hosted Collaboration Solution for Contact Center OVA

The Cisco Hosted Collaboration Solution for Contact Center OVA filename **HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova** contains the deployment configurations for 500, 1000, 4000, 12000 and Small Contact Center agent deployments.

The Shared Management requires the following configurations:

- Unified CCDM Database Server
- Unified CCDM Web Server

The 500 agent deployment requires the following configurations:

- CCE Call Server- 500 Agent
- CCE Data Server- 500 Agent
- CVP Call/VXML Server
- CVP Reporting Server- 500 Agent
- CVP OAMP Server

The 1000 agent deployment requires the following configurations:

- CCE Call Server- 1000 Agent
- CCE Data Server- 1000 Agent
- CVP Call/VXML Server
- CVP Reporting Server- 1000 Agent
- CVP OAMP Server

The 4000 agent deployment requires the following configurations:

- CCE Rogger Server
- CCE AW-HDS-DDS Server
- CCE Agent PG Server
- CCE VRU PG Server
- CVP Call/VXML Server
- CVP Reporting Server
- CVP OAMP Server

The 12000 agent deployment requires the following configurations:

- CCE Router Server - 12000 Agent
- CCE Logger Server - 12000 Agent
- CCE AW-HDS Server - 12000 Agent
- CCE HDS-DDS Server - 12000 Agent
- CCE Agent PG Server
- CCE VRU PG Server
- CVP Call/VXML Server
- CVP Reporting Server
- CVP OAMP Server

The Small Contact Center(SCC) agent deployment requires the following configurations:

- **Shared Core Components**
  - CCE Rogger Server
  - CCE AW-HDS-DDS Server
  - CCE VRU PG Server
  - CVP Call/VXML Server
  - CVP Reporting Server
  - CVP OAMP Server

- **Shared Sub Customer Component**

- CCE Agent PG Server

- **Sub Customer Component**
  - CCE Agent PG Server - SCC100 Agent
  - CCE Agent PG Server - SCC500 Agent

# Unified Communications Manager OVA

The Unified Communications Manager OVA filename **cucm_10.5_vmv8_v1.9.ova** contains the Unified Communications Manager deployment configuration for the Publisher and Subscriber nodes.

**Note** After you deploy OVA for 500 agent deployment model, modify the vCPU value to 2.

- The 500 agent deployment requires **CUCM 2500 user node** configurations
- The 1000 agent deployment requires **CUCM 7500 user node** configurations
- The 4000 agent deployment requires **CUCM 7500 user node** configurations
- The 12000 agent deployment requires **CUCM 7500 user node** configurations
- The Small Contact Center agent deployment with 100 agents requires **CUCM 2500 user node** configurations.
- The Small Contact Center agent deployment with 500 agent requires **CUCM 7500 user node** configurations.

# Unified Intelligence Center OVA

The Cisco Unified Intelligence Center Reporting Server OVA filename **HCS-CC_11.0(1)_CUIC_vmv8_v2.3.ova** contains the Unified Intelligence Center deployment configuration for the Publisher and Subscriber nodes.

- The 500 agent deployment requires **CUIC _LIVEDATA for HCS - 500 Agent** configurations
- The 1000 agent deployment requires **CUIC _LIVEDATA for HCS - 1000 Agent** configurations
- The 4000 agent deployment requires **CUIC for HCS** configurations
- The 12000 agent deployment requires **CUIC for HCS** configurations
- The Small Contact Center agent deployment requires **CUIC for HCS** configurations

# Live Data Reporting System OVA

The Cisco Live Data Reporting System OVA filename **UCCELD_11.0_CVOS_vmv8_v1.0.ova** contains the following Live Data Reporting System deployment configurations:

- The 4000 agent deployment requires **Large Live Data Server** configurations
- The 12000 agent deployment requires **Large Live Data Server** configurations
- Small Contact Center agent deployment requires **Large Live Data Server** configurations

## Cisco Finesse OVA

The Cisco Finesse OVA filename **HCS-CC_11.0(1)_Finesse_vmv8_v1.0.ova** contains the Cisco Finesse deployment configuration for the Primary and Secondary nodes.

- The 500 agent deployment requires **Cisco Finesse - 500 Agent** configuration.
- The 1000 agent deployment requires **Cisco Finesse** configurations.
- The 4000 agent deployment requires **Cisco Finesse** configurations.
- The 12000 agent deployment requires **Cisco Finesse** configurations.
- The Small Contact Center 100 agent deployment requires **Cisco Finesse - SCC 100 Agent** configurations
- The Small Contact Center 500 agent deployment requires **Cisco Finesse - 500 Agent** configurations

## Cisco Remote Silent Monitoring OVA

The Cisco Remote Silent Monitoring OVA filename **HCS-CC_11.0(1)_CCE-RSM_vmv9_v1.0.ova** contains the Cisco Remote Silent Monitoring deployment configurations.

## Cisco MediaSense OVA

The Cisco MediaSense OVA filename **cms_11.0_vmv8_v1.0.ova** contains the following Cisco MediaSense deployment configurations.

- Primary/Secondary node 2 vCPU
- Primary/Secondary node 4 vCPU
- Primary/Secondary node 7 vCPU
- Expansion node 7 vCPU

## Avaya PG OVA

The Avaya PG OVA filename **HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova** contains the Avaya PG deployment configurations.

- The 4000 agent deployment requires **CCE Agent PG Server**
- The 12000 agent deployment requires **CCE Agent PG Server**

## Cisco Virtualized Voice Browser OVA

The Cisco Virtualized Voice Browser OVA file **VB_11.0_vmv8_v2.5.ova** contains the required configuration for deployment of virtual machine.

# Deployment Checklists



## Checklists for 500 and 1000 Agent Deployment

| Sequence | Task | Done |
|---|---|---|
| 1 | **Prerequisites** | |
| | Hardware Requirements, on page 47 | |
| | Software Requirement, on page 49 | |
| | Required Software Licenses, on page 52 | |
| 2 | **Design Consideration** | |
| | Storage, VM Specifications, and IOPS Considerations, on page 168 | |
| 3 | **Shared Management and Aggregation** | |
| | Install and Configure Unified CCDM, on page 195 | |
| | Install and Configure Unified Communication Domain Manager, on page 221 | |
| | Install and Configure ASA Firewall and NAT, on page 227 | |
| 4 | **Create Golden Template** | |
| | Create Golden Template for Unified CCE Call Server, on page 250 | |
| | Create Golden Template for Unified CCE Data Server, on page 255 | |
| | Create Golden Template for Unified CVP Server, on page 259 | |
| | Create Golden Template for Unified CVP OAMP Server, on page 261 | |
| | Create Golden Template for Unified CVP Reporting Server, on page 262 | |
| | Create Golden Template for Cisco Finesse, on page 264 | |

| Sequence | Task | Done |
|---|---|---|
| | Create Golden Template for Cisco Unified Intelligence Center , on page 272 | |
| | Create Golden Template for Cisco Unified Communications Manager, on page 266 | |
| 5 | **Configure Customer Instance Network Infrastructure** | |
| | Implement UCS Platform, on page 281 | |
| | ESX Boot from SAN, on page 288 | |
| | Deploy Nexus 1000v, on page 291 | |
| | Establish Two-Way Forest Trust, on page 456 | |
| 6 | **Clone and OS Customization,** | |
| | Download Golden Template Automation Tool, on page 300 | |
| | Complete Automation Spreadsheet, on page 301 | |
| | Run Automation Script, on page 303 | |
| 7 | **Configure Customer Instance** | |
| | Configure Cisco Unified CCE Call Server, on page 323 | |
| | Configure Unified CCE Data Server, on page 338 | |
| | Configure Unified CVP, on page 347 | |
| | Configure Cisco IOS Enterprise Voice Gateway, on page 369 | |
| | Configure Unified Intelligence Center , on page 423 | |
| | Configure Unified Communications Manager, on page 375 | |
| | Configure Cisco Finesse, on page 392 | |
| 8 | **Administration** | |
| | Provision Unified CCE Using Unified CCDM, on page 501 | |
| | Provision Unified Communications Manager Using UCDM, on page 566 | |

# Checklists for 4000 Agent Deployment

| Sequence | Task | Done |
|---|---|---|
| 1 | **Prerequisites** | |
| | Hardware Requirements, on page 47 | |
| | Software Requirement, on page 49 | |

| Sequence | Task | Done |
|---|---|---|
| | Required Software Licenses, on page 52 | |
| 2 | **Design Consideration** | |
| | Storage, VM Specifications, and IOPS Considerations, on page 168 | |
| 3 | **Shared Management and Aggregation** | |
| | Install and Configure Unified CCDM, on page 195 | |
| | Install and Configure Unified Communication Domain Manager, on page 221 | |
| | Install and Configure ASA Firewall and NAT, on page 227 | |
| 4 | **Create Golden Template** | |
| | Create Golden Template for Unified CCE Rogger, on page 268 | |
| | Create Golden Template for Unified CCE AW-HDS-DDS, on page 269 | |
| | Create Golden Template for Unified CCE Agent Peripheral Gateway, on page 270 | |
| | Create Golden Template for Unified CCE VRU Peripheral Gateway, on page 271 | |
| | Create Golden Template for Unified CVP Server, on page 259 | |
| | Create Golden Template for Unified CVP OAMP Server, on page 261 | |
| | Create Golden Template for Unified CVP Reporting Server, on page 262 | |
| | Create Golden Template for Cisco Finesse, on page 264 | |
| | Create Golden Template for Cisco Unified Intelligence Center , on page 272 | |
| | Create Golden Template for Cisco Unified Communications Manager, on page 266 | |
| 5 | **Configure Customer Instance for Network Infrastructure** | |
| | Implement UCS Platform, on page 281 | |
| | ESX Boot from SAN, on page 288 | |
| | Deploy Nexus 1000v, on page 291 | |
| | Establish Two-Way Forest Trust, on page 456 | |
| 6 | **Clone and OS Customization** | |
| | Download Golden Template Automation Tool, on page 300 | |
| | Complete Automation Spreadsheet, on page 301 | |
| | Run Automation Script, on page 303 | |
| 7 | **Configure Customer Instance** | |
| | Configure Cisco Unified CCE Rogger, on page 404 | |

| Sequence | Task | Done |
|---|---|---|
| | Configure Unified CCE AW-HDS-DDS, on page 409 | |
| | Configure Unified CCE Agent PG 1, on page 412 | |
| | Configure Unified CCE Agent PG 2, on page 418 | |
| | Configure Unified CCE VRU PG, on page 420 | |
| | Configure Unified CVP, on page 347 | |
| | Configure Cisco IOS Enterprise Voice Gateway, on page 369 | |
| | Configure Unified Intelligence Center , on page 423 | |
| | Configure Unified Communications Manager, on page 375 | |
| | Configure Cisco Finesse, on page 392 | |
| 8 | **Administration** | |
| | Provision Unified CCE Using Unified CCDM, on page 501 | |
| | Provision Unified Communications Manager Using UCDM, on page 566 | |

# Checklists for Small Contact Center Agent Deployment

| Sequence | Task | Done |
|---|---|---|
| 1 | **Prerequisites** | |
| | Hardware Requirements, on page 47 | |
| | Software Requirement, on page 49 | |
| | Required Software Licenses, on page 52 (SCC Deployment Model) | |
| | Open Virtualization Format Files, on page 54 | |
| 2 | **Design Consideration** | |
| | Storage, VM Specifications, and IOPS Considerations, on page 168 | |
| 3 | **Shared Management and Aggregation** | |
| | Deploy Unified CCDM Database Server, on page 196 and Deploy Unified CCDM Web Server, on page 205 | |
| | Install and Configure Unified Communication Domain Manager, on page 221 | |
| | Configure Multiple Context Modes, on page 229 | |
| | Configure Perimeta SBC, on page 238 | |

| Sequence | Task | Done |
|---|---|---|
| 4 | **Create Golden Template** | |
| | Create Golden Template for Unified CCE Rogger, on page 268 | |
| | Create Golden Template for Unified CCE AW-HDS-DDS, on page 269 | |
| | Create Golden Template for Unified CCE Agent Peripheral Gateway, on page 270 | |
| | Create Golden Template for Unified CCE VRU Peripheral Gateway, on page 271 | |
| | Create Golden Template for Unified CVP Server, on page 259 | |
| | Create Golden Template for Unified CVP OAMP Server, on page 261 | |
| | Create Golden Template for Unified CVP Reporting Server, on page 262 | |
| | Create Golden Template for Cisco Finesse, on page 264 | |
| | Create Golden Template for Cisco Unified Intelligence Center , on page 272 | |
| | Create Golden Template for Cisco Unified Communications Manager, on page 266 | |
| 5 | **Configure Customer Instance for Network Infrastructure** | |
| | ESX Boot from SAN, on page 288 | |
| | Deploy Nexus 1000v, on page 291 | |
| | Create a Domain Controller Server, on page 321 | |
| | Establish Two-Way Forest Trust, on page 456 | |
| 6 | **Clone and OS Customization** | |
| | Download Golden Template Automation Tool, on page 300 | |
| | Complete Automation Spreadsheet, on page 301 | |
| | Run Automation Script, on page 303 | |
| 7 | **Create Customer Instance for Small Contact Center Agent Deployment** | |
| | Shared Core Components | |
| | Configure Unified CCE Rogger for Small Contact Center Agent Deployment , on page 425 | |
| | Configure Unified CCE AW-HDS-DDS, on page 409 | |
| | Configure Unified CCE VRU PG, on page 420 | |
| | Configure Unified CVP, on page 347 | |
| | Configure Cisco IOS Enterprise Voice Gateway, on page 369 | |
| | Configure Unified Intelligence Center , on page 423 | |
| | Sub Customer Components | |

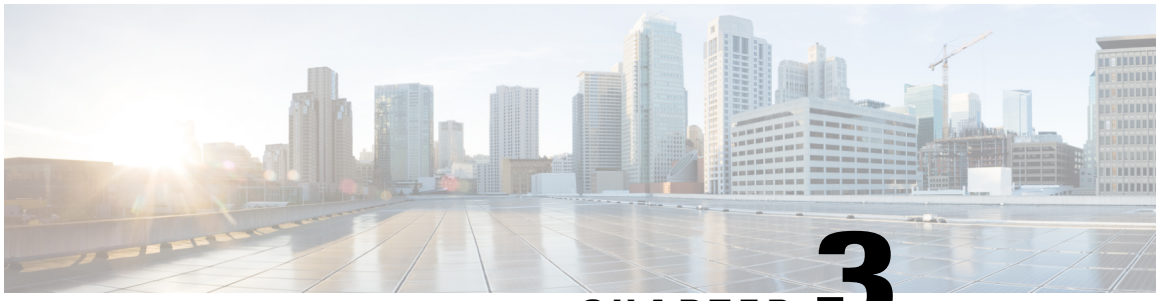
| Sequence | Task | Done |
|---|---|---|
| | Configure Unified CCE Agent PG for Small Contact Center Agent Deployment, on page 428 | |
| | Configure Unified Communications Manager, on page 375 | |
| | Configure Cisco Finesse, on page 392 | |
| 8 | **Administration** | |
| | Provision Unified CCE Using Unified CCDM, on page 501 | |
| | Provision Unified Communications Manager Using UCDM, on page 566 | |

# Checklist for 12000 Agent Deployment

| Sequence | Task | Done |
|---|---|---|
| 1 | **Prerequisites** | |
| | Hardware Requirements, on page 47 | |
| | Software Requirement, on page 49 | |
| | Required Software Licenses, on page 52 | |
| 2 | **Design Consideration** | |
| | Storage, VM Specifications, and IOPS Considerations, on page 168 | |
| | Operating Considerations, on page 70 | |
| | Core Component Integrated Options Considerations, on page 126 | |
| | 12000 Agent Deployment Model Considerations, on page 162 | |
| 3 | **Shared Management and Aggregation** | |
| | Install and Configure Unified CCDM, on page 195 | |
| | Install and Configure Unified Communication Domain Manager, on page 221 | |
| | Install and Configure ASA Firewall and NAT, on page 227 | |
| 4 | **Create Golden Template** | |
| | Create Golden Template for Unified CCE Router, on page 275 | |
| | Create Golden Template for Unified CCE Logger, on page 276 | |
| | Create Golden template for Unified CCE AW-HDS, on page 277 | |
| | Create Golden Template for Unified CCE HDS-DDS, on page 278 | |

| Sequence | Task | Done |
|---|---|---|
| | Create Golden Template for Unified CCE Agent Peripheral Gateway, on page 270 | |
| | Create Golden Template for Unified CCE VRU Peripheral Gateway, on page 271 | |
| | Create Golden Template for Unified CVP Server, on page 259 | |
| | Create Golden Template for Unified CVP OAMP Server, on page 261 | |
| | Create Golden Template for Unified CVP Reporting Server, on page 262 | |
| | Create Golden Template for Cisco Finesse, on page 264 | |
| | Create Golden Template for Cisco Unified Intelligence Center , on page 272 | |
| | Create Golden Template for Cisco Unified Communications Manager, on page 266 | |
| 5 | **Configure Customer Instance for Network Infrastructure** | |
| | Implement UCS Platform, on page 281 | |
| | ESX Boot from SAN, on page 288 | |
| | Deploy Nexus 1000v, on page 291 | |
| | Establish Two-Way Forest Trust, on page 456 | |
| 6 | **Clone and OS Customization** | |
| | Download Golden Template Automation Tool, on page 300 | |
| | Complete Automation Spreadsheet, on page 301 | |
| | Run Automation Script, on page 303 | |
| 7 | **Configure Customer Instance** | |
| | Configure Unified CCE Logger , on page 439 | |
| | Configure Unified CCE Router, on page 441 | |
| | Configure Unified CCE AW-HDS, on page 441 | |
| | Configure Unified CCE HDS-DDS, on page 443 | |
| | Configure Unified CCE Agent PG's for 12000 Agent Deployment, on page 445 | |
| | Configure Unified CCE VRU PG's for 12000 Agent Deployment, on page 447 | |
| | Configure Unified CVP, on page 347 | |
| | Configure Cisco IOS Enterprise Voice Gateway, on page 369 | |
| | Configure Unified Communications Manager, on page 375 | |
| | Configure Unified Intelligence Center , on page 423 | |

| Sequence | Task | Done |
|---|---|---|
| | Configure Cisco Finesse, on page 392 | |
| 8 | **Integration with Shared Management and Aggregation** | |
| | Unified CCDM Configuration, on page 209 | |
| | Cisco UCDM Integration, on page 473 | |
| 9 | **Administration** | |
| | Unified CCE Administration, on page 501 | |
| | Unified CVP Administration, on page 565 | |
| | Unified Communication Manager Administration, on page 566 | |



CHAPTER 3

# Design Consideration



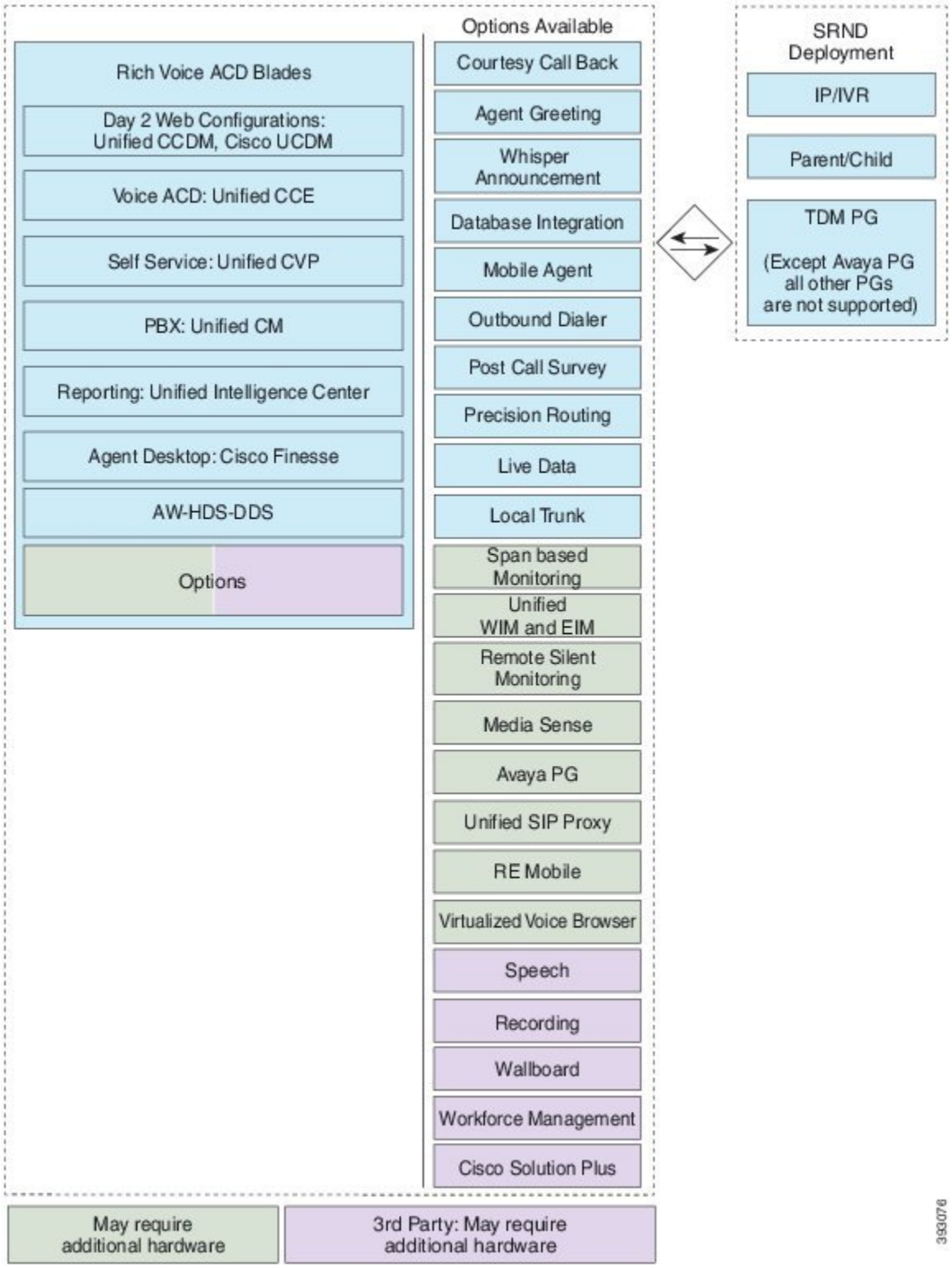
## Deployment Considerations

Cisco HCS for Contact Center supports a subset of the deployment options described in the Unified Contact Center Enterprise Solution Reference Network Design (SRND).

Following figure illustrates the deployment options available to Cisco HCS for Contact Center and shows the options that are supported:

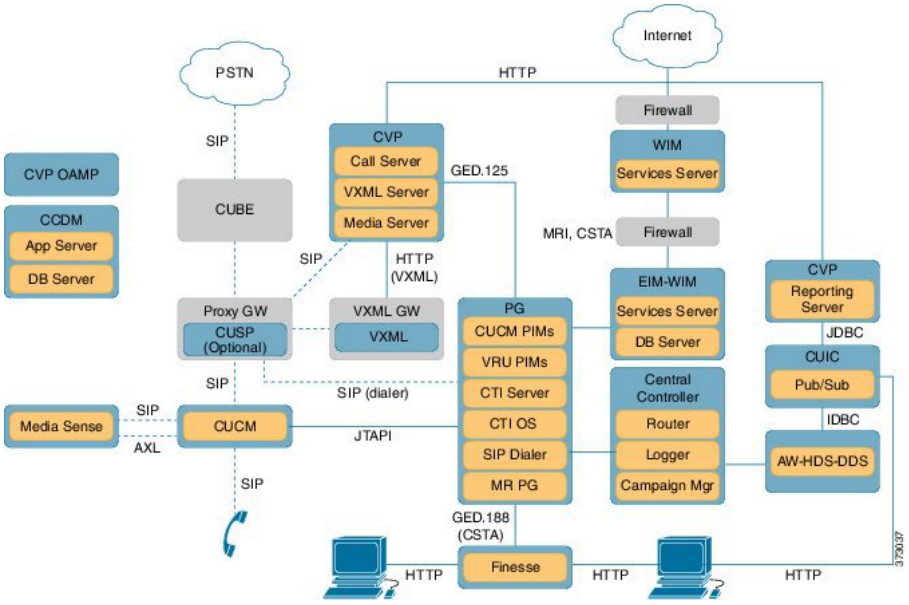
**Note** This is not an exhaustive list. As a rule, if an option or feature is not mentioned in this document, it is not supported in this deployment.

***Figure 15: Cisco HCS for Contact Center and Solution Reference Network Design***


Rich Voice ACD Blades
Day 2 Web Configurations: Unified CCDM, Cisco UCDM
Voice ACD: Unified CCE
Self Service: Unified CVP
PBX: Unified CM
Reporting: Unified Intelligence Center
Agent Desktop: Cisco Finesse
AW-HDS-DDS
Options
Options Available
Courtesy Call Back
Agent Greeting
Whisper Announcement
Database Integration
Mobile Agent
Outbound Dialer
Post Call Survey
Precision Routing
Live Data
Local Trunk
Span based Monitoring
Unified WIM and EIM
Remote Silent Monitoring
Media Sense
Avaya PG
Unified SIP Proxy
RE Mobile
Virtualized Voice Browser
Speech
Recording
Wallboard
Workforce Management
Cisco Solution Plus
SRND Deployment
IP/IVR
Parent/Child
TDM PG
(Except Avaya PG all other PGs are not supported)
May require additional hardware
3rd Party: May require additional hardware
393076

The following figure shows the logical view of Cisco Hosted Collaboration Solution for Contact Center:

***Figure 16: Cisco HCS for Contact Center Logical View***




# Operating Considerations

This section describes the features, configuration limits, and call flows for the Cisco HCS for Contact Center core and optional components.



# Peripheral Gateways

The following table describes the deployment of the Peripheral Gateways.

*Table 7: Peripheral Gateway considerations*

| Number Of Peripheral Gateways | Number of PGs and PIMs | Notes |
|---|---|---|
| **500 and 1000 Agent Model:** Two Peripheral Gateways are supported in this deployment . | One generic PG with the following PIMs:<br>• One CUCM PIM<br>• Four VRU PIMs<br>One Media Routing (MR) PG with the following PIMs:<br>• One Media Routing PIM for Multichannel<br>• One Media Routing PIM for Outbound | • **Unified CCE Call Server** contains the following:<br>◦ One Generic PG<br>◦ One Media Routing PG<br>• Two of the four VRU PIMs connect to the two Unified CVPs on Side A. Other two VRU PIMs connect to the two Unified CVPs on Side B. |
| **4000 Agent Model:** Five Peripheral Gateways are supported in this deployment. | Two CUCM PGs<br>• One CUCM PIM in each PG<br>One VRU PG<br>• Sixteen VRU PIMs ( eight are optional)<br>Two Media Routing (MR) PGs<br>• One Media Routing PIM for Multichannel<br>• Two Media Routing PIM for Outbound one in each MR PG | • There are 3 PG boxes in each side of core blades and contains the following<br>◦ **Unified CCE Agent PG1** contains one CUCM PG, one MR PG with two PIMs, and one Dialer.<br>◦ **Unified CCE Agent PG2** contains one CUCM PG, one MR PG with one PIM, and one Dialer.<br>◦ **Unified CCE VRU PG1** contains sixteen PIMs across both the sides. Eight connects to eight unified CVPs on side A. Other eight connects to eight unified CVPs on side B.<br>**Note** If Avaya PG is used, Outbound is not supported. |

| Number Of Peripheral Gateways | Number of PGs and PIMs | Notes |
|---|---|---|
| **12000 Agent Model:** 15 Peripheral Gateways are supported in this deployment . | Six CUCM PGs<br>• One CUCM PIM in each PG<br>Three VRU PGs<br>• 16 VRU PIMs in each PG<br>Six Media Routing (MR) PGs<br>• One Multichannel PIM for each PG<br>• One Media Routing PIM for Outbound in each PG | There are nine PG boxes in each side of core blades and contain the following:<br>• **Six Unified CCE Agent PGs** contains one CUCM PG, one MR PG with two PIMs, and one Dialer<br>• **Three Unified CCE VRU PGs** contains 16 PIMs across both the sides. Eight connects to eight unified CVPs on side A. Other eight connects to eight unified CVPs on side B.<br>**Note** If Avaya PG is used, Outbound is not supported. |
| **Small Contact Center Model:** 150 Peripheral Gateways are supported in this deployment. | Upto 149 CUCM PGs<br>• One CUCM PIM in each PG .<br>One VRU PG<br>• 16 VRU PIMs (eight are optional).<br>Upto 74 Media Routing (MR) PGs<br>• One Media Routing PIM for Multichannel in each PG.<br>• Two Media Routing PIMs for Outbound in each PG.<br>**Note** Combination of CUCM PGs and MR PGs are restricted to 149. | There are two PGs in each side of the sub customer and contains the following :<br>• **Unified CCE Agent PG** contains one CUCM PG, one MR PG with two PIMs, and one Dialer.<br>There is one PG in each side of the core blade which is shared across all Sub customers.<br>• **Unified CCE VRU PG** contains 16 PIMs across both the sides.<br>Eight of the 16 VRU PIMs connects to eight unified CVPs on side A. Other eight connects to eight unified CVPs on side B. |

**Note** CUCM PIMs are limited to 12, if PQs are used in this deployment.

# Agent and Supervisor Capabilities

Following table lists the agent and Supervisor capabilities:

*Table 8: Agent and Supervisor Capabilities*

| | HCS for Contact Center Deployment | Notes |
|---|---|---|
| Call Flows | All transfers, conferences, and direct agent calls use ICM script. | — |
| Agent Greeting | Supported | — |
| Whisper Announcement | Supported | — |
| Outbound Dialer | Supported | Only SIP dialer is supported. |
| Mobile Agent | Both nailed-up and Call-by-Call modes are supported. | — |
| Silent Monitoring | • Unified CM-based (BiB)<br>• SPAN for Mobile Agent | You can configure either Unified CM-based or SPAN-based but not both. If you configure Unified CM-based silent monitoring, you cannot monitor mobile agents.<br>A separate server is required for SPAN-based silent monitoring. |
| Recording | Following are the supported recording types:<br>• Unified CM based<br>• CUBE(E) based<br>• TDM gateway based | — |

| | HCS for Contact Center Deployment | Notes |
|---|---|---|
| CRM Integration | CRM integration is allowed with custom CTI OS Toolkit or Cisco Finesse API.<br>• Cisco Finesse gadgets<br>• Cisco Finesse web API or CTI OS APIs<br>• Existing CRM connectors | You can integrate with CRM in many ways. You can use:<br>• Cisco Finesse gadgets to build a custom CRM-integrated desktop. For example, this can be a Cisco Finesse gadget that fits in a CRM browser-based desktop.<br>• Cisco Finesse web API or CTI OS APIs or the CTI Server protocol to integrate into a CRM application<br>• Existing CRM connectors. The connectors available from Cisco for SAP. Each of these connectors has its own capacity limits:<br>◦ SAP can support up to 250 agents and Supervisors. Max 3 CPS. Requires its own server. Supports Unified CM BIB-based Recording or Silent Monitoring. Does not support Mobile Agents, Outbound, or Multichannel. |
| Desktop | Cisco Finesse | Supports Outbound feature (Progressive and Predictive only), Mobile Agent, SPAN-based silent monitoring, and Unified CM-based silent monitoring. |
| | Cisco Computer Telephony Integration Option (CTI OS) Desktop:<br>• .NET<br>• Java CIL<br>• Win32 | Supports Agent Greeting, Whisper Announcement, Outbound, Mobile Agent, SPAN-based silent monitoring, and Unified CM-based silent monitoring. |
| | Cisco Finesse IP Phone Support | FIPPA supports fewer features of Cisco Finesse. For more information, see Cisco Finesse Documentation. |
| Desktop Customization | Cisco Finesse API<br>CTI OS Toolkit Desktops | CTI OS Toolkit Desktops are listed above, under Desktop. |

# Voice Infrastructure

The following table lists the voice infrastructure.

***Table 9: Voice Infrastructure***

| Voice Infrastructure | HCS for Contact Center Deployment | Notes |
|---|---|---|
| Music on Hold | Unicast<br>Multicast<br>Unified CM Subscriber source only | This sizing applies to agent node only, for both agent and back-office devices, with all agent devices on the same node pair. |
| Proxy | SIP Proxy is optionally supported. | High Availability (HA) and load balancing are achieved using these solution components:<br>• Time Division Multiplexing (TDM) gateway and Unified CM, which use the SIP Options heartbeat mechanism to perform HA.<br>• Unified CVP servers, which use the SIP server group and SIP Options heartbeat mechanism to perform HA and load balancing. |
| Ingress Gateways | ISR G2 Cisco Unified Border Element with combination VXML | 3925E and 3945E are the supported GWs.<br>For SPAN based Silent Monitoring, the Ingress gateway is spanned.<br>You must configure the gateway MTPs to do a codec pass-through because the Mobile Agent in HCS is configured to use G729 and the rest of the components in HCS support all the codecs. See CVP SRND for list of supported gateway models and corresponding sizing. |

| Voice Infrastructure | HCS for Contact Center Deployment | Notes |
|---|---|---|
| Protocol | Session Initiation Protocol (SIP) over TCP | SIP over UDP, H323, Media Gateway Control Protocol (MGCP) are not supported. |
| Proxy /Cisco Unified SIP Proxy (CUSP) | SIP Proxy is optionally supported. | Outbound Option: The Outbound dialer can connect to only one physical gateway, if SIP proxy is not used. See Configuration Limits, on page 82 |
| Codec | • IVR: G.711ulaw and G.711alaw<br>• Agents: G.711ulaw, G.711 alaw, and G729r8 | G.722, iSAC, and iLBC are not supported. |
| Media Resources | Gateway-based:<br>• Conference bridges<br>• Transcoders and Universal Transcoders<br>• Hardware and IOS Software Media Termination Points. | Unified CM-based (Cisco IP Voice Media Streaming Application) that are not supported:<br>• Conference bridges<br>• MTPs |

# Administration Guidelines

The following table lists the administration tools.

*Table 10: Administration*

| | HCS for Contact Center Deployment | Notes |
|---|---|---|
| | **Supported:** | **Not supported:** |
| Provisioning | • Unified CCE Configuration tools. For more information, see Provision Unified CCE Using Administration Workstation, on page 564.<br>• Unified CCE Web Administration. For more information, see Provision Unified CCE Using Web Administration, on page 564.<br>• Unified CCDM Web Administration. For more information, see Provision Unified CCE Using Unified CCDM, on page 501.<br>• Unified CCE Internet Script Editor. For more information, see Provision Routing Script Using Internet Script Editor, on page 565<br>• Unified CVP Operations Console. For more information, see Configure Cisco Unified CVP Operations Console, on page 359.<br>• Unified Intelligence Center Web Administration. For more information, see Configure Unified Intelligence Center , on page 423.<br>• Cisco Unified CM Administration. For more information, see Provision Unified Communications Manager Using UCDM, on page 566<br>• Cisco Finesse Web Administration. For more information, see Configure Cisco Finesse Administration, on page 398.<br>• Agent Reskilling | Cisco Agent Desktop Admin |
| Service Creation Environment | • Unified CCE Script Editor<br>• CVP Call Studio | — |

| | HCS for Contact Center Deployment | Notes |
|---|---|---|
| | **Supported:** | **Not supported:** |
| Serviceability | • Cisco Prime Collaboration - Assurance<br>• Unified System Command Line Interface (CLI)<br>• RTMT Analysis Manager Diagnosis | RTMT Analysis Manager Analyze Call Path |

# IVR and Queuing

The following table describes the IVR and call queuing to help optimize inbound call management.

***Table 11: IVR and Queuing***

| | HCS for Contact Center Deployment | Notes |
|---|---|---|
| | **Supported:** | **Not supported:** |
| Voice Response Unit (VRU) | • Unified CVP Comprehensive Model Type 10 | • Unified CVP VRU types other than Type 10<br>• Cisco IP IVR<br>• Third-party IVRs |
| Caller Input | • DTMF<br>• Automatic Speech Recognition and Text-to-speech (ASR/TTS) | — |
| Dual Tone Multi-Frequency (DTMF) | • RFC2833 | • Keypad Markup Language (KPML) |
| Video | None | — |
| CVP Media Server | • Third-party Microsoft Internet Information Services (IIS), co-resident on the Unified CVP Server | • Tomcat |

# Reporting

The following table contains information on the reporting.

***Table 12: Reporting***

| | HCS for Contact Center Deployment | Notes |
|---|---|---|
| Tool | Cisco Unified Intelligence Center is the only supported reporting application.<br>**Note** Unified Intelligence Center historical reporting data and Call Detail data are pulled from the Logger database for 500/1000 agent deployment model and the data pulled from the AW-HDS-DDS server for other deployments. | Not supported with reporting from Logger:<br>• Exony VIM<br>• Third-party reporting applications<br>Supported with reporting from AW-HDS-DDS:<br>• Exony VIM<br>• Third-party reporting applications<br>• Custom reporting |
| Database | Historical and Call Detailed data is stored on the Unified CCE Data Server for 500 and 1000 Agent Deployment and stored on Unified AW-HDS-DDS server for other deployments. | — |
| Retention | The logger database retention period is 400 days (13 months) of historical summary data and 35 days (five weeks) of detailed TCD and RCD records.<br>If you require longer retention periods, add a single Historical Data Server (HDS) to the deployment. See the following table for the HDS minimum requirements.<br>**Note** This is applicable only for 500 and 1000 agents deployment model and the Retention values are default for other deployments. | Data beyond the configured retention time is purged automatically at 12:30 AM and uses the time zone setting of the core server.<br>Follow Cisco supported guidelines to run the purge at off-peak hours or during a maintenance window.<br>Note that you can control or change the automatic purge schedule through the command line interface. You can change it if the automated purge does not occur during your off-peak hours.<br>The purge has a performance impact on the Logger.<br>Customers who install the External AW-HDS-DDS on separate servers can point Cisco Unified Intelligence Center to either the logger or the External AW-HDS-DDS, but not to both. |

| | HCS for Contact Center Deployment | Notes |
|---|---|---|
| Reports | Each supervisor can run four concurrent Real-Time reports and two historical reports:<br>• Real-Time reports contain 100 rows.<br>• Historical reports contain 2000 rows. | — |

*Table 13: HDS Minimum Requirements for 500 and 1000 agent deployment model.*

| Virtual Machine | vCPU | RAM (GB) | Disk (GB) | CPU Reservation (MHz) | RAM Reservation (MB) |
|---|---|---|---|---|---|
| Unified CCE HDS | 1 | 2 | 80 (OS) 512* (Database) | — | 2048 |

* The DB vDisk can be custom sized at OVA deployment based on solution sizing and customer retention requirements using the DB Estimator Tool. For more information about the HDS sizing, see Virtualization of Unified CCE .

# Third-Party Integration

The following table contains third-party integration information.

*Table 14: Third-Party Integration*

| Option | Notes |
|---|---|
| Recording | All Recording applications that are supported by Unified CCE are supported on HCS for CC. For details, see Recording section in Agent and Supervisor Capabilities, on page 72. |
| Wallboards | All Wallboard applications that are supported by Unified CCE are supported on HCS for CC.<br>**Note** Unified Intelligence Center can also be used for Wallboards. |
| Workforce Management | If you need access to real-time or historical data, then you will require AW-HDS-DDS. All Workforce Management applications that are supported by Unified CCE are supported on HCS for CC. |
| Database Integration | Unified CVP VXML Server is supported.<br>ICM DB Lookup is supported. |

| Option | Notes |
| --- | --- |
| Automated Call Distributor (ACD) | None |
| Interactive Voice Response (IVR) | • Unified IP IVR is not supported.<br>• No third-party IVRs are supported. |

# Configuration Limits

*Table 15: Agents, Supervisors, Teams, Reporting Users*

| Group | Resource | 500 Agent Deployment | 1000 Agent Deployment | 4000 Agent Deployment | 12000 Agent Deployment | Small Contact Center Deployment |
|---|---|---|---|---|---|---|
| **Agents** | Active Agents* | 500 | 1000 | 4000 | 12000 | 4000 |
| | Configured Agents* | 3000 | 6000 | 24000 | 72000 | 24000 |
| | Agents with Trace ON | 50* | 100* | 400* | 400 | 400* |
| | Agent Desk Settings* | 500 | 1000 | 4000 | 12000 | 4000 |
| | Active Mobile Agents | 125 | 250 | See, Mobile Agent Support, on page 83 | See, Mobile Agent Support, on page 83 | See, Mobile Agent Support, on page 83 |
| | Configured Mobile Agents | 750 | 1500 | 6000 | 8000 | 6000 |
| | Outbound Agents | 500 | 1000 | 4000 | 12000 | 4000 |
| | Agents per team | 50* | 50* | 50* | 50 | 50* |
| | Queues per Agent (Skill Groups and Precision Queues combined) | 15* | 15* | 15* | 15 | 15* |
| | Agents per skill group | No limit | No limit | No limit | No limit | No limit |
| | Attributes per agent* | 50 | 50 | 50 | 50 | 50 |
| | Agents per Avaya PG | NA | NA | 2000 | 6000 | NA |

| Group | Resource | 500 Agent Deployment | 1000 Agent Deployment | 4000 Agent Deployment | 12000 Agent Deployment | Small Contact Center Deployment |
|---|---|---|---|---|---|---|
| **Supervisors** | Active Supervisors* | 50 | 100 | 400 | 1200 | 400 |
| | Configured Supervisors* | 300 | 600 | 2400 | 7200 | 2400 |
| | Active teams* | 50 | 100 | 400 | 1200 | 400 |
| | Configured teams* | 300 | 600 | 2400 | 7200 | 2400 |
| | Supervisors per Team | 10* | 10* | 10* | 10 | 10* |
| | Teams per supervisor | 20* | 20* | 20* | 20 | 20* |
| | Agents per supervisor | 20 | 20 | 20 | 20 | 20 |
| **Reporting** | Active Reporting users | 50 | 100 | 400 | 1200 | 400 |
| | Configured Reporting users | 300 | 600 | 2400 | 7200 | 2400 |
| **Access Control** | Administrator (Users) | 100 | 100 | 1000 | 1000 | 1000 |

### Mobile Agent Support

Follow the below calculation to determine mobile agent capacity:

- Each mobile agent for a nailed connection = two local agents
- Each mobile agent for call-by-call connection = four local agents

**Note**

- Total number of agents should be less than deployment limits
- For 500 and 1000 agent deployments if active mobile agent requirement exceeds the specified limit, use the above formula to determine mobile agent capacity

**Note**

1. Preview, Direct Preview, Progressive and Predictive dialing modes are supported.
2. For SIP Outbound Dialer in HCS for Contact Center deployment, if CUSP is not used only one gateway can be connected.

   If CUSP is not used in the deployment the maximum configured ports are 500 dialer ports in the ICM and in the IOS gateway . If CUSP is used in the deployment the maximum configured ports are 1500 dialer ports.
3. The Symbol "*" indicates that the configuration limits for the above resources are enforced through CCDM.
4. Number of active and configured mobile agents are considered from the total supported active and configured mobile agents.
5. Number of active and configured outbound agents are considered from the total supported active and configured outbound agents.

| Group | Resource | 500 Agent Deployment | 1000 Agent Deployment | 4000 Agent Deployment | 12000 Agent Deployment | Small Contact Center Deployment |
|---|---|---|---|---|---|---|
| **Outbound** | Dialer per system | 1 | 1 | 2 | 6 | 32 |
| | Number of Campaigns (Agent/IVR based) | 50 | 300 | 300 | 300 | 300 |
| | Campaign skill groups per campaign | 20 | 20 | 20 | 20 | 20 |
| | Queues per Agent (Skill Groups and Precision Queues combined) | 15 | 15 | 15 | 15 | 15 |
| | Total Numbers of Agents | 500 | 1000 | 4000 | 12000 | 4000 |
| | Port Throttle | 5 | 10 | 10 | 15 | 10 |

| Group | Resource | 500 Agent Deployment | 1000 Agent Deployment | 4000 Agent Deployment | 12000 Agent Deployment | Small Contact Center Deployment |
|---|---|---|---|---|---|---|
| **Precision Queues** | Precision Queues* | 4000 | 4000 | 4000 | 4000 | 4000 |
| | Precision Queue steps* | 10000 | 10000 | 10000 | 10000 | 10000 |
| | Precision Queue term per Precision Queue* | 10 | 10 | 10 | 10 | 10 |
| | Precision steps per Precision Queue* | 10 | 10 | 10 | 10 | 10 |
| | Unique attributes per Precision Queue* | 10 | 10 | 10 | 10 | 10 |

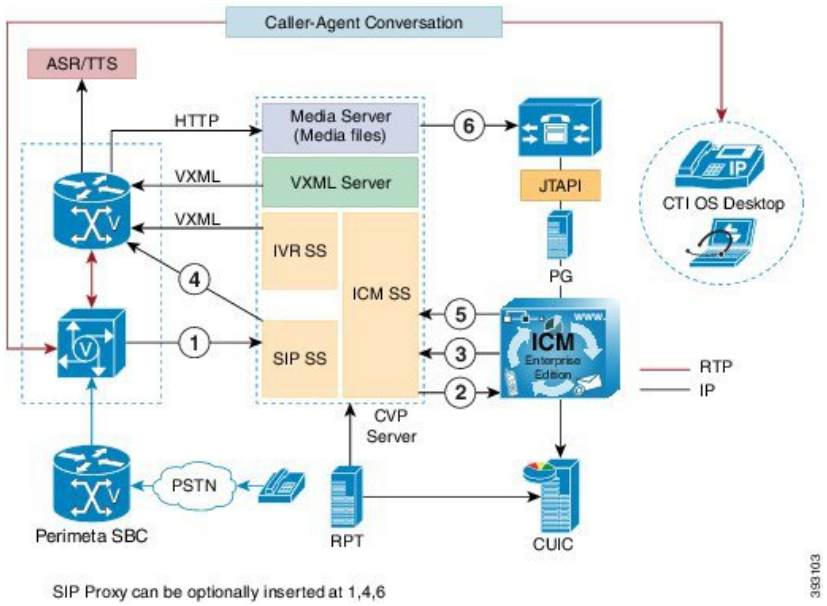
| Group | Resource | 500 Agent Deployment | 1000 Agent Deployment | 4000 Agent Deployment | 12000 Agent Deployment | Small Contact Center Deployment |
|---|---|---|---|---|---|---|
| **General** | Attributes* | 10000 | 10000 | 10000 | 10000 | 10000 |
| | Bucket Intervals | 500 | 1000 | 4000 | 12000 | 4000 |
| | Active Call Types | 1000 | 2000 | 8000 | 8000 | 8000 |
| | Configured Call Types* | 2000 | 2000 | 10000 | 10000 | 10000 |
| | Call Type Skill Group per Interval | 2000 | 2000 | 30000 | 30000 | 30000 |
| | Active Routing Scripts | 250 | 500 | 2000 | 6000 | 2000 |
| | Configured Routing Scripts | 500 | 1000 | 4000 | 12000 | 4000 |
| | Network VRU Scripts * | 500 | 1000 | 4000 | 12000 | 4000 |
| | Reason Codes | 100 | 100 | 100 | 100 | 100 |
| | Skill Groups* | 3000 | 3000 | 3000 | 3000 | 3000 |
| | Persistent Enabled Expanded Call Variables * | 20 | 20 | 5 | 5 | 5 |
| | Persistent Enabled Expanded Call Variable Arrays | 0 | 0 | 0 | 0 | 0 |
| | Nonpersistent Expanded Call Variables(Bytes)* | 2000 | 2000 | 2000 | 2000 | 2000 |
| | Bulk Jobs | 200 | 200 | 200 | 200 | 200 |
| | CTI All event Clients | 9/PG | 9/PG | 9/PG | 9/PG | 9/PG |
| | Services | NA | NA | 3000 | 3000 | NA |
| | Service Member | NA | NA | 350 | 350 | NA |

| Group | Resource | 500 Agent Deployment | 1000 Agent Deployment | 4000 Agent Deployment | 12000 Agent Deployment | Small Contact Center Deployment |
|---|---|---|---|---|---|---|
| **Dialed Number** | Dialed Number (External Voice) | 1000 | 1000 | 4000 | 12000 | 4000 |
| | Dialed Number (Internal Voice) | 1000 | 1000 | 4000 | 12000 | 4000 |
| | Dialed Number (Multichannel) | 500 | 500 | 2000 | 6000 | 2000 |
| | Dialed Number (Outbound Voice) | 500 | 500 | 2000 | 6000 | 2000 |
| **Load** | VRU Ports | 900 | 1800 | 7200 | 21600 | 7200 |
| | Calls per second | 5 | 8 | 35 | 115 | 35 |
| | Agent Load | 30 BHCA | 30 BHCA | 30 BHCA | 30 BHCA | 30 BHCA |
| **Reskilling** | Dynamic (operations/hr.) | 120 | 120 | 120 | 120 | 120 |

# Call Flows

The call flows in the following figures represent units of call flow functionality. You can combine these call flow units in any order in the course of a call.

***Figure 17: Basic Call Flow with IVR and Queue to an Agent***



1 New call from CUBE-E GW to CVP.

2 New call to UCCE from CVP.

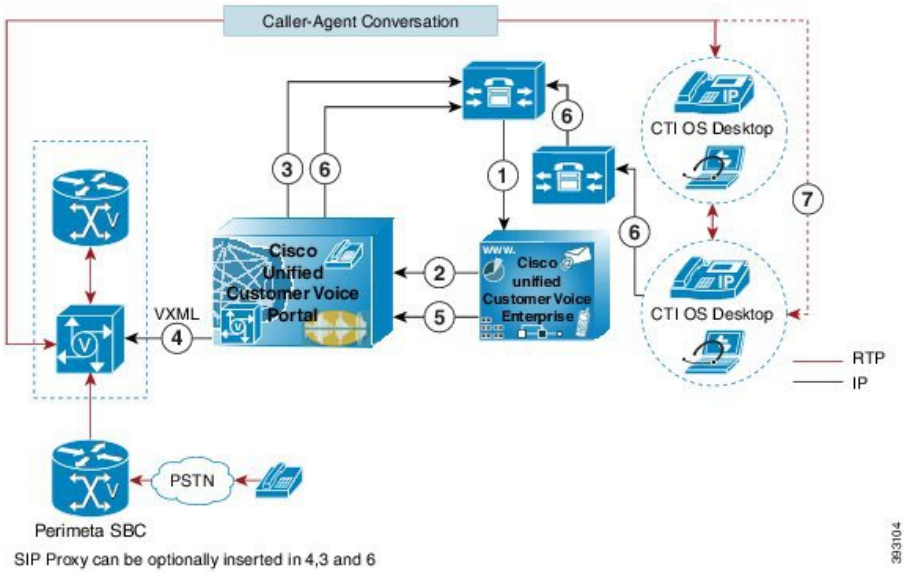
3 Play "Hello World" Prompt.

4 CVP sends call to VXML Gateway, caller hears IVR.

5 Agent is available now.

6 CVP sends call to an agent.

***Figure 18: Consult Call Flow with IVR and Queue to a Second Agent***




1 Agent initiates a consult requests, new call from Unified CM to Unified CCE.

2 Sends to VRU.

3 Unified CM sends call to Unified CVP.

4 Agent is inactive. Therefore, play 'IVR Music'. The agent hears IVR/Music

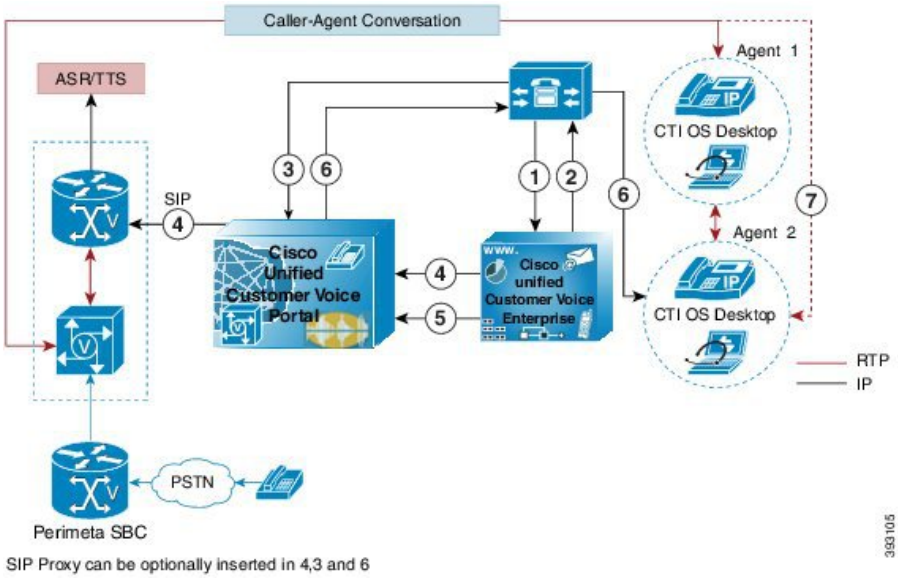
- Caller gets the Music on Hold (MOH).

5 Agent 2 is unavailable.

6 Unified CVP sends SIP calls to agent 2 on second CUCM cluster from cluster IVR is disconnected. Agent 1 consult with Agent 2.

7 Agent 1 completes the consult, caller talks to Agent 1.

*Figure 19: Blind Transfer Call Flow with IVR and Queue to a Second Agent*




1 Agent initiates a blind transfer request, new call form Unified CM to Unified CCE.

2 Agent is unavailable, send to VRU.

3 Unified CM sends call to Unified CVP.

4 Unified CVP sends call to VXML gateway, agent hears IVR/Music.

5 Agent 2 is inactive.

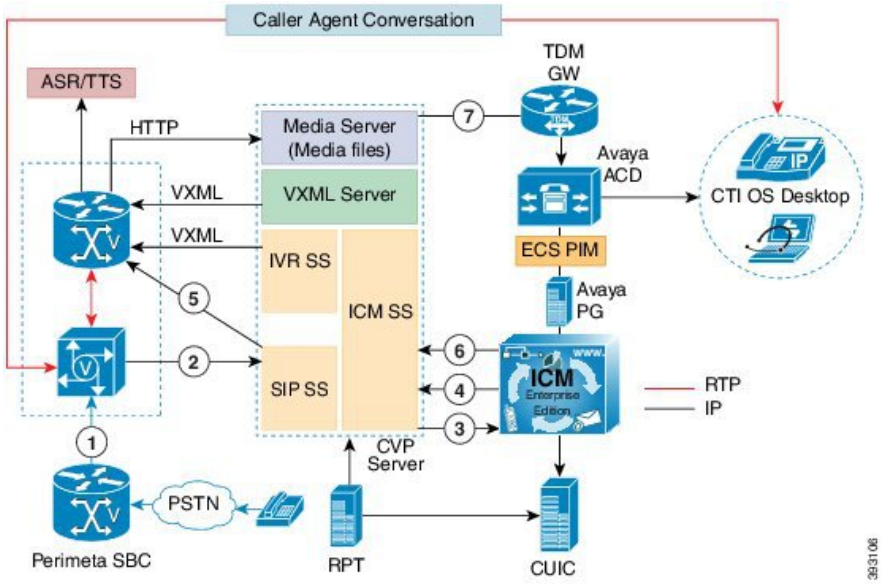
6 Unified CVP sends a SIP call to Agent 2.

- IVR is disconnected.

7 Agent 1 talks to Agent 2. Agent 1 completes the transfer.

- Agent 1 disconnects, caller talks to Agent 2.

*Figure 20: Basic Call Flow with IVR and Queue to Avaya Agent*




1 New call from Perimeta SBC to CUBE-E gateway.

2 New call to CVP from CUBE-E gateway.

3 New call to UCCE from CVP.

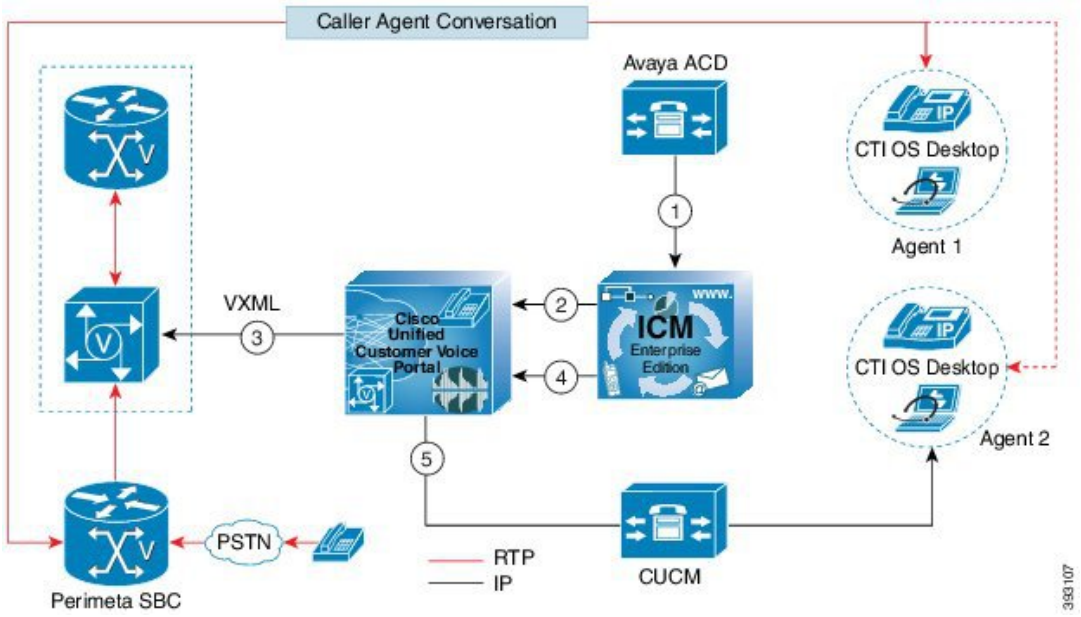
4 Play 'Hello World' prompt.

5 CVP sends call to VXML gateway, caller hears the IVR.

6 Agent becomes available.

7 CVP sends call to Avaya Agent through TDM gateway.

*Figure 21: Blind Transfer Call Flow with IVR and Queue to Avaya Agent*




1. Avaya agent initiates Blind transfer request, new call from Avaya ACD to Unified CCE.
2. CUCM Agent is inactive, UCCE send label to CVP.
3. CVP sends the call to VXML gateway, caller hears the IVR.
4. CUCM agent is active now.
5. CVP sends call to CUCM agent.

**Note** Conference call flows are the same as consult call flows. Both conference call flows and consult call flows conference the call with the agents, rather than holding them during consult. Hold/resume, alternate/reconnect, consult/conference call flows invoke the session initiation protocol (SIP) ReINVITE procedure to move the media streams. Conference to interactive voice response (IVR) call flow is similar to conference with no agent available call flow.

The following table shows the SIP trunk call flow.

*Table 16: SIP Trunk Call Flow*

| Call Flow | Logical Call Routing |
|---|---|
| New call from Perimeta SBC | Caller -->Perimeta SBC --> CUBE(E) --> Unified CVP -->Unified Communications Manager |
| New call from Unified Communications Manager (internal help desk) | Caller --> Unified Communications Manager --> CUBE(E) --> Unified CVP |

| Call Flow | Logical Call Routing |
|---|---|
| Post routed call from agent-to-agent | Agent 1 --> Unified Communications Manager --> Unified CVP --> Unified Communications Manager--> Agent 2 |
| Post routed call from agent to another agent on separate CUCM cluster. | Agent 1 --> Unified Communications Manager 1 --> Unified CVP --> Unified Communications Manager 1--> Unified Communications Manager2--> Agent 2 |

***Table 17: SIP Trunk Call Flow for Small Contact Center Agent Deployment***

| Call Flow | Logical Call Routing |
|---|---|
| New call from Perimeta SBC | Caller -->Perimeta SBC-->CUBE(E)--> Unified CVP-->Perimeta SBC-->Unified Communications Manager |
| New call from Unified Communications Manager (internal help desk) | Caller --> Unified Communications Manager --> Perimeta SBC-->CUBE(E)--> Unified CVP --> Perimeta SBC--> Unified Communications Manager |
| Post routed call from agent-to-agent | Agent 1 --> Unified Communications Manager -->Perimeta SBC --> Unified CVP --> Perimeta SBC --> Unified Communications Manager --> Agent 2 |

**Note** All new calls always enter the Cisco IOS gateway (CUBE-E or TDM-IP gateway) and are associated with the Unified CVP survivability service.

The following table shows the TDM gateway (Local PSTN breakout) call flow.

***Table 18: SIP Trunk Call Flow for Small Contact Center Agent Deployment with CUSP***

| Call Flow | Logical Call Routing |
|---|---|
| New Call from carrier at IVR | Caller -->Perimeta SBC-->CUBE(E)--> CUSP -> Unified CVP-->CUSP -> VXML GW |
| New Call from carrier at agent | Caller -->Perimeta SBC-->CUBE(E)--> CUSP -> Unified CVP--> CUSP -> Perimeta SBC-->Unified Communications Manager |
| New call from Unified Communications Manager (internal help desk) at IVR | Agent 1 --> Unified Communications Manager -->Perimeta SBC --> CUBE-E -> CUSP -> Unified CVP --> CUSP -> VXML GW |

| Call Flow | Logical Call Routing |
|---|---|
| New call from Unified Communications Manager (internal help desk) at agent | Agent 1 --> Unified Communications Manager -->Perimeta SBC --> CUBE-E -> CUSP -> Unified CVP --> CUSP -> Perimeta SBC --> Unified Communications Manager --> Agent 2 |
| Post Routed Call at IVR | Agent 1 --> Unified Communications Manager -->Perimeta SBC --> CUSP -> Unified CVP --> CUSP -> VXML GW |
| Post Routed Call at agent | Agent 1 --> Unified Communications Manager -->Perimeta SBC --> CUSP -> Unified CVP --> CUSP -> Perimeta SBC --> Unified Communications Manager --> Agent 2 |

*Table 19: TDM gateway (Local PSTN breakout) Call Flow*

| Call Flow | Logical Call Routing |
|---|---|
| New call from local PSTN gateway | Caller-->TDM-IP-->Unified CVP-->Unified Communications Manager |
| New call for IVR based | Caller --> TDM-IP -->Unified CVP -->CUBE(E) or VXML gateway |
| New call for agent based | Caller-->TDM-IP-->Unified CVP-->Unified Communications Manager-->Agent1 |

**Note**

- All new calls always enter the Cisco IOS gateway (CUBE-E or TDM-IP gateway) and are associated with the Unified CVP survivability service.
- To change the default settings, see TDM Gateway at Customer Premise, on page 165.

*Table 20: TDM gateway (Local PSTN breakout) Call Flow for Small Contact Center Agent Deployment*

| Call Flow | Logical Call Routing |
|---|---|
| New call from local PSTN gateway | Caller --> TDM-IP--> Perimeta SBC--> CUBE(E)--> Unified CVP-->Perimeta SBC --> Unified Communications Manager |
| New call for IVR based | Caller --> TDM-IP--> Perimeta SBC -->CUBE-E --> Unified CVP --> CUBE(E) or VXMLGW |

| Call Flow | Logical Call Routing |
|---|---|
| New call for agent based | Caller --> TDM-IP --> Perimeta SBC -->CUBE-E --> Unified CVP --> Perimeta SBC--> Unified Communications Manager |

The following table lists the supported system call flows.

**Note**

1 Configure TDM gateway at Perimeta SBC, see Add CUBE(E) Adjacency, on page 487

2 Configure TDM gateway at shared layer, similar to PSTN configuration.

***Table 21: Supported System Call Flows***

| System Call Flows | Supported |
|---|---|
| Conference to IVR | Yes |
| Bridged transfer | Yes |
| Router requery | Yes |
| Postroute using Unified CVP | Yes |
| Prerouting | No |
| Translation route with third-party VRU | No |
| ICM routing to devices other than Cisco HCS Unified CCE | No |

***Table 22: Avaya Call Flow***

| Call Flow | Logical Call Routing |
|---|---|
| New call from local PSTN gateway | Caller --> CUBE(E) --> Unified CVP --> TDM --> Avaya |
| Post Routed call from Avaya Agent – CUCM Agent | Avaya Agent --> Avaya --> Unified CVP --> Unified Communication Manager --> Agent |

# Core Solution Component Considerations

This section describes the High availability and Bandwidth, Latency & QoS considerations for Cisco HCS Contact Center core components:

# Core Component Design Considerations

The section describes the design considerations for Cisco for Contact Center core components:

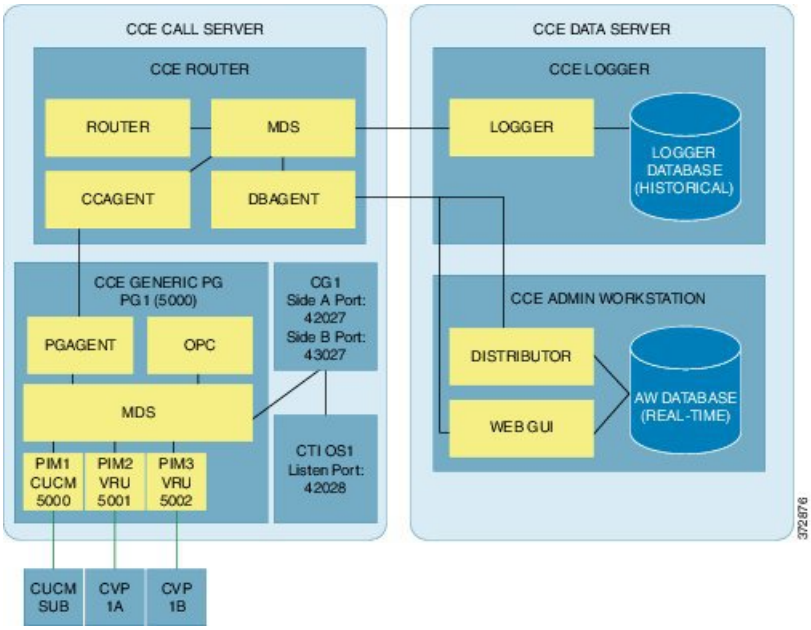


## Unified CCE Design Consideration

This section describes the Unified CCE design for each deployment:

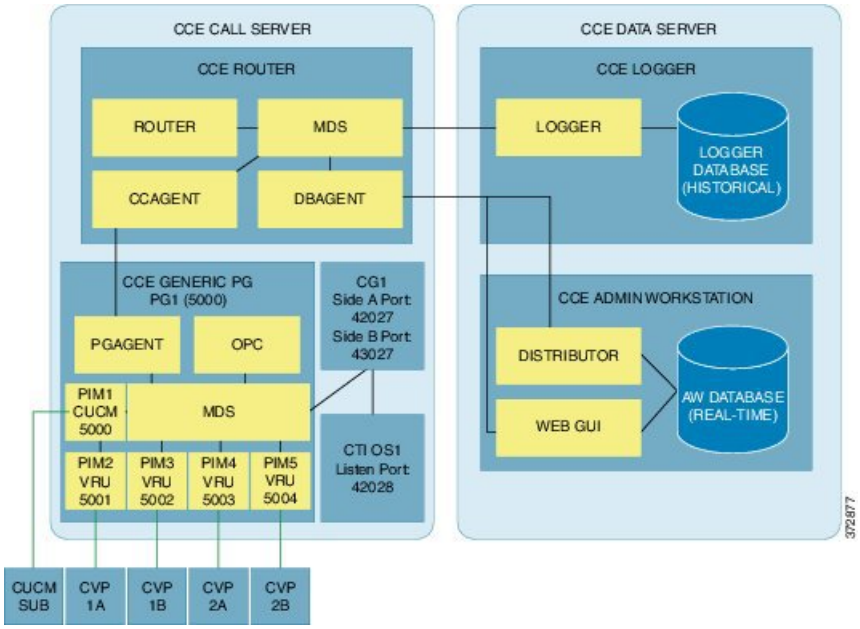
## Unified CCE Design for 500 Agent Deployment

*Figure 22: Unified CCE Design for 500 Agent Deployment*



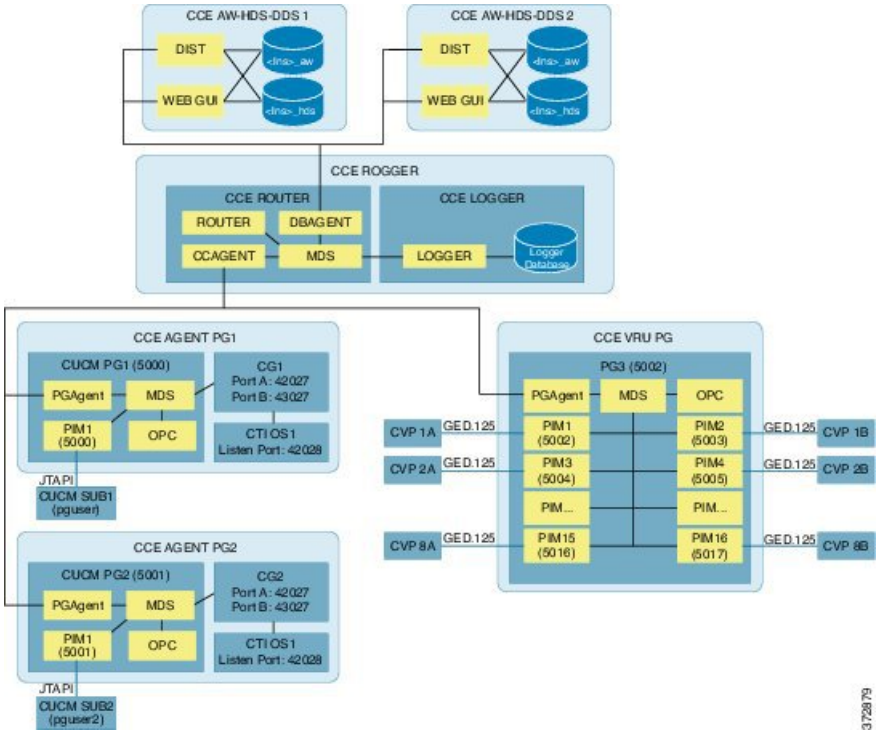

## Unified CCE Design for 1000 Agent Deployment

*Figure 23: Unified CCE Design for 1000 Agent Deployment*



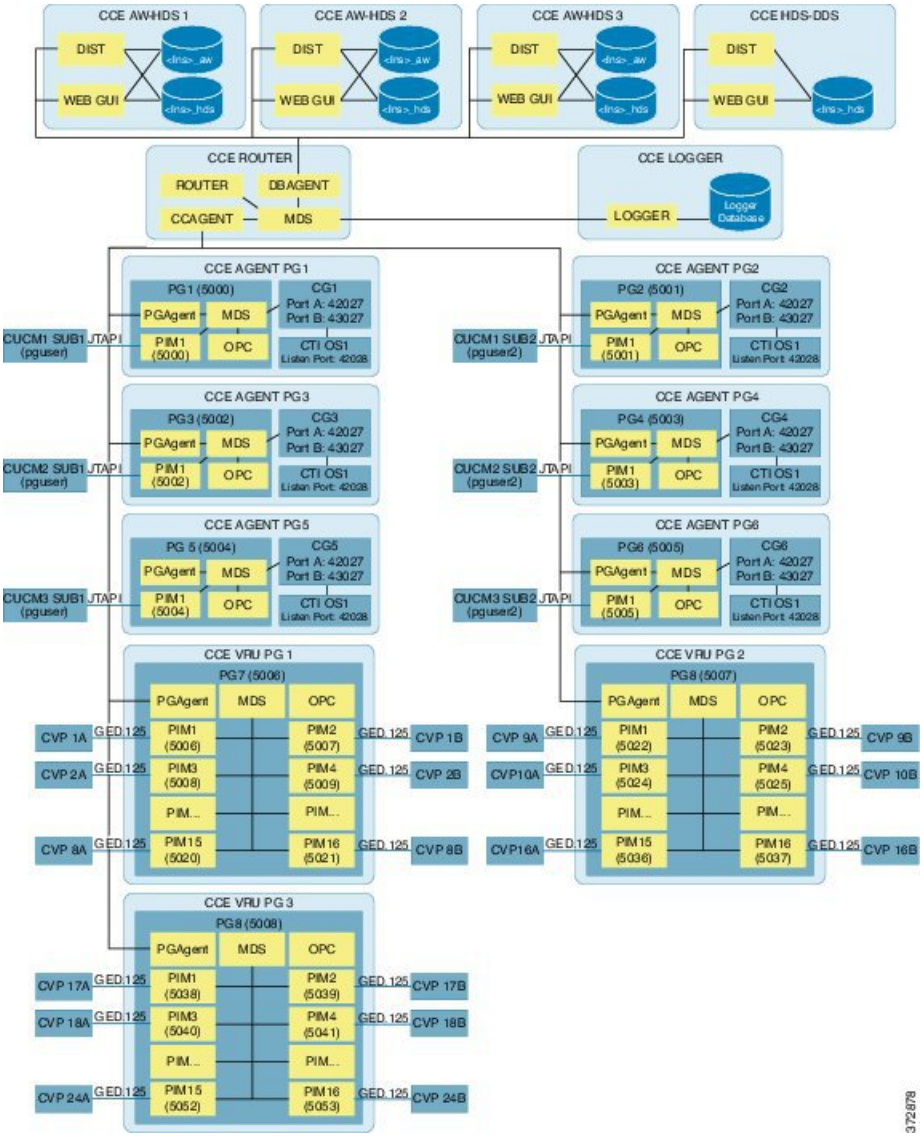
## Unified CCE Design for 4000 Agent Deployment

*Figure 24: Unified CCE Design for 4000 Agent Deployment*



### Unified CCE Design for 12000 Agent Deployment

*Figure 25: Unified CCE Design for 12000 Agent Deployment*



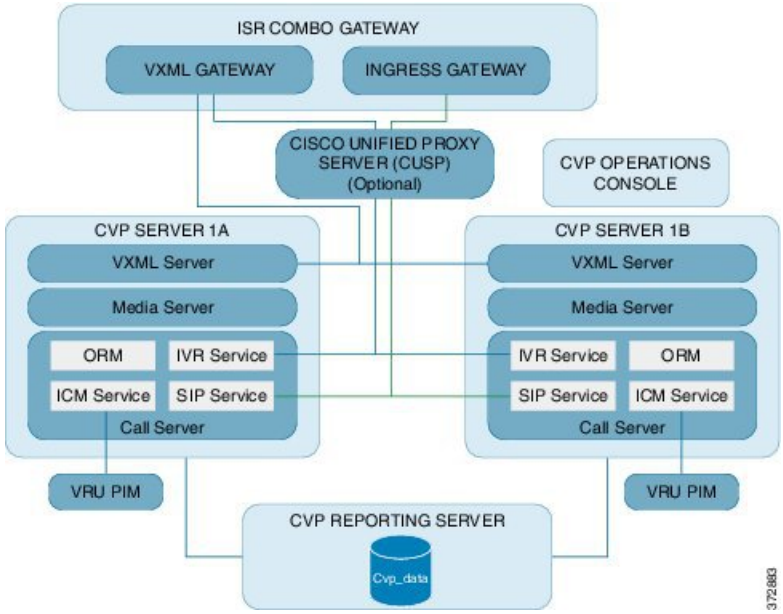

## Unified CVP Design Considerations

This section describes the CVP design for each deployment:

- Unified CVP Design for 500 Agent Deployment, on page 99
- Unified CVP Design for 1000 Agent Deployment, on page 99
- Unified CVP Design for 4000 Agent Deployment, on page 100
- Unified CVP Design for 12000 Agent Deployment, on page 101

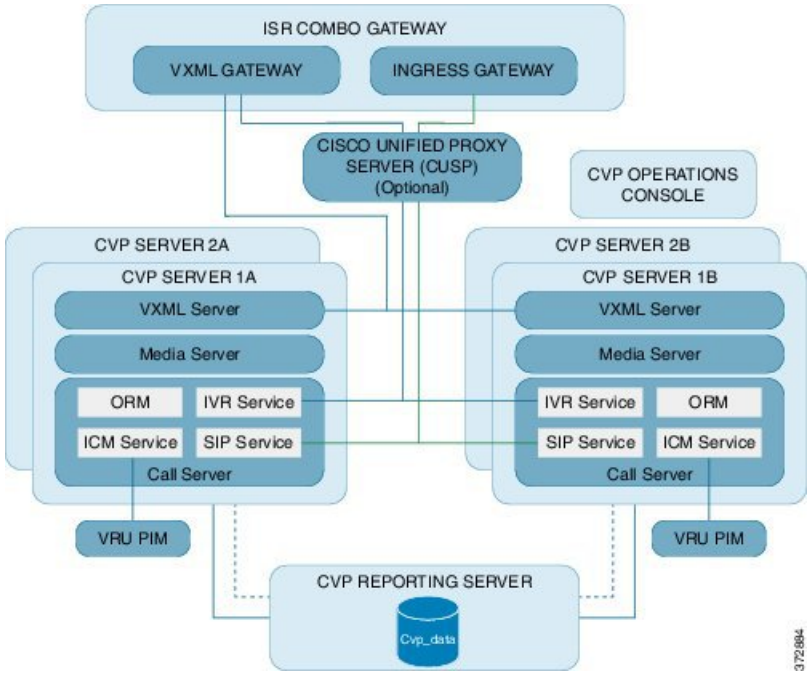
## Unified CVP Design for 500 Agent Deployment

*Figure 26: Unified CVP Design for 500 Agent Deployment*



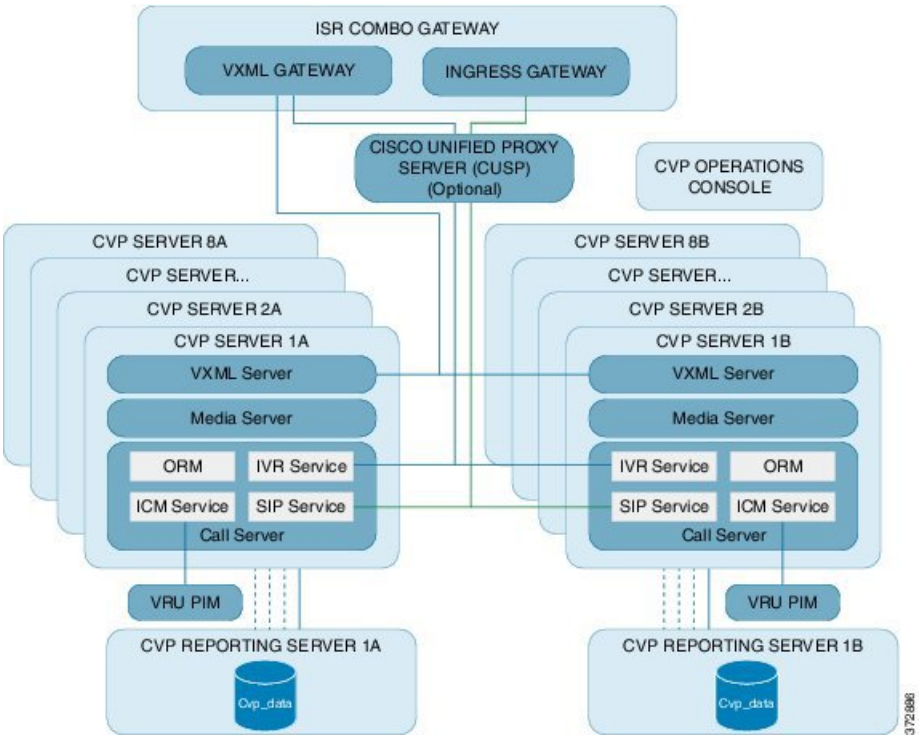

## Unified CVP Design for 1000 Agent Deployment

*Figure 27: Unified CVP Design for 1000 Agent Deployment*



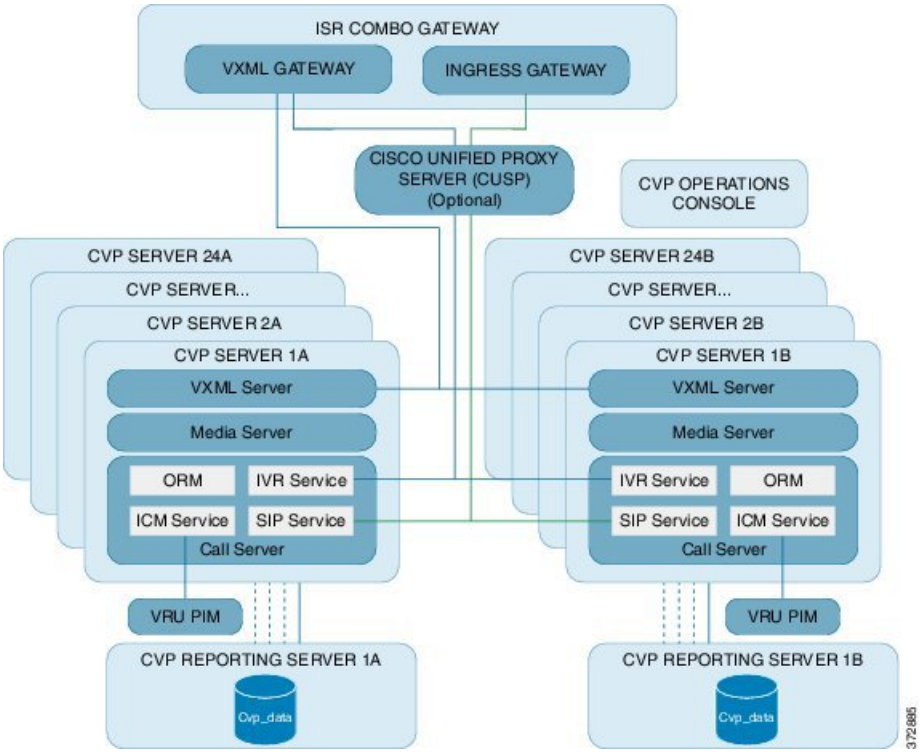
## Unified CVP Design for 4000 Agent Deployment

*Figure 28: Unified CVP Design for 4000 Agent Deployment*



### Unified CVP Design for 12000 Agent Deployment

*Figure 29: Unified CVP Design for 12000 Agent Deployment*



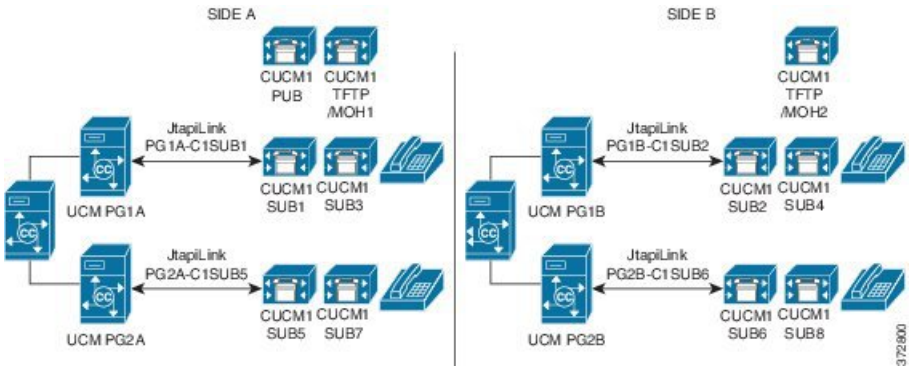

## Unified CM Design Considerations

This section contains the Unified CM cluster design considerations for HCS deployment models.

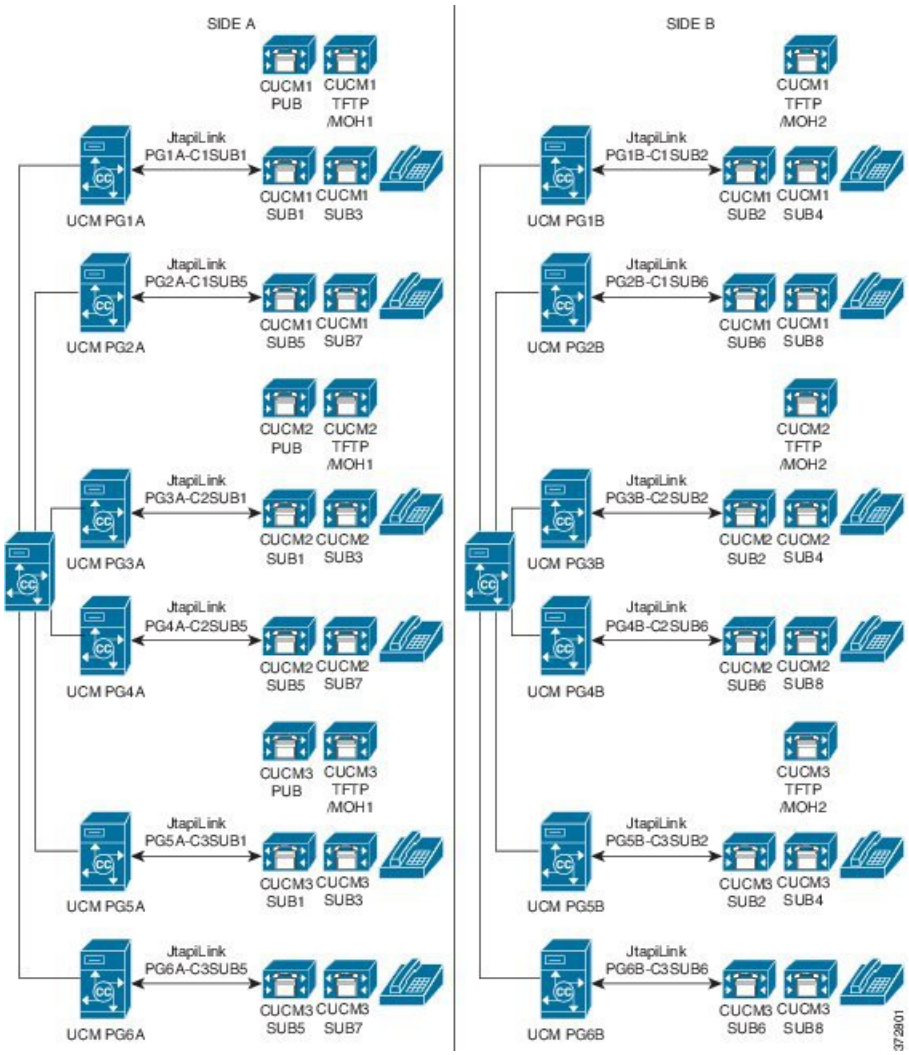
- Unified CM Design for 500 and 1000 Agent Deployment Models , on page 101
- Unified CM Design for 4000 Agent Deployment Model , on page 102
- Unified CM Design for 12000 Agent Deployment Model, on page 103

### Unified CM Design for 500 and 1000 Agent Deployment Models

## Unified CM Design for 4000 Agent Deployment Model



### Unified CM Design for 12000 Agent Deployment Model



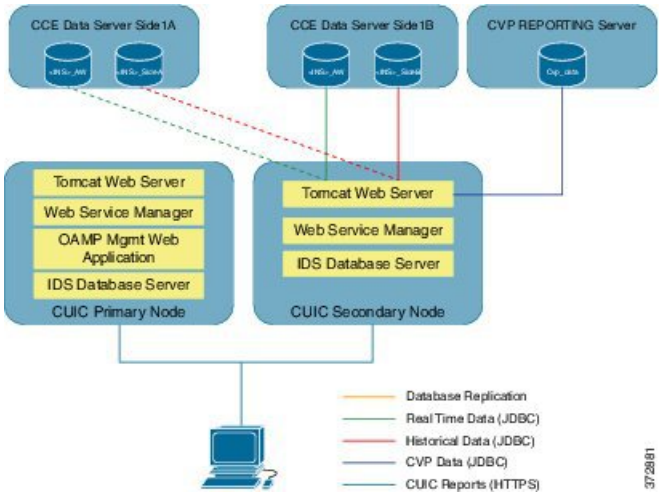

## Unified IC Design Considerations

This section describes IC design for each deployments:

- Unified IC Design for 500 and 1000 Agent Deployments, on page 104
- Unified IC Design for 4000 Agent Deployment, on page 104
- Unified IC Design for 12000 Agent Deployment, on page 105

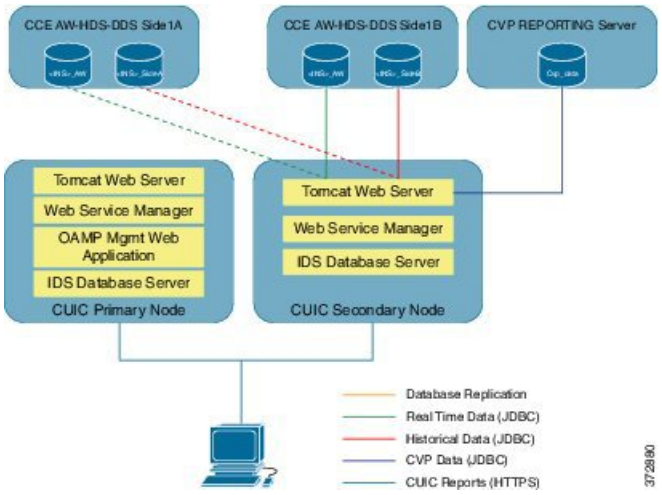
## Unified IC Design for 500 and 1000 Agent Deployments

*Figure 30: Unified IC Design for 500 and 1000 Agent Deployments*



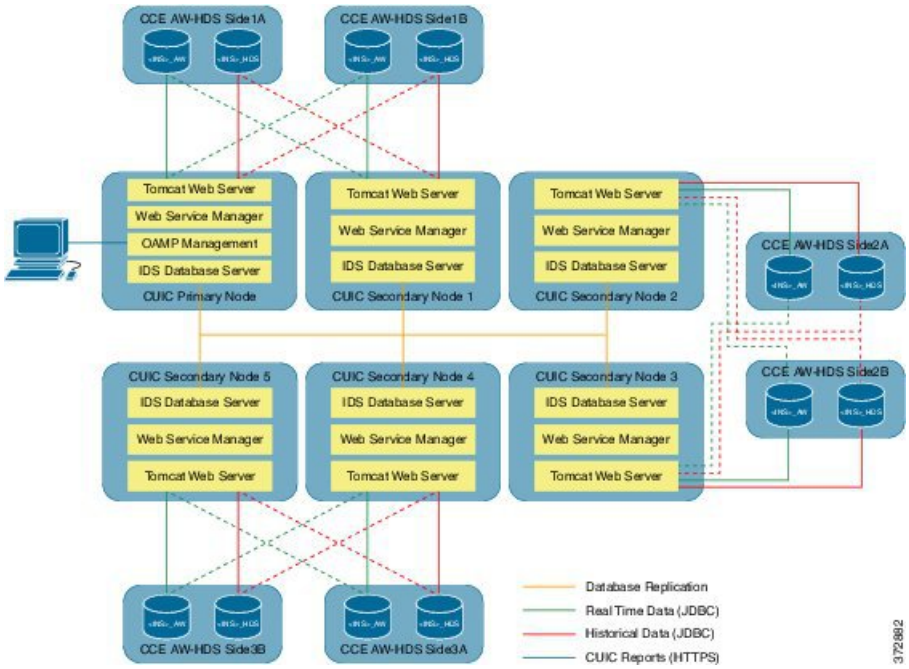

## Unified IC Design for 4000 Agent Deployment

*Figure 31: Unified IC Design for 4000 Agent Deployment*



### Unified IC Design for 12000 Agent Deployment

*Figure 32: Unified IC Design for 12000 Agent Deployment*




# Core Component High Availability Considerations

This section describes the High Availability considerations for Cisco HCS for Contact Center core components:

- Unified CCE High Availability, on page 107
- Unified CVP High Availability, on page 109
- Unified CM High Availability, on page 111
- Gateway High Availability, on page 115
- MRCP ASR/TTS High Availability, on page 115
- Cisco Finesse High Availability, on page 115

The following table shows the failover scenarios for the HCS for Contact Center components, the impact on active and new calls, and the postrecovery actions.

*Table 23: HCS for Contact Center Failover*

| Component | Failover scenario | New call impact | Active call impact | Post recovery action |
|---|---|---|---|---|
| **Unified CM** | Visible network failure | Disrupts new calls while the phones route to the backup subscriber. Processes the calls when the routing completes. | In-progress calls remain active, with no supplementary services such as conference or transfer. | After the network of the primary subscriber becomes active, the phones align to the primary subscriber. |
| | Call manager service in Unified CM primary subscriber failure | Disrupts new calls while the phones route to the backup subscriber. Processes the calls when the routing completes. | In-progress calls remain active, with no supplementary services such as conference or transfer. | After the call manager service in the Unified CM primary subscriber recovers, all idle phones route back to the primary subscriber. |
| | Unified CM CTI Manager service on primary subscriber failure | Disrupts new calls while the phones route to the backup subscriber. Processes the calls when the routing completes. | In-progress calls remain active, with no supplementary services such as conference or transfer. | After the Unified CM CTI Manager service on primary subscriber recovers, peripheral gateway side B remains active and uses the CTI Manager service on the Unified CM backup subscriber. The peripheral gateway does not switch over. |
| **Gateway** | Primary gateway is unreachable | New calls redirect to the backup gateway. | In-progress calls become inactive. | After the primary gateway restores, calls (active and new) route back to the primary gateway. |
| **MRCP ASR/TTS** | Primary server is not accessible | New calls redirect to the backup ASR/TTS server | In-progress calls remain active and redirect to the backup ASR/TTS server. | After the primary server restores, calls (active and new) route back to the primary ASR/TTS server. |

| Component | Failover scenario | New call impact | Active call impact | Post recovery action |
|---|---|---|---|---|
| **Blade** | Blade failover | Disrupts new calls while backup server components become active. | In-progress calls become inactive. | After backup server components restores, calls (active and new) route back to the primary server. |
| **WAN Link** | Unified CM calls survivability during WAN link failure. | The new calls redirects to the Survivable Remote Site Telephony (SRST). | The in-progress calls redirects to the Survivable Remote Site Telephony (SRST). | After the WAN Link restores, the calls redirects to the Unified Communications Manager. |
| | Unified CVP calls survivability during WAN link failure. | A combination of services from a TCL script (survivability.tcl) and SRST functions handles survivability new calls.<br>The TCL script redirects the new calls to a configurable destination.<br>**Note** The destination choices for the TCL script are configured as parameters in the Cisco IOS Gateway configuration.<br>The new calls can also be redirected to the alternative destinations, including the SRST, *8 TNT, or hookflash. For transfers to the SRST call agent, the most common target is an SRST alias or a Basic ACD hunt group. | A combination of services from a TCL script (survivability.tcl) and SRST functions handles survivability in-progress calls.<br>The TCL script redirects the new calls to a configurable destination.<br>**Note** The destination choices for the TCL script are configured as parameters in the Cisco IOS Gateway configuration.<br>The in-progress calls can also be redirected to the alternative destinations, including the SRST, *8 TNT, or hookflash. For transfers to the SRST call agent, the most common target is an SRST alias or a Basic ACD hunt group. | After the WAN Link restores, the calls redirects to the Unified CVP. |

## Unified CCE High Availability

In 500 and 1000 agent deployment model the Unified CCE Call Server contains the Unified CCE Router, Unified CCE PG, CG, and the CTI OS server and the Database server contains the Logger and the Unified

CCE Administration Server and Real-Time Data Server. In 4000 agent deployment the Unified CCE Rogger contains Router and Logger, Unified PG server contains PG, CG, and CTI OS Server.

This section describes how high availability works for each component within a Unified CCE Call Server and Unified Database Server or within CCE Rogger and PG servers.

### Agent PIM

Connect Side A of Agent PIM to one subscriber and Side B to another subscriber. Each of Unified CM subscribers A and B must run a local instance of CTI Manager. When PG(PIM) side A fails, PG(PIM) side B becomes active. Agents' calls in progress continue but with no third-party call control (conference, transfer, and so forth) available from their agent desktop softphones. Agents that are not on calls may notice their CTI desktop disable their agent state or third-party call control buttons on the desktop during the failover to the B-Side PIM. After the failover completes, the agent desktop buttons are restored. When PG side A recovers, PG side B remains active and uses the CTI Manager on Unified CM Subscriber B. The PIM does not fail-back to the A-Side, and call processing continues on the PG Side B.

### VRU PIM

When the VRU PIM fails, all the calls in progress or queued in the Unified CVP does not drop. The Survivability TCL script in the Voice Gateway redirects the calls to a secondary Unified CVP or a number in the SIP dial plan, if available. The redundant (duplex) VRU PIM side connects to the Unified CVP and begins processing new calls upon failover. The failed VRU PIM side recovers, and the currently running VRU PIM continues to operate as the active VRU PIM.

### CTI Server

CTI Server is redundant and resides on the Unified CCE Call server or PG. When the CTI Server fails, the redundant CTI server becomes active and begins processing call events. Both CTI OS and Unified Finesse Servers are clients of the CTI Server and are designed to monitor both CTI Servers in a duplex environment and maintain the agent state during failover processing. Agents (logged in to either CTI OS desktops or Cisco Finesse) see their desktop buttons dim during the failover to prevent them from attempting to perform tasks while the CTI Server is down. The buttons are restored as soon as the redundant CTI Server is restored and the agent can resume tasks . In some cases, an agent must sign in again after the failover completes.

### CTI OS Server

CTI OS server is a software component that runs co-resident on the Unified CCE Call server or PG. Unlike the PG processes that run in hot-standby mode, both of the CTI OS Server processes run in active mode all the time. The CTI OS server processes are managed by Node Manager, which monitors each process running as part of the CTI OS service and which automatically restarts abnormally terminated processes. When a CTI OS client loses connection to CTI OS side A, it automatically connects to CTI OS server side B. During this transition, the buttons of the CTI Toolkit Agent Desktop are disabled and return to the operational state as soon as it is connected to CTI OS server B. Node Manager restarts CTI OS server A. When the failed server restarts, new agent desktop sessions can sign in on that server. Agent desktops that are signed in on the redundant server remain on that server.

### Unified CCE Call Router

The Call Router software runs in synchronized execution. Both of the redundant systems run the same memory image of the current state across the system and update this information by passing the state events between the servers on the private connection. If one of the Unified CCE Call Routers fails, the surviving server detects the failure after missing five consecutive TCP keepalive messages on the private LAN. During Call Router failover processing, any Route Requests that are sent to the Call Router from a peripheral gateway (PG) are queued until the surviving Call Router is in active simplex mode. Any calls in progress in the Unified CVP or at an agent are not impacted.

### Unified CCE Logger

If one of the Unified CCE Logger and Database Servers fails, there is no immediate impact except that the local Call Router is no longer able to store data from call processing. The redundant Logger continues to accept data from its local Call Router. When the Logger server is restored, the Logger contacts the redundant Logger to determine how long it was off-line. The Loggers maintain a recovery key that tracks the date and time of each entry recorded in the database and these keys are used to restore data to the failed Logger over the private network. Additionally, if the Unified Outbound Option is used, the Campaign Manager software is loaded on Logger A only. If that platform is out of service, any outbound calling stops until the Logger is restored to operational status.

### Unified CCE Administration and Data Server

The Unified Contact Center Enterprise Administration and Data Server provides the user interface to the system for making configuration and scripting changes. This component does not support redundant or duplex operation as do the other Unified Contact Center Enterprise system components.

## Unified CVP High Availability

Unified CVP high availability describes the behavior of the following Unified CVP solution components.

- Unified CVP Call Server, on page 109
- Unified CVP Media Server, on page 110
- Cisco Voice XML Gateway, on page 110
- Unified CVP Reporting Server, on page 111
- Unified CM, on page 111

### Unified CVP Call Server

The Unified CVP Call Server component provides the following independent services:

- Unified CVP SIP Service, on page 110
- Unified CVP IVR Service, on page 110

### Unified CVP SIP Service

The Unified CVP SIP Service handles all incoming and outgoing SIP messaging and SIP routing. If the SIP service fails, the following conditions apply to call disposition:

- Calls in progress - If the Unified CVP SIP Service fails after the caller is transferred (including transfers to an IP phone or VoiceXML gateway), then the call continues normally until a subsequent transfer activity (if applicable) is required from the Unified CVP SIP Service.
- New calls - New calls are directed to an alternate Unified CVP Call Server.

### Unified CVP IVR Service

The Unified CVP IVR Service creates the Voice XML pages that implement the Unified CVP Micro applications based on Run VRU Script instructions received from Cisco Unified Intelligent Contact Management (ICM). If the Unified CVP IVR Service fails, the following conditions apply to the call disposition:

- Calls in progress - Calls in progress are routed by default to an alternate location by survivability on the originating gateway.
- New calls - New calls are directed to an in-service Unified CVP IVR Service.

## Unified CVP Media Server

Store the audio files locally in flash memory on the VoiceXML gateway or on an HTTP or TFTP file server. Audio files stored locally are highly available. However, HTTP or TFTP file servers provide the advantage of centralized administration of audio files. If the media server fails, the following conditions apply to the call disposition:

- Calls in progress - Calls in progress recover automatically. The high-availability configuration techniques make the failure transparent to the caller.
- New calls - New calls are directed transparently to the backup media server, and service is not affected.
- The Unified CVP VXML Server executes advanced IVR applications by exchanging VoiceXML pages with the VoiceXML gateways' built-in voice browser. If the Unified CVP VXML Server fails, the following conditions apply to the call disposition:
  - Calls in progress - Calls in progress in an ICM-integrated deployment can be recovered using scripting techniques.
  - New calls - New calls are directed transparently to an alternate Unified CVP VXML Server.

## Cisco Voice XML Gateway

The Cisco VoiceXML gateway parses and renders VoiceXML documents obtained from one or several sources. If the VoiceXML gateway fails, the following conditions apply to the call disposition:

- Calls in progress - Calls in progress are routed by default to an alternate location by survivability on the ingress gateway.
- New calls - New calls find an alternate VoiceXML gateway.

### Unified CVP Reporting Server

The Reporting Server does not perform database administrative and maintenance activities such as backups or purges. However, the Unified CVP provides access to such maintenance tasks through the Operations Console. The Single Reporting Server does not necessarily represent a single point of failure, because data safety and security are provided by the database management system, and temporary outages are tolerated due to persistent buffering of information on the source components.

### Unified CM

The Unified CVP Call Server recognizes that the Unified CM has failed, assumes the call should be preserved, and maintains the signaling channel to the originating gateway. In this way, the originating gateway has no knowledge that Unified CM has failed.

Additional activities in the call (such as hold, transfer, or conference) are not possible. After the parties go on-hook, the phone routes to another Unified CM server.

New calls are directed to an alternate Unified CM server in the cluster.

## Unified CM High Availability


- Unified CM Design Considerations, on page 101
- Unified CM High Availability Scenarios , on page 111


### Unified CM High Availability Scenarios

This section contains various high availability scenarios including Unified CM PG and Unified CM services.


- Cisco Call Manager and CTI Manager Service Fail , on page 111
- Cisco CTI Manager Service Fails , on page 112
- Cisco Call Manager Service Fails , on page 114

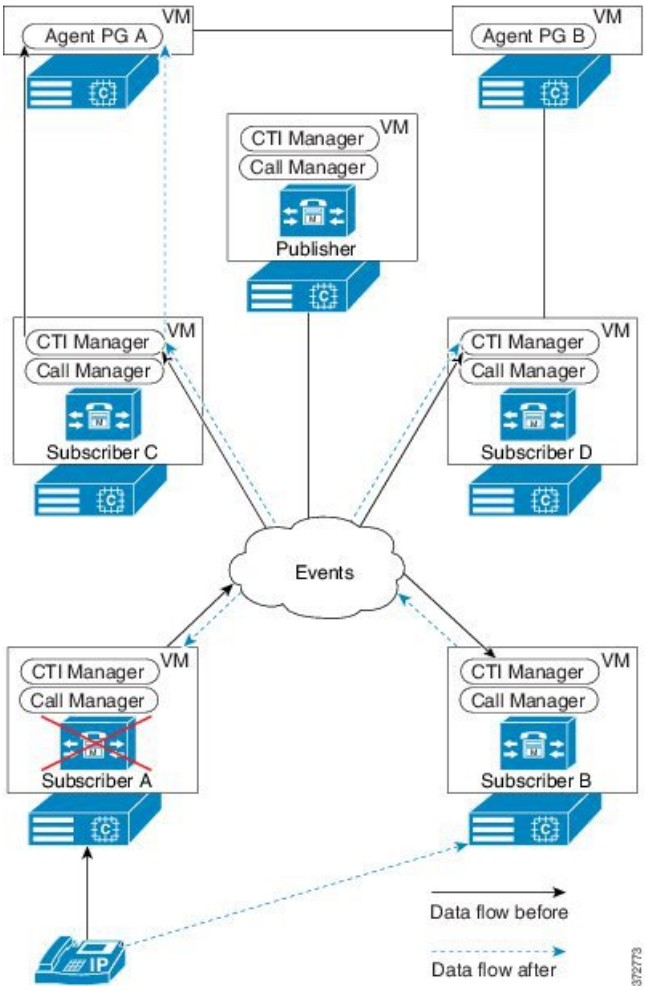

#### *Cisco Call Manager and CTI Manager Service Fail*

This scenario describes about a complete system failure or loss of network connectivity on Unified CM Subscriber A. The Cisco CTI Manager and Call Manager services are both active on the same server, and Unified CM Subscriber A is the primary CTI Manager in this case. The following conditions apply to this scenario.

- All phones and gateways are registered with Unified CM Subscriber A.
- All phones and gateways are configured to re-home to Unified CM Subscriber B( here B is the backup).
- Unified CM Subscriber A and B are each running a separate instance of CTI Manager.
- When all of the software services on Unified CM Subscriber A fail (call processing, CTI Manager, and so on), all phones and gateways re-home to Unified CM Subscriber A.
- PG side A detects a failure and induces a failover to PG side B.
- PG side B becomes active and registers all dialed numbers and phones; call processing continues.

- After an agent disconnects from all calls, the IP phone re-homes to the backup Unified CM Subscriber B. The agent will have to log in again manually using the agent desktop.
- When Unified CM Subscriber A recovers, all phones and gateways re-home to it.
- PG side B remains active, using the CTI Manager on Unified CM Subscriber B.
- During this failure, any calls in progress at an UCCE agent will remain active. When the call is completed, the phone will re-home to the backup Unified CM Subscriber B automatically.
- After the failure is recovered, the PG will not fail back to the A side of the duplex pair. All CTI messaging will be handled using the CTI Manager on Unified CM Subscriber B, this will communicate to Unified CM Subscriber A to obtain phone state and call information

***Figure 33: Subscriber Failure***




### *Cisco CTI Manager Service Fails*

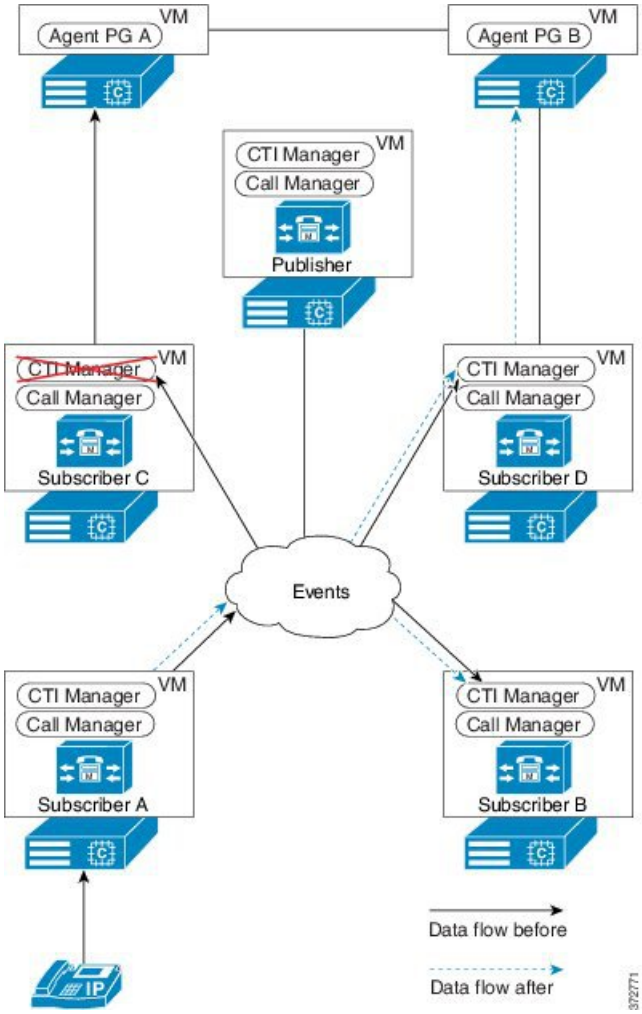
This scenario describes about a CTI Manager service failure on Unified CM Subscriber A. The CTI Manager and Cisco Call Manager services are both active on the same server, and Unified CM Subscriber A is the primary CTI Manager in this case. However, all phones and gateways are registered with Unified CM Subscriber A. During this failure, both the CTI Manager and the PG fail-over to their secondary sides. Because the JTAPI

service on PG side B is already logged into the secondary (now primary) CTI Manager, the device registration and initialization time is significantly shorter than if the JTAPI service on PG side B had to log into the CTI Manager. The following conditions apply to this scenario.

- All phones and gateways are registered with Unified CM Subscriber A.
- All phones and gateways are configured to re-home to Unified CM Subscriber B (here B is the backup).
- Unified CM Subscribers A and B are each running a separate instance of CTI Manager.
- When CTI Manager service on Unified CM Subscriber A fails, PG side A detects a failure of the CTI Manager on that server and induces a failover to PG side B.
- PG side B registers all dialed numbers and phones with Unified CM Subscriber B, and call processing continues.
- After an agent disconnects from all calls, that agent's desktop functionality is restored to the same state prior to failover.

- When Unified CM Subscriber A recovers, PG side B continues to be active and uses the CTI Manager on Unified CM Subscriber

***Figure 34: CTI Manager Failure***




### *Cisco Call Manager Service Fails*

This scenario describes about a failure on Cisco Call Manager service on Unified CM Subscriber A. The CTI Manager and Cisco Call Manager services are both active on the same server, and Unified CM Subscriber A is the primary CTI Manager in this case. However, all phones and gateways are registered with Unified CM Subscriber A. During this failure, Cisco CTI Manager is not affected because the PG communicates with the CTI Manager service, not the Cisco Call Manager service. All phones re-home individually to the standby Unified CM Subscriber B, if they are not in a call. If a phone is in a call, it re-homes to Unified CM Subscriber B after it disconnects from the call. The following conditions applies to this scenario.

- All phones and gateways are registered with Unified CM Subscriber A.
- All phones and gateways are configured to re-home to Unified CM Subscriber B (that is, B is the backup).
- Unified CM Subscribers A and B are each running a separate instance of CTI Manager.

- When Cisco Call Manager service in Unified CM Subscriber A fails, phones and gateways re-home to Unified CM Subscriber B.
- PG side A remains connected and active, with a CTI Manager connection on Unified CM Subscriber A. It does not fail-over because the JTAPI/CTI Manager connection has not failed. However, it will see the phones and devices being unregistered from Unified CM Subscriber A (where they were registered) and will then be notified of these devices being re-registered on Unified CM Subscriber B automatically. During the time that the agent phones are not registered, the PG will disable the agent desktops to prevent the agents from attempting to use the system while their phones are not actively registered with a Unified CM Subscriber B
- Call processing continues for any devices not registered to Unified CM Subscriber A. Call processing also continues for those devices on Unified CM Subscriber A when they are re-registered with their backup subscriber.
- Agents on an active call will stay in their connected state until they complete the call; however, the agent desktop will be disabled to prevent any conference, transfer, or other telephony events during the failover. After the agent disconnects the active call, that agent's phone will re-register with the backup subscriber, and the agent will have to log in again manually using the agent desktop.
- When Unified CM Subscriber A recovers, phones and gateways re-home to it. This re-homing can be set up on Unified CM to gracefully return groups of phones and devices over time or to require manual intervention during a maintenance window to minimize the impact to the call center.
- Call processing continues normally after the phones and devices have returned to their original subscriber.

## Gateway High Availability

If the primary gateway is unreachable, the CUBE redirects the calls to the backup gateway. Active calls fail. After the primary gateway becomes accessible, calls are directed back to the primary gateway.

## MRCP ASR/TTS High Availability

The VoiceXML gateway uses gateway configuration parameters to locate an ASR/TTS primary and the backup server. The backup server is invoked only if the primary server is not accessible and if this is not a load-balancing mechanism. Each new call attempts to connect to the primary server. If failover occurs, the backup server is used for the duration of the call; the next new call attempts to connect to the primary server.

## Cisco Finesse High Availability

Cisco Finesse high availability affects the following components:

- CTI, on page 116
- AWDB, on page 116
- Cisco Finesse Client, on page 117
- Desktop Behavior, on page 117

## CTI

### Pre-requisites for CTI high availability

The prerequisites for CTI high availability are as follows:

1. The Unified CCE is deployed in Duplex mode.
2. The backup CTI server is configured through the Finesse Administration Console.

When Cisco Finesse loses connection to the primary CTI server, it tries to reconnect five times. If the number of connection attempts exceeds the retry threshold, Cisco Finesse then tries to connect to the backup CTI server the same number of times. Cisco Finesse keeps repeating this process until it makes a successful connection to the CTI server.

A loss of connection to the primary CTI server can occur for the following reasons:

- Cisco Finesse misses three consecutive heartbeats from the connected CTI server.
- Cisco Finesse encounters a failure on the socket opened to the CTI server.

**Note** The new calls and the existing calls do not have any impact during the CTI failover.

During failover, Cisco Finesse does not handle client requests. Requests made during this time receive a `503 Service Unavailable` error message. Call control, call data, or agent state actions that occur during CTI failover are published as events to the Agent Desktop following CTI server reconnection.

If an agent makes or answers a call and ends that call during failover, the corresponding events are not published following CTI server reconnection.

Additionally, CTI failover may cause abnormal behavior with the Cisco Finesse Desktop due to incorrect call notifications from Unified CCE. If during failover an agent or supervisor is in a conference call, or signs-in after being on active conference with other devices not associated with another agent or supervisor, the following desktop behaviors may occur:

- The desktop does not reflect all participants in a conference call.
- The desktop does not reflect that the signed-in agent or supervisor is in an active call.
- Cisco Finesse receives inconsistent call notifications from the Unified CCE.

Despite these behaviors, the agent or supervisor can continue to perform normal operations on the phone and normal desktop behavior resumes after the agent or supervisor drops-off the conference call.

## AWDB

### Pre-requisites for AWDB high availability

The prerequisites for Administrative Workstation Database (AWDB) high availability are as follows:

- The secondary AWDB is configured.
- The secondary AWDB host is configured through the Finesse Administration Console.

The following example describes how AWDB failover occurs:

- When an agent or supervisor makes a successful API request (such as a sign-request or call control request) their credentials are cached in Cisco Finesse for 30 minutes from the time of the request. Therefore, after an authentication, that user is authenticated for 30 minutes, even if both AWDB(s) are down. Cisco Finesse attempts to re-authenticate the user only after the cache expires.
- AWDB failover occurs if Cisco Finesse loses connection to the primary server and it tries to reconnect to the secondary server. If it cannot connect to any of the AW servers and the cache expired, it returns a `401 Unauthorized HTTP` error message.

Cisco Finesse repeats this process for every API request until it connects to one of the AW servers.

During failover, Cisco Finesse does not process requests, but clients still receive events.

**Note** The new calls and the existing calls do not have any impact during the AWDB failover.

### Cisco Finesse Client

With a two-node Cisco Finesse setup (primary and secondary Cisco Finesse server), if the primary server goes out of service, agents who are signed-in to that server are redirected to the sign-in page of the secondary server.

Client failover can occur for the following reasons:

- The Cisco Tomcat Service goes down.
- The Cisco Finesse Web application Service goes down.
- The Cisco Notification Service goes down.
- Cisco Finesse loses connection to both CTI servers.

### Desktop Behavior

If the Cisco Finesse server fails, the agents logged into that server are put into a NOT READY or pending NOT READY state. Agents remain unaffected as they migrate to the back up side.

If a client disconnects, the agent is put into a NOT READY state with reason code 255. If the agent reconnects within minutes or seconds, the agent is forced to log out.

# Core Component Bandwidth, Latency and QOS Considerations

This section describes the bandwidth and QOS considerations for Cisco HCS for Contact Center core and optional components.

- Unified CCE Bandwidth, Latency and QOS Considerations, on page 118
- Unified CVP Bandwidth, Latency and QOS Considerations, on page 121
- Unified CM Bandwidth, Latency and QOS Considerations, on page 122
- Unified IC Bandwidth, Latency and QOS Considerations, on page 123
- Cisco Finesse Bandwidth, Latency and QOS Considerations, on page 126

# Unified CCE Bandwidth, Latency and QOS Considerations

## Agent Desktop to Unified CCE Call Servers/ Agent PG

There are many factors to consider when assessing the traffic and bandwidth requirements between Agent or Supervisor Desktops and Unified CCE Call Servers/Agent PG. While the VoIP packet stream bandwidth is the predominant contributing factor to bandwidth usage, you must also consider other factors such as call control, agent state signaling, silent monitoring, recording, and statistics.

The amount of bandwidth required for CTI Desktop to CTI OS Server messaging is (0.5 x n) + (16 x cps), where n is the number CTI Clients and cps is the number of calls per second.

For example, for a 500 agent deployment, for each contact center (datacenter) and remote site the approximate bandwidth is, (0.5 x 500) + (16 x 1) = 340 kbps.

For example, for a 1000 agent deployment, for each contact center (datacenter) and remote site the approximate bandwidth is, (0.5 x 1000) + (16 x 8) = 608 kbps.

Cisco supports limiting the latency between the server and agent desktop to 400 ms round-trip time for CTI OS (preferably less than 200 ms round-trip time).

## Unified CCE Data Server to Unified CCE Call Server for 500 and 1000 Agent Deployment Model

Unified CCE Central Controllers (Routers and Loggers) require a separate network path or link to carry the private communications between the two redundant sides. Latency across the private separate link must not exceed 100 ms one way (200 ms round-trip), but 50 ms (100 ms round-trip) is preferred.

## Private Network Bandwidth Requirements for Unified CCE

The following table is a worksheet to assist with computing the link and queue sizes for the private network. Definitions and examples follow the table.

**Note** Minimum link size in all cases is 1.5 Mbps (T1).

***Table 24: Worksheet for Calculating Private Network Bandwidth***

| Component | Effective BHCA | Multiplication Factor | Recommended Link | Multiplication Factor | Recommended Queue | |
|---|---|---|---|---|---|---|
| Router + Logger | | * 30 | | * 0.8 | | Total Router + Logger High- Priority Queue Bandwidth |

| Component | Effective BHCA | Multiplication Factor | Recommended Link | Multiplication Factor | Recommended Queue | |
|---|---|---|---|---|---|---|
| Unified CM PG | | * 100 | | * 0.9 | | Add these numbers together and total in the box below to get the PG High- Priority Queue Bandwidth |
| Unified VRU PG | | * 120 | | * 0.9 | | |
| Unified CVP Variables | | * ((Number of Variables * Average Variable Length)/40) | | * 0.9 | | |
| | | **Total Link Size** | | | | **Total PG High-Priority Queue Bandwidth** |

If one dedicated link is used between sites for private communications, add all link sizes together and use the Total Link Size at the bottom of the table above. If separate links are used, one for Router/Logger Private and one for PG Private, use the first row for Router/Logger requirements and the bottom three (out of four) rows added together for PG Private requirements.

Effective BHCA (effective load) on all similar components that are split across the WAN is defined as follows:

**Router + Logger**

This value is the total BHCA on the call center, including conferences and transfers. For example,10,000 BHCA ingress with 10% conferences or transfers are 11,000 effective BHCA.

**Unified CM PG**

This value includes all calls that come through Unified CCE Route Points controlled by Unified CM and/or that are ultimately transferred to agents. This assumes that each call comes into a route point and is eventually sent to an agent. For example, 10,000 BHCA ingress calls coming into a route point and being transferred to agents, with 10% conferences or transfers, are 11,000 effective BHCA.

**Unified VRU PG**

This value is the total BHCA for call treatment and queuing coming through a Unified CVP. 100%treatment is assumed in the calculation. For example, 10,000 BHCA ingress calls, with all of them receiving treatment and 40% being queued, are 14,000 effective BHCA.

**Unified CVP Variables**

This value represents the number of Call and ECC variables and the variable lengths associated with all calls routed through the Unified CVP, whichever technology is used in the implementation.

### Example of a Private Bandwidth Calculation

The table below shows an example calculation for a combined dedicated private link with the following characteristics:

- BHCA coming into the contact center is 10,000.

- 100% of calls are treated by Unified CVP and 40% are queued.
- All calls are sent to agents unless abandoned. 10% of calls to agents are transfers or conferences.
- There are four Unified CVPs used to treat and queue the calls, with one PG pair supporting them.
- There is one Unified CM PG pair for a total of 900 agents.
- Calls have ten 40-byte Call Variables and ten 40-byte ECC variables.

***Table 25: Example Calculation for a Combined Dedicated Private Link***

| Component | Effective BHCA | Multiplication Factor | Recommended Link | Multiplication Factor | Recommended Queue | |
|---|---|---|---|---|---|---|
| Router + Logger | 11,000 | * 30 | 330,000 | * 0.8 | 264,000 | Total Router + Logger High- Priority Queue Bandwidth |
| Unified CM PG | 11,000 | * 100 | 1,100,000 | * 0.9 | 990,000 | Add these numbers together and total in the box below to get the PG High- Priority Queue Bandwidth |
| Unified VRU PG | 0 | * 120 | 0 | * 0.9 | 0 | |
| Unified CVP Variables | 14,000 | * ((Number of Variables * Average Variable Length)/40) | 280,000 | * 0.9 | 252,000 | |
| | | **Total Link Size** | 1,710,000 | | 1,242,000 | **Total PG High-Priority Queue Bandwidth** |

For the combined dedicated link in this example, the results are as follows:

- Total Link Size = 1,710,000 bps
- Router/Logger high-priority bandwidth queue of 264,000 bps
- PG high-priority queue bandwidth of 1,242,000 bps

If this example were implemented with two separate links, Router/Logger private and PG private, the link sizes and queues are as follows:

- Router/Logger link of 330,000 bps (actual minimum link is 1.5 Mb, as defined earlier), with high-priority bandwidth queue of 264,000 bps
- PG link of 1,380,000 bps, with high-priority bandwidth queue of 1,242,000 bps

When using Multilink Point-to-Point Protocol (MLPPP) for private networks, set the following attributes for the MLPPP link:

- Use per-destination load balancing instead of per-packet load balancing.
- Enable Point-to-Point Protocol (PPP) fragmentation to reduce serialization delay.

**Note** You must have two separate multilinks with one link each for per-destination load balancing.

## Unified CVP Bandwidth, Latency and QOS Considerations

### Bandwidth Considerations for Unified CVP

The ingress and VoiceXML gateway is separated from the servers that provide it with media files, VoiceXML documents, and call control signaling. Therefore, you must consider the bandwidth requirement for the Unified CVP.

For example, assume that all calls to a branch begin with 1 minute of IVR treatment followed by a single transfer to an agent that lasts for 1 minute. Each branch has 20 agents, and each agent handles 30 calls per hour for a total of 600 calls per hour per branch. The call average rate is therefore 0.166 calls per second (cps) per branch.

Note that even a small change in these variables can have a large impact on sizing. Remember that 0.166 calls per second is an average for the entire hour. Typically, calls do not come in uniformly across an entire hour, and there are usually peaks and valleys within the busy hour. You should find the busiest traffic period, and calculate the call arrival rate based on the worst-case scenario.

### VoiceXML Document Types

On average, a VoiceXML document between the Unified CVP Call Server or Unified CVP VXML Server and the gateway is 7 kilobytes. You can calculate the bandwidth used by approximating the number of prompts that are used per call, per minute. The calculation, for this example, is as follows:

7000 bytes x 8 bits = 56,000 bits per prompt

(0.166 call/second) x (56,000 bit/prompt) x (no. of prompts/call) = bps per branch

### Media File Retrieval

You can store the Media files prompts locally in flash memory on each router. This method eliminates bandwidth considerations, but maintainability becomes an issue because you must replace the prompts on every router. If you store the prompts on an HTTP media server (or an HTTP cache engine), the gateway can locally cache voice prompts after it first retrieves them. The HTTP media server can cache many, if not all, prompts, depending on the number and size of the prompts. The refresh period for the prompts is defined on the HTTP media server. Therefore, the bandwidth utilized is limited to the initial load of the prompts at each gateway, plus periodic updates after the expiration of the refresh interval. If the prompts are not cached at the

gateway, a significant Cisco IOS performance degradation (as much as 35% to 40%) in addition to the extra bandwidth usage occurs.

Assume that there are a total of 50 prompts, with an average size of 50 KB and a refresh interval of 15 minutes.

The bandwidth usage is:

(50 prompts) x (50,000 bytes/prompt) x (8 bits/byte) = 20,000,000 bits

(20,000,000 bits) / (900 secs) = 22.2 average kbps per branch

### QOS Considerations for Unified CVP

The Unified CVP Call Server marks the QoS DSCP for SIP messages.

***Table 26: Unified CVP QoS***

| Component | Port | Queue | PHB | DSCP | Max latency Round Trip |
|---|---|---|---|---|---|
| Media Server | TCP 80 | CVP-data | AF11 | 10 | 1 sec |
| Unified CVP Call Server (SIP) | TCP 5060 | Call Signaling | CS3 | 24 | 200 ms |
| Unified CVP IVR service | TCP 8000 | CVP-data | AF11 | 10 | 1 sec |
| Unified CVP VXML Server | TCP 7000 | CVP-data | AF11 | 10 | 1 sec |
| Ingress Gateway SIP | TCP 5060 | Call Signaling | CS3 | 24 | 200 ms |
| VXML Gateway SIP | TCP 5060 | Call Signaling | CS3 | 24 | 200 ms |

**Note** The Unified CCE and Unified CVP provide a Layer 3 marking (not a Layer 2).

As a general rule, activate QoS at the application layer and trust it in the network.

## Unified CM Bandwidth, Latency and QOS Considerations

### Agent Phones to Unified Communications Manager Cluster

The amount of bandwidth that is required for phone-to-Unified Communications Manager signaling is 150 bps x n, where n is the number of phones.

For example for a 500 agent deployment model, for each contact center site the approximate required bandwidth is 150 x 500 phones = 75kbps

For example for a 1000 agent deployment model, for each contact center site the approximate required bandwidth is 150 x 1000 phones = 150kbps

## Unified IC Bandwidth, Latency and QOS Considerations

### Reporting Bandwidth

The following parameters have a combined effect on the responsiveness and performance of the Cisco Unified Intelligence Center on the desktop:

- Real-time reports: Simultaneous real-time reports run by a single user.
- Refresh rate/realtime: Note that if you have a Premium license you can change the refresh rate by editing the Report Definition. The default refresh rate for Unified Intelligence Center Release 9.1(1) is 15 seconds.
- Cells per report — The number of columns that are retrieved and displayed in a report.
- Historical report — Number of historical reports run by a single user per hour.
- Refresh rate/historical — The frequency with report data are refreshed on a historical report.
- Rows per report — Total number of rows on a single report.
- Charts per dashboard — Number of charts (pie, bar, line) in use concurrently on a single dashboard.
- Gauges per dashboard — Number of gauges (speedometer) in use concurrently on a single dashboard.

### Network Bandwidth Requirements

The exact bandwidth requirement differs based on the sizing parameters used, such as the number of rows, the refresh frequency, and the number of columns present in each report.

You can use the Bandwidth Calculator to calculate the bandwidth requirements for your Unified Intelligence Center implementation. (Use the same Microsoft Excel file for Releases 9.0 and 8.5.)

Two examples for bandwidth calculation (50 and 100 users):

| Unified Intelligence Center User Profile | Customer Parameters | Value | Network Bandwidth Requirement (in Kbps) | | | |
|---|---|---|---|---|---|---|
| | | | Unified Intelligence Center–AW/HDS | Client–Unified Intelligence Center | Unified Intelligence Center--Unified Intelligence Center | Unified Intelligence Center--Unified Intelligence Center for each node |
| Profile 1 (500 agent deployment) | Total concurrent Users | 50 | 1,283 | 1,454 | N/A | N/A |
| | Number of Real Time Reports | 2 | | | | |
| | Real Time Report Interval (in second) | 15 | | | | |
| | Number of Average Rows per RT Report | 50 | | | | |
| | Number of Average Columns per RT Report | 10 | | | | |
| | Number of Historical Report | 1 | | | | |
| | Historical Report Interval (in second) | 1800 | | | | |
| | Number of Average Rows per Historical Report | 800 | | | | |
| | Number of Average Columns per Historical Report | 10 | | | | |
| | Number of Nodes on side A | 1 | | | | |
| | Number of Nodes on side B | 0 | | | | |

| Unified Intelligence Center User Profile | Customer Parameters | Value | Network Bandwidth Requirement (in Kbps) | | | |
|---|---|---|---|---|---|---|
| | | | Unified Intelligence Center–AW/HDS | Client–Unified Intelligence Center | Unified Intelligence Center--Unified Intelligence Center | Unified Intelligence Center--Unified Intelligence Center for each node |
| Profile 2 (1000 agent deployment) | Total concurrent Users | 100 | 1,783 | 4,554 | 1,935 | 967 |
| | Number of Real Time Reports | 2 | | | | |
| | Real Time Report Interval (in second) | 15 | | | | |
| | Number of Average Rows per RT Report | 50 | | | | |
| | Number of Average Columns per RT Report | 20 | | | | |
| | Number of Historical Report | 1 | | | | |
| | Historical Report Interval (in second) | 1800 | | | | |
| | Number of Average Rows per Historical Report | 200 | | | | |
| | Number of Average Columns per Historical Report | 20 | | | | |
| | Number of Nodes on side A* | 1 | | | | |
| | Number of Nodes on side B* | 2 | | | | |

### Cisco Finesse Bandwidth, Latency and QOS Considerations

The most expensive operation from a network perspective is the agent or supervisor login. This operation involves the web page load and includes the CTI login and the display of the initial agent state. After the desktop web page loads, the required bandwidth is significantly less.

The number of bytes transmitted at the time an agent logs in is approximately 2.8 megabytes. Because of the additional gadgets on the supervisor desktop (Team Performance, Queue Statistics), this number is higher for a supervisor login - approximately 5.2 megabytes. Cisco does not mandate a minimum bandwidth for the login operations. You must determine how long you want the login to take and determine the required bandwidth accordingly. To help you with this calculation, Cisco Finesse provides a bandwidth calculator to estimate the bandwidth required to accommodate the client login time. Note that during failover, agents are redirected to the alternate Finesse server and required to log in again. For example, if you configure your bandwidth so that login takes 5 minutes and a client failover event occurs, agents will take 5 minutes to successfully log in to the alternate Finesse server.

**Note** The Cisco Finesse bandwidth calculator does not include the bandwidth required for any third-party gadgets in the Finesse container or any other applications running on the agent desktop client.

# Core Component Integrated Options Considerations



# Courtesy Callback Considerations

## Callback Criteria

In your callback script, you can establish criteria for offering a caller courtesy callback. Examples of callback criteria include:

- Number of minutes a customer is expected to be waiting in queue that exceeds a maximum number of minutes (based on your average call handling time per customer)
- 

**Note** The included example scripts use this method for determining callback eligibility.

- Assigned status of a customer (gold customers may be offered the opportunity to be called back instead of remaining on the line)
- The service a customer has requested (sales calls, or system upgrades, for example, may be established as callback criteria)

## Sample Scripts and Audio Files for Courtesy Callback

The courtesy callback feature is implemented using Unified CCE scripts. The installation provides a set of modifiable example CCE scripts, call studio scripts, and audio files to get you started. You can use these scripts in your implementation after making a few required changes.

## Typical Use Scenario

**Note** Courtesy Callback is supported for IP originated calls as well.

A typical use of the Courtesy Callback feature follows this pattern:

1. The caller arrives at Unified CVP and the call is treated in the normal IVR environment.
2. The Call Studio and Unified ICM Courtesy Callback scripts determine if the caller is eligible for a callback based on the rules of your organization (such as in the prior list of conditions).
3. If a courtesy callback can be offered, the system notifies the caller the approximate wait time and offers to call the customer back when an agent is available.
4. If the caller chooses not to use the callback feature, queuing continues as normal. Otherwise, the call continues as indicated in the remaining steps.
5. If the caller chooses to receive a callback, the system prompts the caller to record their name and to key in their phone number.
6. The system writes a database record to log the callback information.

**Note** If the database is not accessible, then the caller is not offered a callback and they are placed in queue.

7. The caller is disconnected from the TDM side of the call. However, the IP side of the call in Unified CVP and Unified ICM is still active. This keeps the call in the same queue position. No queue music is played, so Voice XML gateway resources used during this time are less than if the caller had actually been in queue.

8 When an agent in the service/skill category the caller is waiting for is close to being available (as determined by your callback scripts), then the system calls the person back. The recorded name is announced when the callback is made to insure the correct person accepts the call.

9 The system asks the caller, through an IVR session, to confirm that they are the person who was waiting for the call and that they are ready for the callback.

If the system cannot reach the callback number provided by the caller (for example, the line is busy, RNA, network problems, etc.) or if the caller do not confirm they are the caller, then the call is not sent to an agent. The agent is always guaranteed that someone is there waiting when they take the call. The system ensures that the caller is already on the line by the time the agent gets the call.

This feature is called preemptive callback as the system assumes that the caller is already on the line by the time the agent gets the call and that the caller has to wait minimal time in queue before speaking to an agent.

10 The system presents the call context on the agent screen-pop, as normal.

In the event that the caller cannot be reached after a configurable maximum number and frequency of retries, the callback is aborted and the database status is updated appropriately. You can run reports to determine if any manual callbacks are necessary based on your business rules.

# Agent Greeting Considerations


- Agent Greeting Phone Requirements (for Local Agents only), on page 128
- Agent Greeting Design Considerations, on page 129


**Note** VXML gateway IVR leg dial-peer must not use the voice-class codec, it should use either the codec G.711u-law or the codec G.711a-law.

## Agent Greeting Phone Requirements (for Local Agents only)

Agent greeting is available to agents and supervisors who use IP Phones with Built-In Bridge (BIB). These agents are typically located within a contact center. Phones used with Agent Greeting must meet these requirements:

- The phones must have the BIB feature

**Note** If you disable BIB, the system attempts to use a conference bridge for agent greeting call flow and raises a warning event.

- The phones must be running firmware version CM 8.5(1) or greater (In most cases, phone firmware upgrades automatically when you upgrade your Unified Communications Manager installation.)
- See the IP Phone support for the list of supported phone models

## Agent Greeting Design Considerations

The following sections list the functional limitations for Agent Greeting and Whisper Announcement.

Agent Greeting has the following limitations:

- Agent Greeting is not supported with outbound calls made by an agent. The announcement plays for inbound calls only.
- Only one Agent Greeting file plays per call.
- Supervisors cannot listen to agents' recorded greetings.
- Agent Greetings do not play when the router selects the agent through a label node.
- The default CTI OS Toolkit agent desktop includes the Agent Greeting buttons. If Agent Greeting is not configured, the Agent Greeting buttons do not work. If you use the default desktop but do not plan to use Agent Greeting, you should remove the Agent Greeting button.
- Silent Monitoring (CTI OS and Unified CM-based) is supported with Agent Greeting with the following exception: For Unified-CM based Silent Monitoring, supervisors cannot hear the greetings. If a supervisor clicks the Silent Monitor button on the CTI OS desktop while a greeting is playing, a message displays stating that a greeting is playing and to try again shortly.

You can use Agent Greeting with the Whisper Announcement feature. Here are some things to consider when using them together:

- On the call, the Whisper Announcement always plays first
- To shorten your call-handling time, use shorter Whisper Announcements and Agent Greetings than you might if you were using either feature by itself. A long Whisper Announcement followed by a long Agent Greeting equals a long wait before an agent actively handles a call
- If you use a Whisper Announcement, your agents probably handle different types of calls: for example, "English-Gold Member-Activate Card," "English-Gold Member-Report Lost Card," "English-Platinum Member-Account Inquiry." Therefore, you may want to ensure that greetings your agents record are generic enough to cover the range of call types

# Whisper Announcement Considerations

Whisper announcement has the following Considerations:

- Announcements do not play for outbound calls made by an agent. The announcement plays for inbound calls only
- For Whisper Announcement to work with agent-to-agent calls, use the SendToVRU node before you send the call to the agent. You must send the transferred call to Unified CVP before you send the call to another agent. Then, Unified CVP can control the call and play the announcement, regardless of which node sends the call to Unified CVP
- CVP Refer Transfers do not support Whisper Announcement
- Whisper Announcement supports Silent Monitoring (CTI OS and Unified CM-based) with this exception:

- For Unified Communications Manager-based Silent Monitoring, supervisors cannot hear the announcements themselves. The supervisor desktop dims the Silent Monitor button while an announcement plays
- Only one announcement can play for each call. While an announcement plays, you cannot put the call on hold, transfer, or conference; release the call; or request supervisor assistance.These features become available again after the announcement completes.

# Mobile Agent Considerations



## Cisco Unified Mobile Agent Description

Mobile Agent enables an agent to use any PSTN phone and a broadband VPN connection (for agent desktop communications). The agent has the same capabilities as an agent in your call center using a Cisco IP Phone.

Unified Mobile Agent supports call center agents using phones that HCS-CC does not directly control. You can deploy a Mobile Agent as follows:

- Outside the contact center, by using an analog phone or a mobile phone in the home.
- On an IP phone connection that is not CTI-controlled by Packaged CCE, by Unified CCE, by HCS-CC or by an associated Unified Communications Manager.
- On any voice endpoint of any ACD (including endpoints on other Unified Communication Managers) that the contact center Unified Communication Manager can reach by a SIP trunk.

A Mobile Agent can use different phone numbers at different times; the agent enters the phone number at login time. An agent can access the Mobile Agent functionality using any phone number that is included in the Unified Communications Manager dial plan.

### Unified Mobile Agent Provides Agent Sign-In Flexibility

Agents can be either local agents or Mobile Agents, depending on how they sign in at various times.

Regardless of whether agents sign in as local or Mobile Agents, their skill groups do not change. Because agents are chosen by existing selection rules and not by how they are connected, the same routing applies regardless of how the agents log in. If you want to control routing depending on whether agents are local or mobile, assign the agents to different skill groups and design your scripts accordingly.

### Connection Modes

Cisco Unified Mobile Agent allows system administrators to configure agents to use either call by call dialing or a nailed connection, or the administrator can configure agents to choose a connection mode at login time.

Mobile Agents are defined as agents using phones not directly controlled by Unified CC, irrespective of their physical location. (The term local agent refers to an agent who uses a phone that is under control of Unified CC, irrespective of physical location.)

You can configure Mobile Agents using either of two delivery modes:

- Call by Call—In this mode, the Mobile Agent's phone is dialed for each incoming call. When the call ends, the Mobile Agent's phone is disconnected before being made ready for the next call.
- Nailed Connection—In this mode, the agent is called at login time and the line stays connected through multiple customer calls.

**Note** The administrator can select the *Agent chooses* option, which allows an agent to select a call delivery mode at login.

### *Call by Call*

In a *call by call* delivery mode, the Mobile Agent's phone is dialed for each incoming call. When the call ends, the Mobile Agent's phone disconnects before is it made ready for the next call.

The *call by call* call flow works as follows:

1. At login, the agent specifies an assigned extension for a CTI port.
2. A customer call arrives in the system and, through normal Unified ICM configuration and scripting, is queued for a skill group or an agent. (This is no different than existing processing for local agents.)
3. The system assigns an agent to the call. If the agent's Desk Setting is Unified Mobile Agent-enabled and configured for either call by call or Agent chooses mode, the router uses the extension of the agent's CTI port as a label.
4. The incoming call rings at the agent's CTI port. The JTAPI Gateway and PIM notice this but do not answer the call.
5. A call to the agent is initiated on another CTI port chosen from a preconfigured pool. If this call fails, Redirect on No Answer processing is initiated.

**Note** In call by call mode, the Answer Wait Time is 3 to 15 seconds longer than in a local agent inbound call scenario. Specify a Redirect on No Answer setting large enough to accommodate the extra processing time.

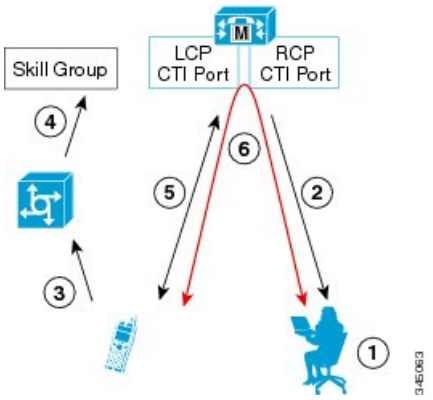
6. When the agent takes the remote phone off-hook to answer the call, the system directs the customer call to the agent's call media address and the agent's call to the customer's call media address.
7. When the call ends, both connections are terminated and the agent is ready to accept another call.

**Note** In call by call delivery mode, callers often perceive a longer ring time compared to nailed connection delivery mode. This is because callers hear the ringtone during the call flow; ringing stops only after the agent answers. From the Unified CCE reporting perspective, a Mobile Agent in call by call delivery mode has a longer Answer Wait Time for the same reason.

### *Nailed Connections*

In *nailed connection* delivery mode, the agent is called once, at login, and the phone line remains connected through multiple customer calls. See the following figure.

***Figure 35: Nailed Connection Call Flow***




The nailed connection call flow works as follows:

1. At login, the agent enters the directory number of the local CTI port (LCP) in the Instrument Number field and the remote phone number in CTI OS Desktop. The remote phone number can be any phone number reachable by Unified CM.

   When the agent clicks the Login button, a call is initiated to the agent's remote CTI port (RCP) and the agent's remote phone rings.
2. When the agent answers the call, the call is then nailed up. This means that the agent will remain on this call until the agent logs out or hangs up.
3. A customer's call arrives in the system , and scripting, is queued for a skill group/precision queue. (This is no different than existing processing for local agents.)
4. When the agent clicks the Answer button, the voice path between the agent and the customer phone is established, and the two parties can talk.
5. When the system assigns an agent to the call, the call is routed to the agent's LCP port. The agent then hears the connect tone on the headset.
6. When the call ends, the customer connection is terminated and the agent state returns to Ready.

## Feature Requirements

### Phone Requirements

A Unified Mobile Agent can use an analog, digital, or IP phone to handle calls.

**Note** When Unified Mobile Agent phones are located on a cluster and a SIP Trunk is used to connect the cluster to another cluster, you must either use SIP phones as Mobile Agent phones or select mtp required on to allow Mobile Agent calls to work.

### Conference Requirements

To use Agent Greeting for Mobile Agents, you must configure external conference-bridge (hardware) resources. To estimate the number of required resources, you can use the following formula:

Number of conference bridge resources = Mobile Agent call rate × Average greeting time (in seconds)

### CTI Port Requirements

You need two CTI ports (local and remote) for every logged-in Mobile Agent.

Unified Mobile Agent uses Unified CM CTI Port as a proxy for the agent's phone. When this proxy is set up, whenever a Mobile Agent is selected to handle a customer call, the following happens:

- The call is directed to the CTI port extension
- Unified CCE intercepts the call arriving on the CTI Port and directs Unified CM to connect the call to the Mobile Agent

For Unified Mobile Agent to work properly, you must configure two CTI ports:

- One port to serve as the agent's virtual extension
- The other port to initiate calls to the agent

## Unsupported Features

The following is a list of unsupported features for Mobile Agent:

- Web Callback
- Unified CM-based Silent Monitoring

# Outbound Dialer Considerations



## Dialing Modes

Outbound Option supports various dialing modes, described in the following sections.

**Note** All dialing modes reserve an agent at the beginning of every outbound call cycle by sending a reservation call to the agent.

### Predictive Dialing

In predictive dialing, the dialer determines the number of customers to dial per agent based on the abandon rate. The agent must take the call if that agent is logged into a campaign skill group.

A Predictive Dialer is designed to increase the resource utilization in a call center. It is designed to dial several customers per agent. After reaching a live contact, the Predictive Dialer transfers the customer to a live agent along with a screen pop to the agent's desktop. The Predictive Dialer determines the number of lines to dial per available agent based on the target abandoned percentage.

Outbound Option predictive dialing works by keeping outbound dialing at a level where the abandon rate is below the maximum allowed abandon rate. Each campaign is configured with a maximum allowed abandon rate. In Predictive mode, the dialer continuously increments the number of lines it dials per agent until the abandon rate approaches the pre-configured maximum abandon rate. At this point, the dialer begins lowering the lines per agent until the abandon rate goes below the pre-configured maximum. In this way, the dialer stays just below the pre-configured maximum abandon rate. Under ideal circumstances, the dialer internally targets an abandon rate of 85% of the pre-configured maximum abandon rate. Due to the random nature of outbound dialing, the actual attainable abandon rate at any point in time may vary for your dialer.

### Preview Dialing

Preview dialing reserves an agent prior to initiating an outbound call and presents the agent with a popup window. The agent may then Accept, Skip, or Reject the call with the following results:

- **Accept** - The customer is dialed and transferred to the agent.
- **Skip** - The agent is presented with another customer call.
- **Skips-Close** - The customer will not be called again, and the agent is presented with another customer call.
- **Reject** - The agent is released. At this point, the system delivers another call to the agent, either another preview outbound call, or a new inbound call..
- **Rejects-Close** - The agent is released and the record is closed so it is not called again. At this point, the system delivers another call to the agent, either another Preview outbound call or a new inbound call.

### Direct Preview Dialing

The Direct Preview mode is similar to the Preview mode, except that the call is automatically placed by the dialer from the agent's phone after the agent accepts. Because the call is initiated from the agent's phone, the agent hears the ringing, and there is no delay when the customer answers. However, in this mode, the agent must deal with answering machines and other results that the Dialer Call Progress Analysis (CPA) normally handles for other campaign dialing modes.

**Note**

- The CPA and the transfer to IVR features are not available while using Direct Preview Dialing mode
- A zip tone is a tone that announces incoming calls. There is no zip tone in Direct Preview mode

### Progressive Dialing

Progressive Dialing is similar to predictive dialing (see Predictive Dialing, on page 113). The only difference is that in Progressive Dialing mode, Outbound Option does not calculate the number of lines to dial per agent, but allows users to configure a fixed number of lines that will always be dialed per available agent.

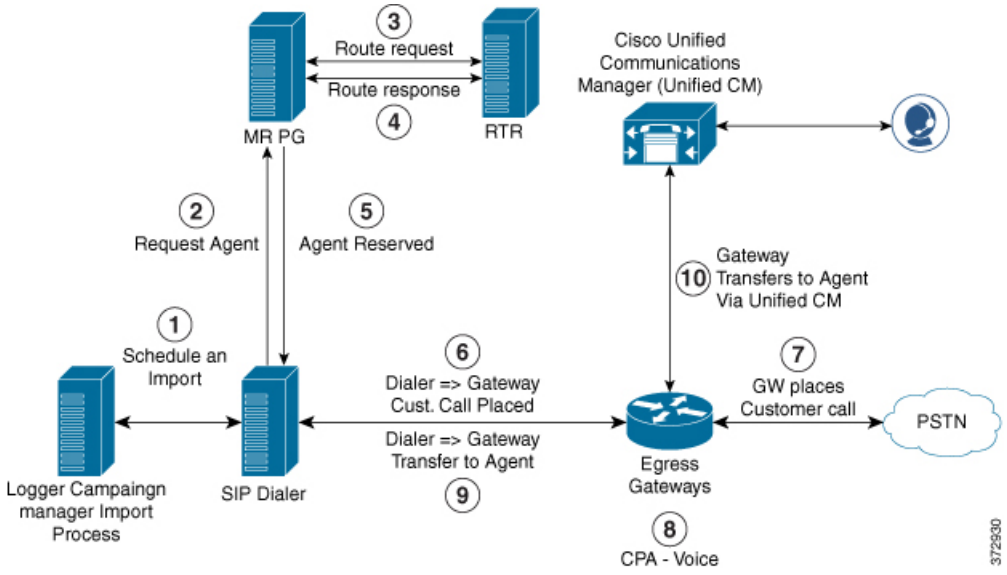
# Outbound SIP Dialer Call-flow

The following sections provide diagrams that describe the outbound SIP dialer call flow. The first describes a call flow for a SIP dialer agent campaign. The second describes a call flow for an unattended IVR campaign.

## Call Flow Diagram for Agent Campaign

The following figure illustrates a transfer to agent call flow in an Outbound Option deployment with a SIP dialer.

***Figure 36: SIP Dialer Agent Campaign Call Flow***



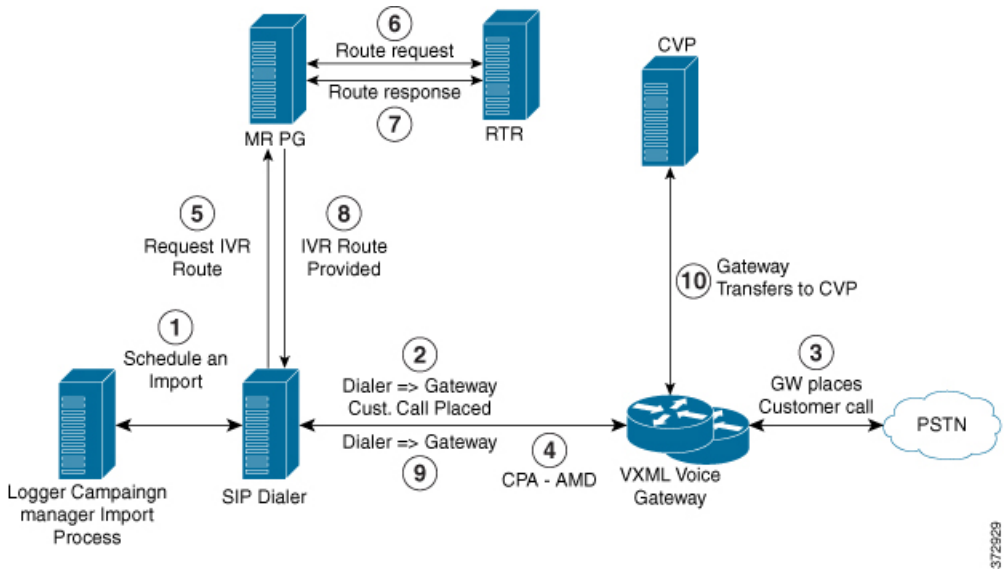

The following steps describe this call flow in detail:

1. The import is scheduled and the campaign starts. The records are delivered to the dialer.
2. The dialer looks for an available agent through the media routing interface.
3. The media routing peripheral gateway (MR PG) forwards the request to the router.
4. The routing script identifies an agent and responds to the MR PG.
5. The media routing peripheral interface manager (PIM) notifies the dialer that the agent is available.
6. The dialer signals the gateway to place a call to the customer.
7. The gateway places a call to the customer, and the dialer is notified of the attempted call.
8. Call Progress Analysis (CPA) is done at the gateway. When voice is detected, the dialer is notified.
9. The dialer asks the voice gateway to transfer the call to the reserved agent by its agent extension.
10. The gateway directs the call to the agent through Unified Communications Manager (using dial peer configuration to locate the Unified Communications Manager). Media are set up between the gateway and the agent's phone.

### Call Flow Diagram for IVR campaign

The following figure illustrates a transfer-to-IVR call flow in an Outbound Option deployment with a SIP dialer.

*Figure 37: SIP Dialer Unattended IVR Campaign Call Flow*




The following steps describe this call flow in detail:

1. An unattended IVR campaign starts, scheduling an import. Customer records are delivered to the dialer.
2. The dialer sends a SIP INVITE to the voice gateway to start a call to a customer.
3. The gateway places the customer call.
4. The voice gateway does Call Progress Analysis (CPA) and detects an answering machine (AMD). The dialer is notified.
5. The dialer sends an IVR route request to the MR PG.
6. The MR PG forwards the route request to the router and the routing script is invoked.
7. The router sends the route response with the network VRU label to the MR PG.
8. The MR PG forwards the route response to the dialer.
9. The dialer sends a SIP REFER request for the label to the voice gateway.
10. The voice gateway transfers the call to Unified CVP. At this point, Unified CVP takes control of the call.

# Post Call Survey Considerations

Observe the following conditions when designing the Post Call Survey feature:

- A Post Call Survey is triggered by the hang-up event from the last agent. When the agent hangs up, the call routing script launches a survey script.
- The mapping of a dialed number pattern to a Post Call Survey number enables the Post Call Survey feature for the call
- The value of the expanded call variable user.microapp.isPostCallSurvey controls whether the call is transferred to the Post Call Survey number

- If user.microapp.isPostCallSurvey is set to **y** (the implied default), the call is transferred to the mapped post call survey number
- If user.microapp.isPostCallSurvey is set to **n**, the call ends
- To route all calls in the dialed number pattern to the survey, your script does not have to set the user.microapp.isPostCallSurvey variable. The variable is set to y by default
- To test for conditions and dynamically route calls to the survey based on the results of the test, your script must explicitly set user.microapp.isPostCallSurvey to y and n as appropriate
- REFER call flows are not supported with Post Call Survey. (The two features conflict: REFER call flows remove Unified CVP from the call; Post Call Survey needs Unified CVP because the agent has already disconnected.)
- For Unified CCE reporting purposes, when a survey is initiated, the call context of the customer call that was just transferred to the agent is replicated into the call context of the Post Call Survey call

# a-Law Codec Support Considerations

HCS for Contact Center supports G.711 a-law codec. This means that the SIP carrier sends the capability as G.711 a-law and G.729. The prompts at the VXML gateway should be G.711 a-law and the agents need to support both G.711 a-law and G.729. a-law supports the following features for Cisco HCS:

- Agent Greeting
- Whisper Announcement
- Call Manager Based Silent Monitoring
- Outbound (SIP Dialer)
- Courtesy Callback
- Post Call Survey
- Mobile Agents

**Note** SIP Dialers with Cisco UBE can support A-Law with specific design considerations. The SIP Dialer does not advertise A-Law. So, the deployment needs DSP resources (Transcoder) on Cisco UBE during the initial negotiation (no media) between the SIP Dialer and the SIP service provider. During a REFER from the Dialer to the agent, Cisco UBE renegotiates the code with the agent to use A-Law. Cisco UBE can then release the DSP resource (Transcoder).

For information on the core component configurations for a-law codec support, see Configure a-Law Codec, on page 642.

# Back-Office Phone Support Considerations

Following are the considerations for the back-office phone support on the same Unified CM for HCS for Contact Center:

- You must meet the minimum OVA requirements of Unified CM for all agent deployment as described in Open Virtualization Format Files, on page 54
- If you are replacing the Contact Center agent phone already pre-sized in the OVA defined in Configuration Limits, on page 82 with the regular back-office phone. This does not require the re-sizing of the OVA.
- If you plan to use the Unified CM for all the agents and additional back-office phones or want to increase the OVA size, you must follow the guidelines for Specification-Based Hardware Support, on page 48 and do appropriate sizing.

## Finesse IP Phone Agent Considerations

Finesse IPPA supports fewer features than the Finesse desktop in the browser, but it does allow agents and supervisors to receive and manage calls if they lose or do not have access to a desktop. For more information about installation, configuration and administration of FIPPA, see http://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html.

## Live Data Reporting System Considerations

Live Data server components cannot be installed in HCS-CC deployments with more than 12 agent peripheral gateways, for Unified CM or Avaya (Definity).

## Precision Routing Considerations

Precision queues cannot be configured on HCS-CC deployment models with more than 12 agent peripheral gateways, for Unified CM or Avaya (Definity).

# Optional Component Considerations

This section describes the capabilities of the following Cisco Optional Components:

- Cisco MediaSense Capabilities, on page 151
- Unified WIM and EIM Considerations, on page 139
- Cisco RSM Considerations, on page 147
- Cisco MediaSense Considerations, on page 150
- Cisco Unified SIP Proxy Considerations, on page 152
- Cisco SPAN based Monitoring Considerations, on page 153
- Avaya PG Considerations , on page 153
- Cisco Virtualized Voice Browser Considerations, on page 154

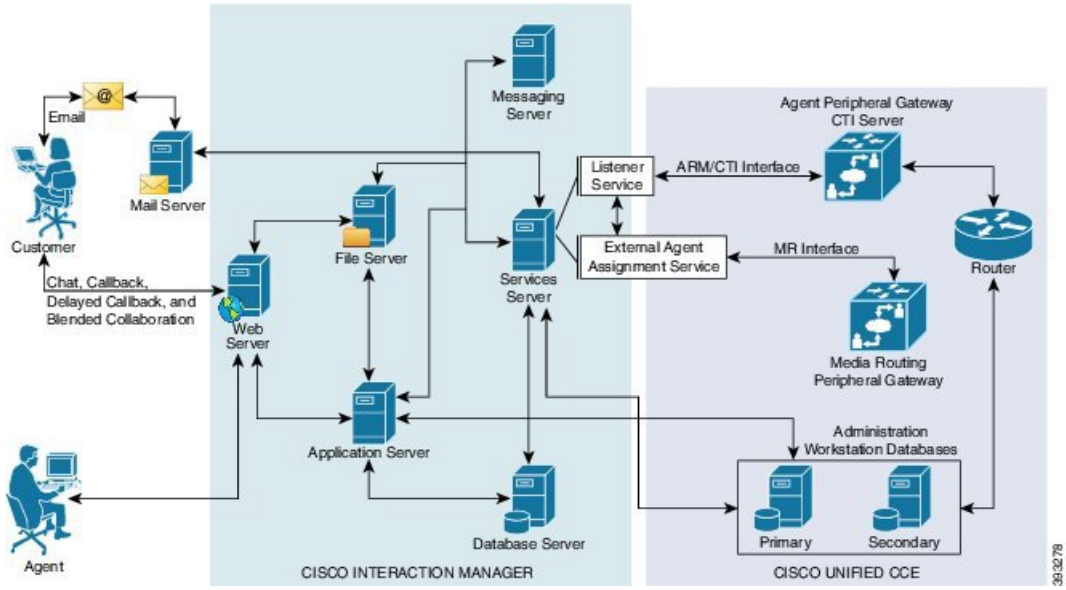
# Unified WIM and EIM Considerations

This section describes the following considerations for Unified WIM and EIM.



## Unified WIM and EIM Design Considerations

***Figure 38: Unified WIM and EIM Design Considerations***



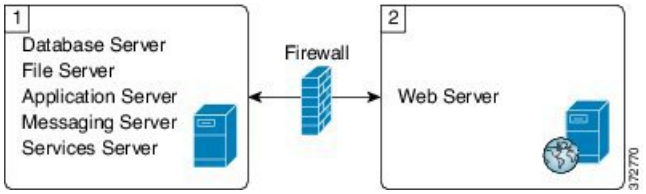

## Unified WIM and EIM Deployment Options

Due to the modular, component-based nature of the architecture, Cisco WIM and EIM has the ability to cater to the growing demands for concurrent user loads. To provide the flexibility to suit deployments of varied sizes, Cisco WIM and EIM supports various components that may be distributed across various servers in a deployment.

### Collocated Deployment

In Collocated deployment option, the web server is installed on a separate machine and all other components are installed on one machine. The web server may be installed outside the firewall, if required.

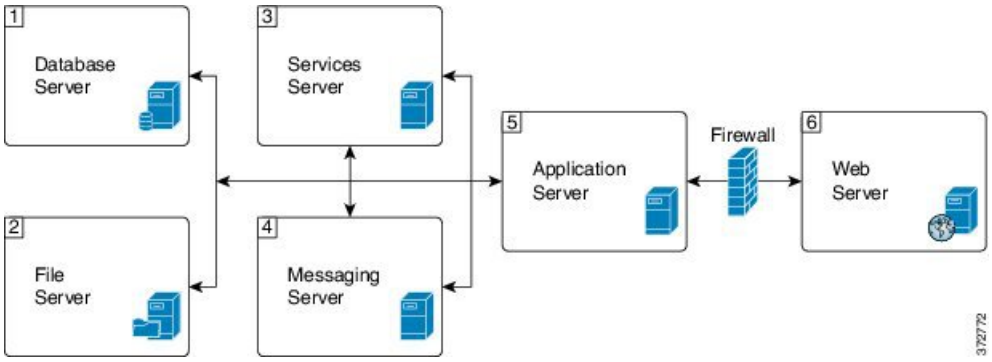
***Figure 39: Collocated Deployment***




### Distributed-Server Deployment

In this configuration, each component is on a separate machine, with the web server installed outside the firewall. The application, messaging, services, and web servers in this configuration can be restarted without restarting any other servers.

***Figure 40: Distributed-Server Deployment***



# Unified WIM and EIM Configuration Limits

## Unified WIM and EIM Configuration Limits

*Table 27: Unified WIM and EIM Configuration Limits*

| Group | Resource | 120 Multimedia Agent Deployment (One PG) | 240 Multimedia Agent Deployment (One PG) | 1250 Multimedia Agent Deployment (Two PGs) |
|---|---|---|---|---|
| Multimedia | Agents (any combination of Email, Chat and Web callback activities) | 120 | 240 | 1250 # |
| | Maximum Number of Emails per agent per hour | 12 | 12 | 5 |
| | Maximum Number of chats per agent per hour | 12 | 12 | 5 |
| | Maximum Number of Web Callback per agents per hour | 12 | 12 | 12 |

*Table 28: Unified WIM and EIM Configuration Limits*

| Group | Resource | Unified WIM and EIM Distributed server Deployment | Unified WIM and EIM Collocated Deployment |
|---|---|---|---|
| Multimedia | Agents (any combination of Email, Chat and Web callback activities) | 1250 # | 200 ## |
| | Maximum Number of Emails per agent per hour | 5 | 12 |
| | Maximum Number of chats per agent per hour | 5 | 10 |
| | Maximum Number of Web Callback per agents per hour | 5 | 5 |

**Note** The Symbol "#" indicates that the Unified WIM and EIM Distributed server Deployment allows combination of maximum 600 concurrent Web Callback and for the remaining it allows any combination of Email or Chat activities. The Symbol "##" indicates that the Unified WIM and EIM Collocated Deployment allows combination of maximum 100 concurrent Web Callback and for the remaining it allows any combination of Email or Chat activities.

# HCS Support Matrix for Unified WIM and EIM

### HCS Support Matrix for Unified WIM and EIM

***Table 29: HCS Support Matrix for Unified WIM and EIM***

| HCS for CC Deployment | 120 Multimedia Deployment | 240 Multimedia Deployment | 1250 Multimedia Deployment |
|---|---|---|---|
| HCS for CC 500 Agent Deployment | Yes | Yes | Support can't exceed 500 Multimedia agents |
| HCS for CC 1000 Agent Deployment | Yes | Yes | Support can't exceed 1000 Multimedia agents |
| HCS for CC 4000 Agent Deployment | Yes | Yes | YES |

***Table 30: HCS Support Matrix for Unified WIM and EIM***

| HCS for CC Deployment | Unified WIM and EIM Distributed server Deployment | Unified WIM and EIM Collocated Deployment |
|---|---|---|
| HCS for CC 500 Agent Deployment | Support can't exceed 500 Multimedia agents | Yes |
| HCS for CC 1000 Agent Deployment | Support can't exceed 1000 Multimedia agents | Yes |
| HCS for CC 4000 Agent Deployment | Yes | Yes |
| HCS for CC 12000 Agent Deployment | Yes | Yes |
| HCS for CC Small Contact Center Agent Deployment | No | Yes |

## Unified WIM and EIM High Availability

The following table contains the Cisco Unified WIM and EIM high availability during the failover of Unified CCE processes.

| Component | Failover scenario | New session (Web Callback/ Delayed callback/ Chat/ Email) impact | Active session (Web Callback/ Delayed callback/ Chat/ Email) impact | Post recovery action |
|---|---|---|---|---|
| PG | Unified Communications Manager PG Failover | Web Callback - The new call is lost, because there is no Longest Available agent during the failure of PG.<br>Delayed Callback - The new call reaches the customer and the agent after the PG on the other side becomes active and the delay that the customer specifies gets complete.<br>Chat - The new chat initiated by the customer reaches the agent after the other side of the PG becomes active.<br>Email - The new Email sent by the customer reaches the agent. | Active Web Callback, Delayed callback, Chat, and Email sessions continue uninterrupted. | Agent receives the Call, Chat or Email after the PG becomes active and the agent logins again. |

| Component | Failover scenario | New session (Web Callback/ Delayed callback/ Chat/ Email) impact | Active session (Web Callback/ Delayed callback/ Chat/ Email) impact | Post recovery action |
|---|---|---|---|---|
| PG | MR PG Failover | Web Callback - The new call is established between the customer and the agent after the PG becomes active.<br>Delayed Callback - The new call reaches the customer and the agent after the PG on the other side becomes active and the delay that the customer specifies gets complete.<br>Chat - The new chat initiated by the customer reaches the agent once the other side of the PG becomes active.<br>Email - The new Email sent by the customer reaches the agent. | Active Web Callback, Delayed callback, Chat, and Email sessions continue uninterrupted. | Agent receives the Call, Chat or Email once the PG becomes active. |

| Component | Failover scenario | New session (Web Callback/ Delayed callback/ Chat/ Email) impact | Active session (Web Callback/ Delayed callback/ Chat/ Email) impact | Post recovery action |
|---|---|---|---|---|
| CG | CTI Failover | Web Callback -The new call cannot be placed and the customer receives the message, "System cannot assign an Agent to the request."<br>Delayed Callback - The new call reaches the customer and the agent after the CG on the other side becomes active and the delay that the customer specifies gets complete.<br>Chat - The new chat initiated by the customer reaches the agent after the other side of the CG process becomes active.<br>Email - The new Email sent by the customer reaches the agent. | Active Web Callback, Delayed callback, Chat, and Email sessions continue uninterrupted. | Agent receives the Call, Chat or Email once the process becomes active. |

| Component | Failover scenario | New session (Web Callback/ Delayed callback/ Chat/ Email) impact | Active session (Web Callback/ Delayed callback/ Chat/ Email) impact | Post recovery action |
|---|---|---|---|---|
| CTI OS | CTI OS Server Failure | Web Callback - The new call is established without any impact.<br>Delayed Callback - The new call is established without any impact after the delay that the customer specifies gets complete.<br>Chat - The new chat reaches the agent without any impact.<br>Email - The new Email sent by the customer reaches the agent. | Active Web Callback, Delayed callback, Chat, and Email sessions continue uninterrupted. | Seamless. |
| Router | Router fails | Web Callback - The new call is established through other side of the router process.<br>Delayed Callback - The new call is established through other side of the router process and once the delay mentioned by the customer completes.<br>Chat - The new chat reaches the agent through other side of the router process.<br>Email - The new Email sent by the customer reaches the agent through other side of the router process. | Active Web Callback, Delayed callback, Chat and Email sessions continue uninterrupted. | Agent gets the Call, Chat or Email with other side of the router process. |

## Cisco WIM and EIM Bandwidth, Latency and QOS Considerations

The minimum required network bandwidth for an agent connecting to the Cisco Interaction Manager servers on login is 384 kilobits/second or greater. After login in a steady state an average bandwidth of 40 kilobits/second or greater is required.

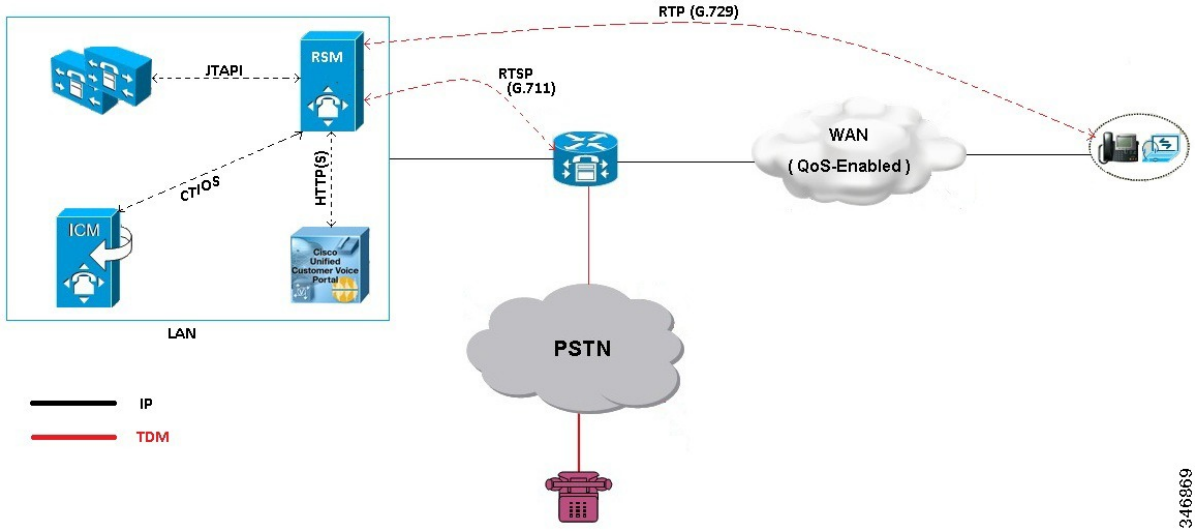
An attachment of size up to 50 KB is supported within this required bandwidth. For attachments of size greater than 50 KB, you may experience slow speed temporarily in the agent user interface during download of the attachments.

# Cisco RSM Considerations



## Cisco RSM Design Considerations

***Figure 41: Cisco RSM Design Considerations***




## Cisco RSM High Availability

The following table shows the Cisco RSM High Availability.

*Table 31: Cisco RSM High Availability*

| Component | Failover/Failure Scenario | New Call Impact | Active Call Impact | Post-recovery Action |
|---|---|---|---|---|
| RSM Server | RSM server (hardware) fails | Attempts to contact the RSM server fail | Active monitoring sessions terminate and supervisor is directed to the main menu | Supervisor can monitor calls after the RSM server becomes active |
| CTI OS Server | CTI OS Server Failure | Supervisor can monitor new calls without any failure | Active monitoring sessions will continue normally | Failover is seamless |
| CTI | Active CTI Gateway process fails | Supervisor can establish new monitoring sessions until the secondary CTI process becomes active | Active monitoring sessions continue normally | After the CTI Gateway becomes active the supervisor can establish new monitoring sessions |
| VLEngine | VLEngine fails | Supervisor can establish new monitoring sessions when VLEngine becomes active | Active monitoring sessions terminate and supervisor is directed to the main menu | After the VLEngine becomes active the supervisor can establish new monitoring sessions |
| PhoneSim | PhoneSim fails | Supervisor can monitor new calls when PhoneSim becomes active | Active monitoring sessions continue normally | After the PhoneSim becomes active the supervisor can establish new monitoring sessions |
| Unified CM | Active Subscriber fails | New calls cannot be established until the secondary subscriber becomes active | Active monitoring sessions continue normally | After the secondary subscriber becomes active the supervisor can establish new monitoring sessions |
| JTAPI | JTAPI gateway fails | Supervisor can establish new calls without any failure | Active monitoring sessions continue normally | Failover is seamless |
| Unified CVP | Active CVP fails | New calls cannot be established until the Unified CVP becomes active | Active monitoring sessions terminate | After the Unified CVP becomes active the supervisor can establish new monitoring sessions |

## Cisco RSM Capabilities

| Platform | Capabilities |
|---|---|
| Call Flow | The Supervisor can only monitor agents who are in talking state. |
| Desktop | CTIOS |
| Voice Codec | Between Agent and RSM: G.729 (RTP)<br>Between RSM and VXML Gateway: G.711 (RTSP) |
| Concurrent Monitoring Sessions | 120 |
| Monitored Calls (per minute) | 17 |
| Maximum Configured Agents per PG | 12000 |
| SimPhone Start line Number Range | Four to fifteen digits |

## Cisco RSM Bandwidth, Latency and QOS Considerations

| RSM Peer | Purpose | Protocols Used | Data Format | Relative Bandwidth Requirements | Link Latency Requirements |
|---|---|---|---|---|---|
| VRU | Service Requests and Responses | TCP (HTTP) | Textual | Minimal | < 500 ms avg. |
| VRU | Requested Voice Data from PhoneSim to VRU | TCP (HTTP) | G711, chunked transfer mode encoding | High (about 67 to 87 kbps per session) | < 400 ms avg. |
| Unified CM | Issuance of Agent Phone Monitoring | TCP (JTAPI) | Binary (JTAPI stream) | Minimal | < 300 ms avg. |
| CTI OS Server (PG) | Environment Events and Supervisor Logins | TCP (CTI OS) | Binary (CTI OS stream) | Minimal | < 300 ms avg. |
| Agent Phones | Simulated Phone Signaling | TCP or UDP (SIP) | Textual | Minimal | < 400 ms avg. |

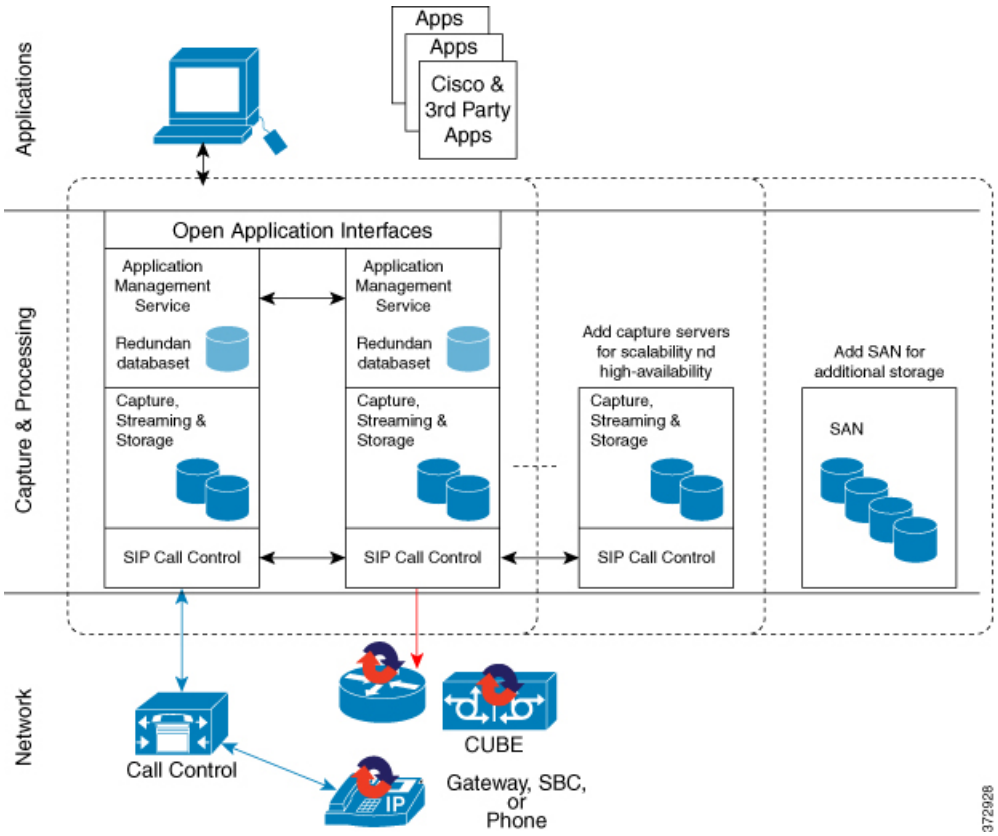
| RSM Peer | Purpose | Protocols Used | Data Format | Relative Bandwidth Requirements | Link Latency Requirements |
|---|---|---|---|---|---|
| Agent Phones | Monitored Phone Voice Data | UDP (RTP) | Binary (G.711) | High (about 67 to 87 kbps per session) | < 400 ms avg |

# Cisco MediaSense Considerations



## Cisco MediaSense Design Considerations

*Figure 42: Cisco MediaSense Design Considerations*



## Cisco MediaSense Capabilities

| Platform | Capabilities |
|---|---|
| Phone | All HCS supported Phone. See list of supported phones in Voice Infrastructure, on page 75 section. |
| Supported Model | 2vCPU, 4vCPU and 7vCPU profiles. |
| Voice Codec | G.711 and G.729 |
| Session | See session related details in http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_MediaSense#Version_10.x. |
| Media Forking | CUBE, Phone and TDM |
| Network | Inter cluster communication over WAN is not supported. |

## Cisco MediaSense High Availability

| Component | Failover/Failure Scenario | New Call Impact | Active Call Impact | Postrecovery Action |
|---|---|---|---|---|
| Recording Sever | Primary Recording Sever is down | Distributes the incoming load across the remaining severs. | Unified CM sets a time limit beyond which, if the recording hasn't begun, it will stop trying, and Active calls will not get recorded till CM established the connection with Recording server. | Call will get recorded on failed recording sever once it becomes active. |
| | Secondary Recording Server | No Impact | No Impact | No Impact |
| Database | Either Primary or Secondary server goes down | No Impact | No Impact | Data Replication begins automatically. |

## Cisco MediaSense Bandwidth, Latency and QOS Considerations

MediaSense requires gigabit LAN connectivity with 2ms or less between servers within a cluster.

# Cisco Unified SIP Proxy Considerations

- Consists of 2 gateways for redundancy, geographically separated, 1 proxy module each, using SRV priority for redundancy of proxies, no HSRP
- CUSP can co-reside with VXML or TDM gateways. In earlier versions of Unified CVP due to platform validation restriction co-residency was not supported, and a dedicated ISR was required for proxy functionalities
- TDM gateways are configured with SRV or with Dial Peer Preferences to use the primary and secondary CUSP proxies
- CUSP is set with Server Groups to find primary and back up Unified CVP, Unified CM and VXML gateways
- Unified CVP is set up with Server Group to use the primary and secondary CUSP proxies
- Cisco Unified CM is set up with a Route Group with multiple SIP Trunks, to use the primary and secondary CUSP proxies

## Performance Matrix for CUSP Deployment

CUSP baseline tests were done in isolation on the proxy, and capacity numbers (450 TCP transactions per second) should be used as the highest benchmark, and most stressed condition allowable. A CVP call, from the proxy server perspective, entails on average, 4 separate SIP calls:

- Caller inbound leg
- VXML outbound leg
- Ringtone outbound leg
- Agent outbound leg

When a consult with CVP queuing occurs, an additional 4 SIP transactions will be incurred for the session, effectively doubling the number of calls.

**Note** Always turn the Record Route setting off on the proxy server to avoid a single point of failure and allow fault tolerance routing, as well as increase the performance of the Proxy server. Using record route setting on the proxy server doubles the impact to performance, as shown in the CUSP baseline matrix, and also breaks the high availability model since the proxy becomes a single point of failure for the call, if the proxy were to go down.

Record Route is turned off by default on CUSP.

# Cisco SPAN based Monitoring Considerations

## Silent Monitoring Bandwidth, Latency and QOS Considerations

With Silent Monitoring supervisors can listen to the agent calls in Unified CCE call centers that use CTI OS. Voice packets sent to and received by the monitored agent's IP hardware phone are captured from the network and sent to the supervisor desktop. At the supervisor desktop, these voice packets are decoded and played on the supervisor's system sound card. Silent Monitoring of an agent consumes approximately the same network bandwidth as an additional voice call. If a single agent requires bandwidth for one voice call, then the same agent being silently monitored requires bandwidth for two concurrent voice calls. To calculate the total network bandwidth required for your call load, multiply the number of calls by the per-call bandwidth figure for your particular codec and network protocol.

# Avaya PG Considerations



## Avaya PG Design Considerations

The following table includes the deployment consideration for Avaya PG. The Avaya PG is supported only in 4000 and 12000 agent deployment models.

| Feature/Call Flow | Design Considerations |
|---|---|
| Agent Reporting | Supported |
| Duplexed PG Implementation | Supported |
| Unified ICM web Option | Supported |
| Straight Calls | Supported |
| Transfer Calls | Supported |
| Conference Calls | Supported |
| Translation Route | Supported |
| Remote Silent Monitoring (RSM) | Not Supported |
| MediaSense | Not Supported |
| Multimedia support (EIM/WIM) | Not Supported |
| Precision Queues | Not Supported |
| Finesse Desktop support | Not Supported |
| Outbound | Not Supported |

| Feature/Call Flow | Design Considerations |
|---|---|
| Split PG over WAN | Not Supported |
| Avaya ACD remote from PG | Not Supported |
| Extension Digits Supported | 10 |
| Agents per PG | 2000 |
| Maximum Skills per agent | 20 |
| Maximum UII size | 40 bytes |

### Avaya PG High Availability

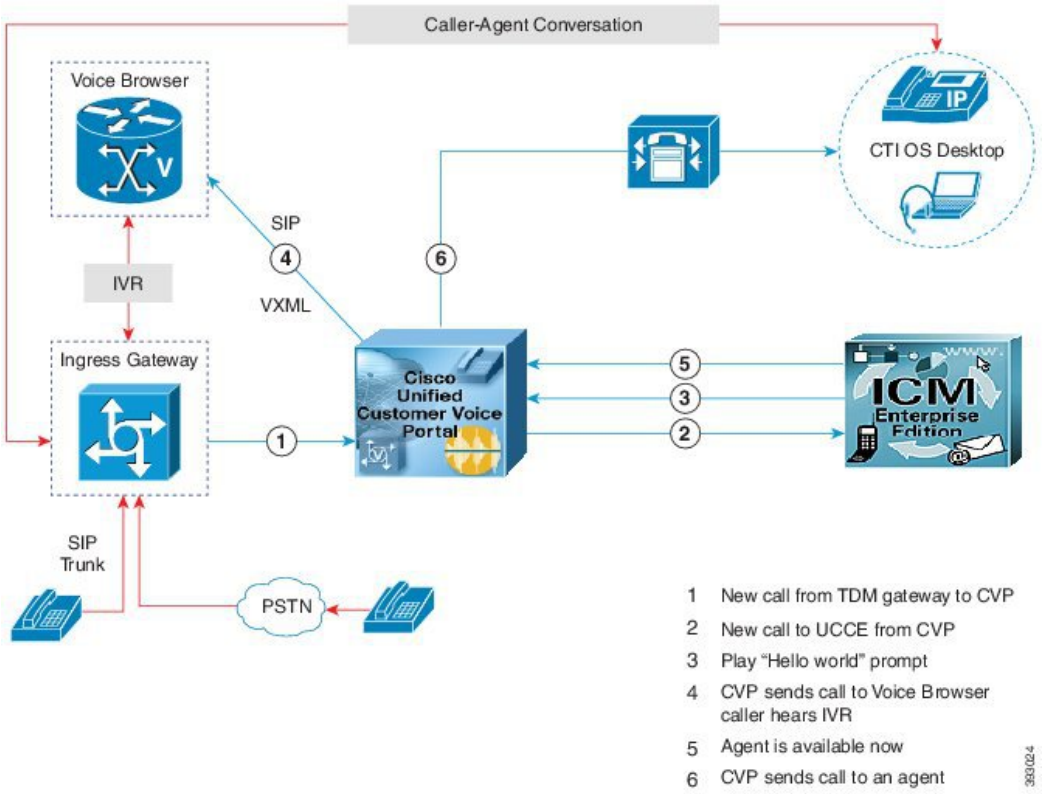
When PG(PIM) side A fails, PG(PIM) side B becomes active. Agents who are on call continues, with no third-party call control (conference, transfer, and so on) available from their agent desktop. During the failover to the B-Side PIM. Agents who are not on a call, CTI desktop disable their agent state or third-party call control buttons on the desktop. After the failover completes, the agent desktop buttons are restored. When PG side A recovers, the PIM does not fall-back, PG side B remains active and call processing continues.

## Cisco Virtualized Voice Browser Considerations


- Cisco Virtualized Voice Browser Design Considerations, on page 155
- Cisco Virtualized Voice Browser Capabilities, on page 156
- Cisco Virtualized Voice Browser High Availability, on page 156
- Cisco Virtualized Voice Browser Bandwidth, Latency and QoS Considerations, on page 156

# Cisco Virtualized Voice Browser Design Considerations

*Figure 43: Cisco Virtualized Voice Browser Design Considerations*




Virtualized VB does not depend on the number of agents. It depends on number of concurrent SIP sessions and CPS supported. Install Virtualized VB depending on the number of SIP sessions required for an HCS deployment.

| Platform/Feature | Cisco Virtualized Voice Browser Considerations |
|---|---|
| Video | Not Supported |
| MRCPv2 | Not Supported |
| Voice Codec | G711 |
| VoiceXML 2.1 | Not Supported |
| Call Flows | Standalone, Comprehensive, Blind transfer Supported |
| ASR/TTS | Supported |
| C-series Server | Supported |

| Platform/Feature | Cisco Virtualized Voice Browser Considerations |
|---|---|
| HTTPS | Supported |
| HTTP | Supported |
| **Browser** | |
| Firefox 35.0.1 or later | Supported |
| Internet Explorer 11 | Not Supported |

## Cisco Virtualized Voice Browser Capabilities

| Platform | Capabilities |
|---|---|
| Media Protocol | MRCPv1 for ASR/TTS |
| Maximum Sessions | 600 |

## Cisco Virtualized Voice Browser High Availability

| Component | Failover/Failure Scenario | New Call Impact | Active Call Impact | Post-recovery Action |
|---|---|---|---|---|
| Virtualized Voice Browser | Virtualized Voice Browser fails | CVP routes call to other Virtualized Voice Browser | Gets disconnected and data gets lost | Virtualized Voice Browser takes care of new sessions |

## Cisco Virtualized Voice Browser Bandwidth, Latency and QoS Considerations

Cisco Virtualized Voice Browser supports up to 200ms round-trip delay with CVP.

# Deployment Model Considerations

## Small Contact Center Deployment Consideration

*Table 32: Aggregation Components*

| Components | Design considerations |
|---|---|
| Unified Contact Center Domain Manager | Parameters moved to respective folders by administrator. System Configuration limits enforced at solution level, not at sub customer level.<br>Outbound configuration and administration per sub customer has to be configured by service provider.<br>Each sub customer must have AD for logging. |
| | There are three options for ISE users:<br>1 CCDM domain users<br>2 CCE domain users.<br>3 Sub Customer domain users.<br>Because of existing two-way trust between CCDM and CCE domain, either first or second option is recommended.<br>If service provider and sub customer security permits the two-way trust between CCE and customer domain, third option is recommended. Third option is not supported with one-way trust.<br>For creating a customer domain user, see Create User, on page 504. |
| Cisco Unified Communications Domain Manager | In **Network** > **Contact Center Server** add a dummy CVP Server for each sub customer. Associate the same CVP server in the sub customer hardware group. |
| | Agent Extension across sub customer must be unique. overlapping of agent extension/dial plan is not supported. Example: If sub_cust1 uses 801xxxxxx extension, sub_cust2 cannot use the same extension. |
| | Each sub customer must have unique internal help desk number. |
| Perimeta SBC | Sip signaling and media passes through Perimeta SBC. Data traffic passes through ASA. |

| Components | Design considerations |
|---|---|
| ASA/NAT | Data traffic passes only through ASA.<br>ASA is required for shared and sub customers. Do not enable SIP ALG in ASA. |
| Cisco Prime Collaboration | Static mapping of internal IP to an external IP is required for Prime to work with SCC. |

***Table 33: Shared Components***

| Components | Design considerations |
|---|---|
| Unified CCE Router | Congestion Control Configuration, on page 186 |
| Logger | System Configuration limits enforced at solution level, not at sub customer level. See Configuration Limits, on page 82. |
| AW-HDS-DDS | See Set the HCS Deployment Type, on page 346, deployment for small contact center is similar to HCS-CC 4000 agent deployment. You can deploy Small contact center deployment only on 4000 agent deployment. |
| VRU Peripheral Gateways | |
| Unified CVP Call Server | Dial number patterns across sub customer needs to be unique. Example: If sub_cust1 uses 801xxxxxx dial number pattern, sub_cust2 cannot use the same dial number pattern. |
| CVP Reporting Server | Use Exony VIM for multi tenant reporting. |
| Cisco Unified IC | CUIC is used for simple collections using the department ID of UCCE. See Configure Unified Intelligence Center Reporting, on page 382. You can also use Exony VIM for multi-tenant reporting. |
| CUBE- Enterprise | CUBE Enterprise Considerations. See CUBE-Enterprise at Customer Premise, on page 164 |

***Table 34: Dedicated Sub-customer Components***

| Components | Design Considerations |
|---|---|
| Cisco Unified CM | CUCM software resource is recommended. You can also use dedicated DSP resources for each sub-customer. |

| Components | Design Considerations |
|---|---|
| Peripheral Gateways | Follow any of the below domain consideration to configure peripheral gateway:<br>• PG can install on sub customer domain. Both sub customer domain and service provider (UCCE) domain instance number and name should be same.<br>• Configure static NAT between UCCE domain and PG machine that is installed on service provider (UCCE) domain.<br>Maximum number of PG's Peripheral Gateways, on page 70. |
| Cisco Finesse | Each sub customer should have local DNS. See Create DNS Server for Finesse in Small Contact Center Deployment, on page 436 |

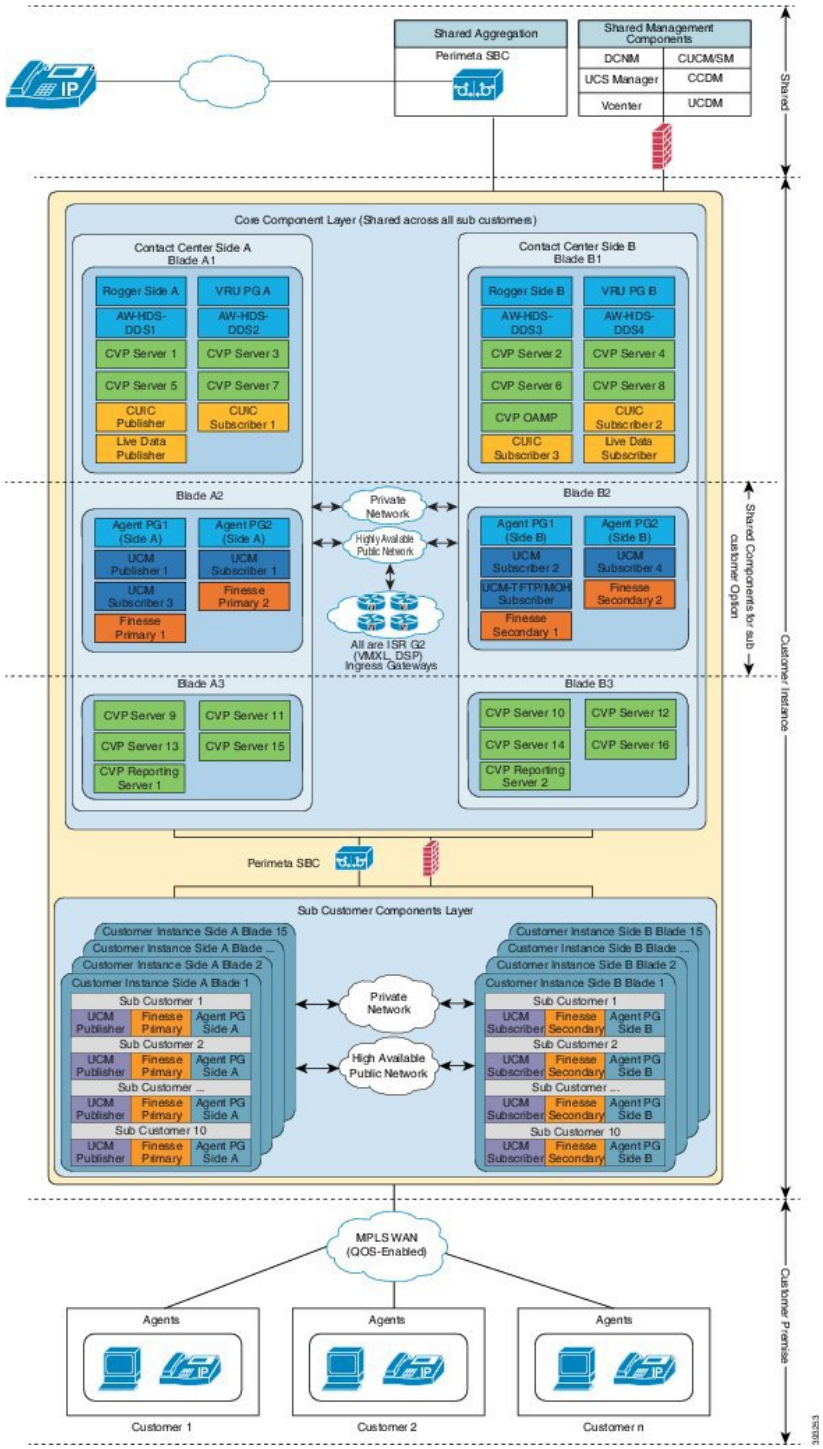
***Table 35: Optional Components***

| Components | Design considerations |
|---|---|
| Cisco Unified WIM and EIM | A single Cisco Unified WIM and EIM instance per sub customer is supported, not exceeding 74 sub customers.<br>**Note** Shared Sub Customer Components option is not supported. |
| Cisco RSM | A single RSM server is supported per sub customer. RTSP flow between RSM and CUBE gateway is via ASA.<br>**Note** Shared Sub Customer Components option is not supported. |
| Cisco MediaSense | A single MediaSense server is supported per sub customer CUCM controlled CUBE Forking not supported, only cube level recording supported for mobile agents. |
| | Media class should not be enabled on the common outbound dial-peer. Inbound Dial-peer has to be created for each sub customer and Media class should be enabled.<br>**Note** Shared Sub Customer Components option is not supported. |
| SPAN Based Monitoring | Span from CUCM is supported for Mobile Agents. See Configurations for SPAN from Call Manager, on page 653. |

*Table 36: Core Features*

| Components | Design considerations |
|---|---|
| Agent Greeting | |
| Whisper Announcement | |
| Courtesy Call Back | |
| Outbound Dialer | Maximum of 32 Dialers are supported and Maximum 4000 ports are supported.<br>**Note** There is no solution for sub customers to manage outbound campaigns. You must provide services or custom solutions to manage outbound campaigns for each sub customer. |
| Mobile Agents | |
| A-law & u-law support | |
| Post Call Survey | |
| Database Integration | ICM DB lookup is not supported. See Configure Database Integration, on page 614. |
| Local Trunk PSTN Local Breakout | . |
| Local Trunk Location based CAC | Not supported for dedicated components sub-customer option. |
| CM based Silent Monitoring | |

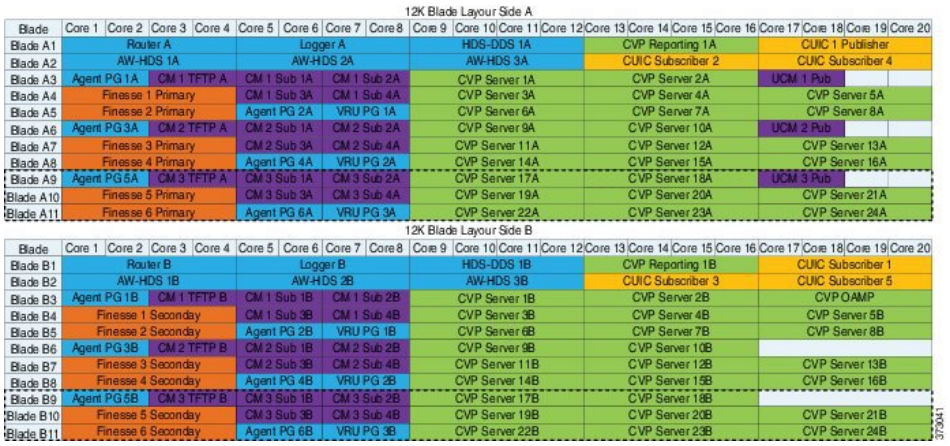
*Figure 44: Cisco HCS Small Contact Center Deployment Topology*



# 12000 Agent Deployment Model Considerations

| Components | Design Considerations |
|---|---|
| CUIC | A maximum of 6 CUIC nodes are supported(3 nodes on each side) accommodating 1200 Reporting users, if one of the side completely fails then only 3 CUIC nodes will be available supporting up to 600 reporting users. |
| AW-HDS | A maximum of 6 AW-HDS nodes are supported(3 nodes on each side) accommodating 1200 Reporting users, if one of the side completely fails then only 3 AW-HDS nodes will be available which can support up to 600 reporting users. |
| CVP | A maximum of 10000 IVR calls is supported by the system. See License Considerations. |
| vCPU Oversubscription | The oversubscription on vCPU's is not supported. |

***Figure 45: 12000 Agent Deployment Model***




# Remote Deployment Option Considerations

## Global Deployment Considerations

- The maximum Round Trip Time (RTT) between the core data center and Remote data center is restricted up to 400 milli seconds.
- The maximum Round Trip Time (RTT) between the Data center components and customer premise is restricted up to 200 milli seconds.
- The maximum Round Trip Time (RTT) between the Side A Data center components and Side B Data center is restricted up to 80 milli seconds.

**Note**

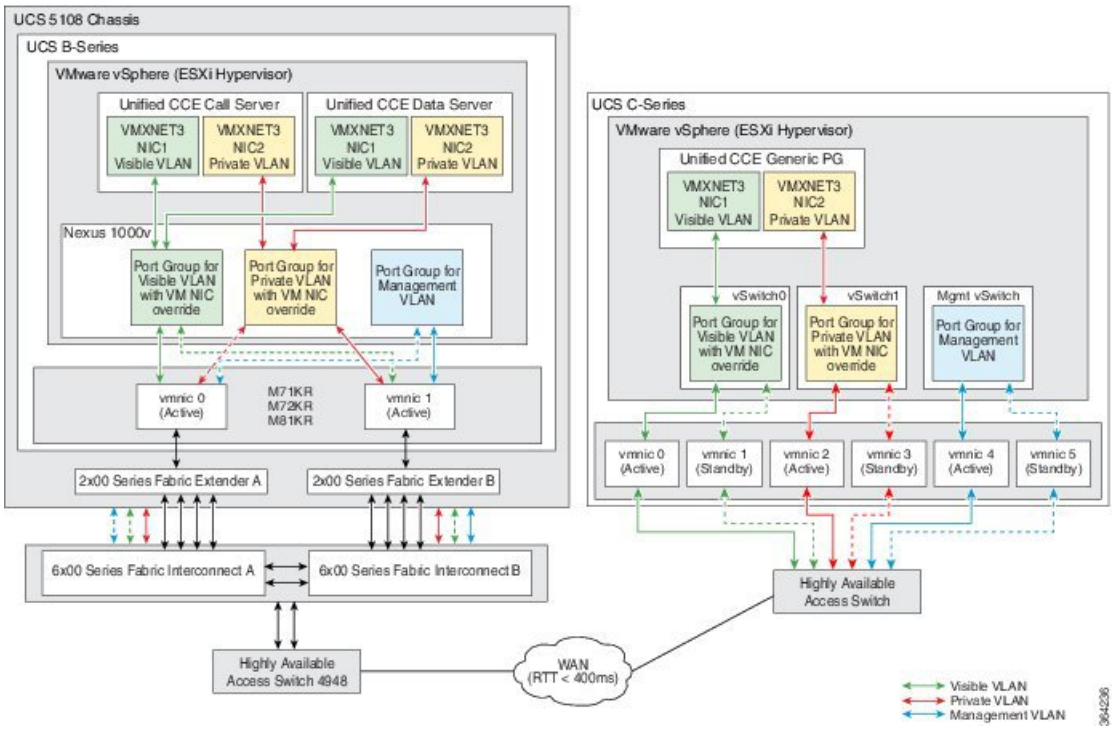
- Side A and Side B latency cannot exceed 80 ms RTT.
- CUCM PIMs are limited to 12 including both central and remote site, if PQs are used in this deployment.

- Use the hostname for CVP Media Servers and configure the IOS gateways pointing to the local CVP servers.

## Global Deployment UCS Network Reference Design

The figure illustrates the default design for HCS Core Data Center on UCS B Series blades and HCS remote Data Center on UCS C-series servers to meet Public and Private Network communications requirements.

***Figure 46: UCS Network Reference Design for Global Deployment***

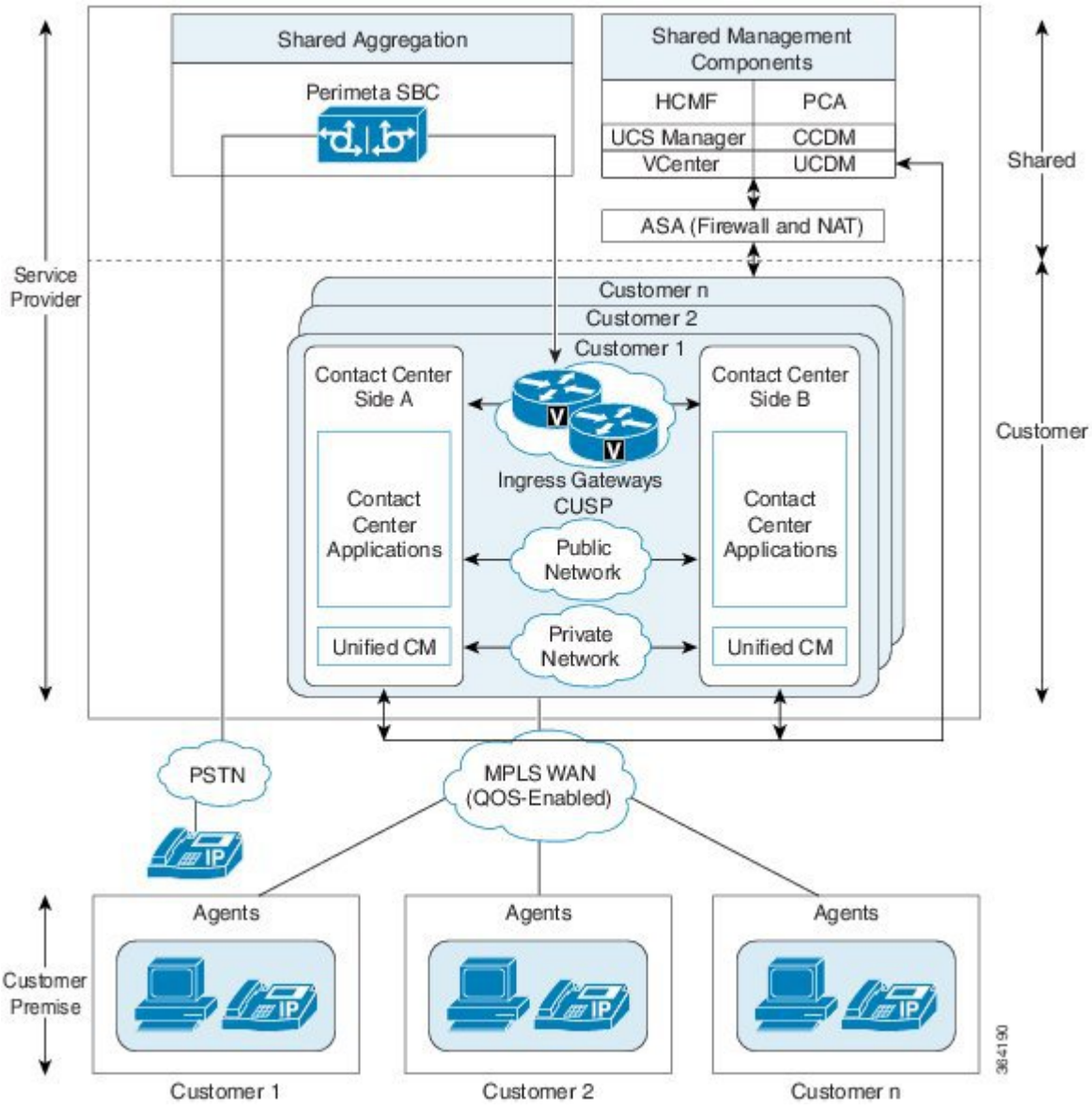



# Local Trunk Design Considerations


- CUBE-Enterprise at Customer Premise, on page 164
- TDM Gateway at Customer Premise, on page 165
- Location-Based Call Admission Control, on page 165

The following figure shows these two options, Cisco Unified Border Element—Enterprise at the customer premise and TDM gateway at the customer premise.

***Figure 47: CUBE(E) or TDM Gateway at the Customer Premise***




## CUBE-Enterprise at Customer Premise

Consider the following if you use the Cisco Unified Border Element - Enterprise at the customer premise:

- Cisco Unified Border Element - Enterprise gateway and the Cisco VXML gateway reside at the customer premise and calls are queued at the customer premise.

- The Cisco Unified Border Element - Enterprise and VXML gateway can be co-located on the same ISR, or located on different ISRs for cases where the number of IVR ports to agent ratio is small.
- Cisco Unified Border Element - Enterprise Integrated Services Router (ISR) provides the security, routing, and Digital Signal Processors (DSPs) for transcoders.
- Redundant Cisco Unified Border Element - Enterprise and Cisco VXML ISRs for failover and redundancy.
- WAN bandwidth must be sized appropriately for calls from Perimeta SBC to CUBE - Enterprise at the customer premise.
- Cisco Unified Border Element Enterprise supports flow-through mode. Flow-around mode is not supported.

## TDM Gateway at Customer Premise

You can route PSTN calls using local gateway trunks if you prefer to keep your E1/T1 PSTN.

Consider the following if you use the TDM gateway at the customer premise:

- Both the Cisco TDM Gateway and the Cisco VXML gateway reside at the customer premise.
- PSTN delivery is at the local customer premise.
- The media stays local at the customer premise for the local PSTN breakout. The IVR call leg is deterministically routed to the local VXML gateway and only uses the centralized resources in spill-over scenarios.
- When media is delivered to a different site, Cisco Unified Communications Manager location-based call admission control limits the number of calls over the WAN link.
- Calls local to a customer premise use the G.711 codec. Calls going over the WAN link can use the G.729 codec to optimize the WAN bandwidth.
- ASR/TTS server for local breakout is at the customer premise and resides on a UCS or bare metal server.
- An incoming call for HCS for Contact Center must originate from the TDM gateway to anchor the call to the survivability service. The Contact Center dialed number to route the calls to Unified Communications Manager must be configured manually.

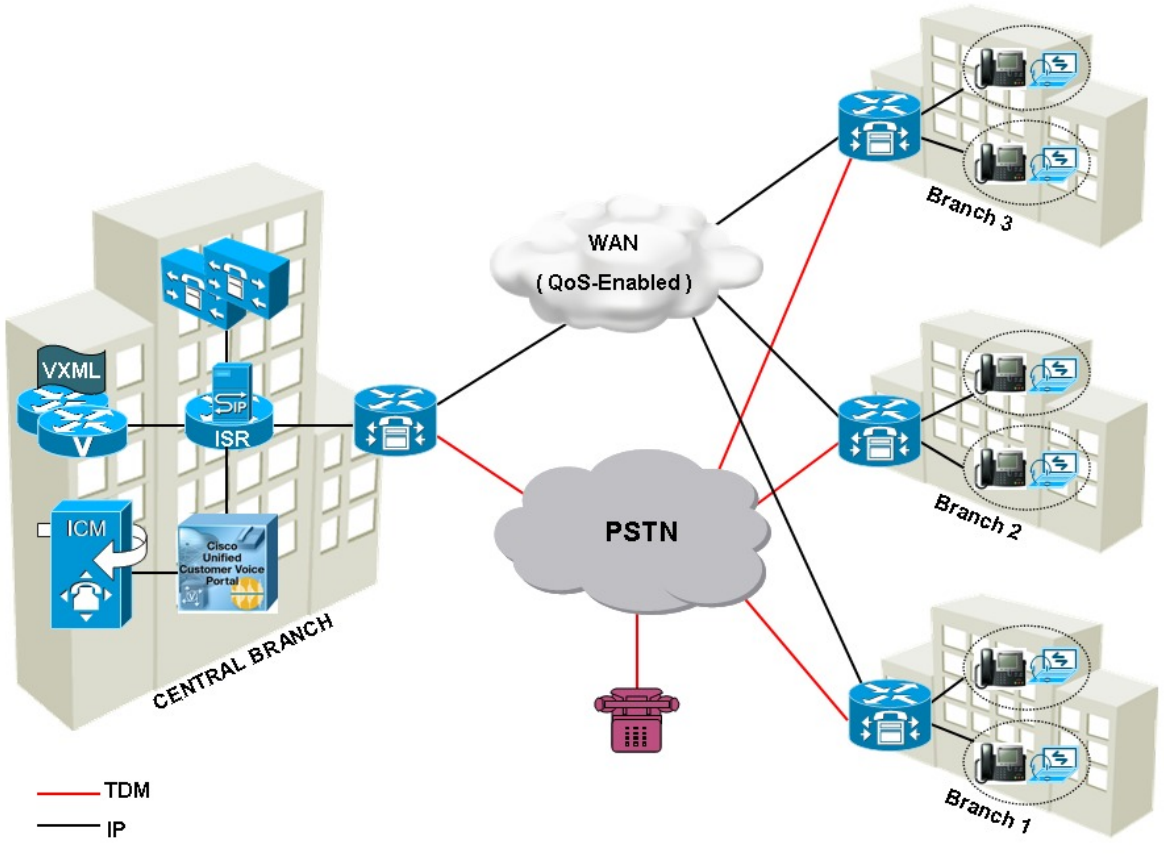
**Note** Manually modify the call routing from TDM gateway for the session target to route the call directly to Unified CVP.

## Location-Based Call Admission Control

Location-based Call Admission Control (LBCAC) maximizes local branch resources, keeping a call within the branch whenever possible and limiting the number of calls that go over the WAN. Unified CVP supports queue-at-the-edge, a simpler and more effective configuration. Using the queue-at-the-edge functionality, the

originating call from a specific branch office is routed to a local VXML Gateway based on priority. That is, it always chooses a local branch agent if possible.

***Figure 48: Location-based Call Admission Control***




**Note** Multi-Cluster, EL-CAC is not supported.

# Domain and Active Directory Considerations

The Unified CCE uses Active Directory (AD) to control users' access rights to perform setup, configuration, and reporting tasks. AD also grants permissions for different components of the system software to interact; for example, it grants permissions for a Distributor to read the Logger database. For more information, see Staging Guide for Cisco Unified Contact Center Enterprise.

Each Cisco HCS for Contact Center must have its own set of Windows Server domain controllers with the functional level 2003 or above version. The domain controller must meet the minimum requirements shown in the following table:

*Table 37: Domain Controller Minimum Requirements*

| Virtual Machine | vCPU | RAM (GB) | Disk C (GB) | CPU Reservation (MHz) | RAM Reservation (MB) |
|---|---|---|---|---|---|
| Cisco HCS Domain Controller | 1 | 4 | 60 | 1400 | 512 |

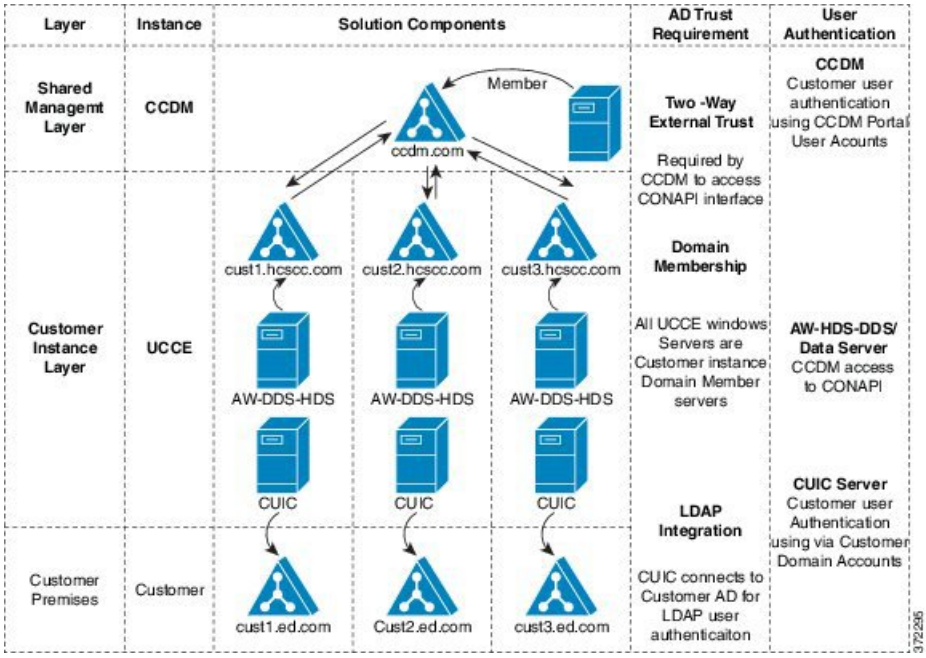
**Note** Use 2 vCPUs for larger directories.

Cisco HCS for Contact Center supports two AD deployment models:

- AD at Customer Premises, on page 168
- AD at Service Provider Premises, on page 168

The following figure shows the Cisco HCS for Contact Center AD deployment.

*Figure 49: Cisco HCS for Contact Center AD Deployment*




For more information on Active directory support for UCCE see, Staging Guide for Cisco Unified ICM/ Contact Center Enterprise.

# AD at Customer Premises

In the AD at the customer premises model, the service provider needs to request that the customer add entries into the customer AD to enable the service provider to sign into the system deployed in the domain. The service provider should be a local machine administrator and belong to the setup group for components that need to be installed and managed in the Cisco HCS for Contact Center environment. To run the Domain Manager, the service provider must be a domain administrator or a domain user with domain read and write permissions to create Organizational Units (OU) and groups.

The end-customer use of the Cisco HCS for Contact Center solution is limited if the customer premises AD is inaccessible to the Cisco HCS for Contact Center Virtual Machines. Cisco strongly advises service providers to work with end customers to ensure that they understand the potential service limitations when they use the AD at the customer premises model.

Cisco HCS for Contact Center also supports a deployment where the Cisco HCS for Contact Center components are associated with the AD at the service provider premises, and the CTI OS client desktops are part of the customer premises corporate AD. Consider the following for the AD in this deployment:

- The instance administrator account is created in the service provider domain.
- The instance administrator uses the Unified CCDM and Unified Intelligence Center to create agents, supervisors, and reporting users in the service provider domain.
- The instance administrator configures all supervisors and reporting users.

# AD at Service Provider Premises

In the AD at the service provider premises model, the service provider must have a dedicated AD for each customer instance. Each customer AD needs to be updated with Cisco HCS for Contact Center servers and accounts. The service provider administrator needs to be added to each customer AD to manage the Contact Center environment.

You can use overlapping IP addresses for each customer deployment. For example, Cisco Unified Border Element — Enterprise, Unified CCE, and Unified CVP should be able to overlap IP addresses across customers. When you use overlapping IP addresses, the static Network Address Translation (NAT) provides access from the management system to each Cisco HCS for Contact Center environment.

**Note** You must create a two-way forest trust between each customer AD and Service provider Management AD to integrate customer instance with Unified CCDM. You must also open the ports in the ASA firewall. Refer to the Install and Configure ASA Firewall and NAT, on page 227 section.

For opening ports and configurations, see http://support.microsoft.com/kb/224196

# Storage, VM Specifications, and IOPS Considerations

# Storage Considerations for All Deployments



## vSphere Storage Design

This section describes the storage configuration to be used for the HCS VMware vSphere environment. For similar reasons to aforementioned caveats around over subscription and resource assignment from a VMware perspective, similar restrictions apply to storage also, they are as follows:

- Thin provisioning of UC App VMDKs is not supported
- A VM datastore should consist of a single LUN (i.e. 1:1 LUN to Datastore)
- Cisco recommends no more than 8 UC VMs per LUN
- Cisco recommends LUNs for UC applications should be between 500GB and 2TB in volume
- Cisco recommends that 10% of a LUN should be left as head room

Using Cisco provided OVA templates to deploy HCS components and UC applications ensure that thick provisioned disks are used for production.

Tiered storage is the preferred deployment option for HCS, and if the selected array provides this capability, then it should be utilised. Testing has shown that the UC applications have a 95% skew, where 95% of disk I/O occurs on only 5% of the capacity. The array identifies these "hot" blocks automatically and move to a faster tier of storage.

## Shared LUNs

Following are the key requirements for HCS storage:

- Each VMware cluster require its own set of datastores for hosting HCS applications
- An additional shared datastore is required for the HCS-F IPA function to store virtual floppy disk images. This is shared across the Oversubscribed UC and Dedicated UC hosting clusters
- An additional shared datastore is required to store virtual machine templates. This is shared across the, Oversubscribed UC, Dedicated UC and Auxiliary hosting clusters
- There is a limit of 8 UC VMs per LUN
- At least 10% of each LUN should be reserved as overhead
- LUNs should be distributed across the VNX storage processors to load balance IO requests across the SAS buses within the array
- Thin provisioning of LUNs is not recommended due to the potential for service failures should a LUN become exhausted and UC apps become unable to write to their vDisks

# Storage, VM Specifications, and IOPS Considerations for HCS Shared Management Components



## SAN Configuration for HCS Shared Management Components

The HCS deployment requires 1.2 TB of SAN storage for the shared management components. The following table contains the SAN configuration for HCS Shared Management Components.

***Table 38: SAN Configuration for the Management Components***

| RAID Group* | VM Datastore | Virtual Machine |
|---|---|---|
| RAID5 | Datastore-600 GB | Unified CCDM Database Server, Side A<br>Unified CCDM Web Server, Side A |
| | Datastore-600 GB | Unified CCDM Database Server, Side B<br>Unified CCDM Web Server, Side B |

## VM Specifications for HCS Shared Management Components

The HCS deployment requires a single high-density (B200 M4) blade for the shared management components.

The following tables contain the VM specifications for the shared management components, chassis 1 and 2.

***Table 39: VM Specifications for the Management Components***

| Virtual Machine | vCPU | RAM (GB) | Disk C (GB) | Disk D (GB) | CPU Reservation (MHz) | RAM Reservation (MB) |
|---|---|---|---|---|---|---|
| Unified CCDM Database Server | 8 | 32 | 100 | 200 | 15000 | 20480 |
| Unified CCDM Web Server | 8 | 32 | 100 | 60 | 11000 | 12288 |

## IOPS Requirement for HCS Shared Management Components

The following table contain the IOPS (Input/Output Operations Per Second) 95th percentile value to design the SAN array and the IOPS average value to monitor the SAN array.

*Table 40: IOPS, Disk Read, and Disk Write*

| Virtual Machine | IOPS | | | Disk Read Kbytes/sec | | | Disk Write Kbytes / sec | | |
|---|---|---|---|---|---|---|---|---|---|
| | Peak | 95th Percentile | Average | Peak | 95th Percentile | Average | Peak | 95th Percentile | Average |
| Unified CCDM Database Server | 5900 | 1050 | 775 | 300 | 50 | 75 | 1400 | 250 | 175 |
| Unified CCDM Web Server | 900 | 650 | 565 | 100 | 50 | 65 | 200 | 150 | 125 |

# Storage, VM Specifications, and IOPS Considerations for HCS Core Components



## SAN Configuration for HCS Core Components

The following table contains the SAN configuration for all HCS deployment models.

**Note** HCS for Contact Center recommends configuring the SAN disk as RAID5 for added performance and fault tolerance.

*Table 41: SAN Configuration for HCS Core Components*

| Virtual Machines | 500 Agent | 1000 Agent | 4000 Agent | 12000 Agent | Small Contact Center (Shared) |
|---|---|---|---|---|---|
| Unified CCE - All VMs | 1 Datastore (1.5 TB) | 1 Datastore (2.0 TB) | 2 Datastores (2.0 TB) | 4 Datastores (2.0 TB) | 1 Datastore (2.0 TB)<br>1 Datastore (1.5 TB) |
| Unified CVP - All VMs | 1 Datastore (1.0 TB) | 1 Datastore (1.5 TB) | 2 Datastores (2.0 TB) | 5 Datastores (2.0 TB) | 2 Datastores (2.0 TB) |
| CUCM, CUIC, Finesse - All VMs | 1 Datastore (1.0 TB) | 1 Datastore (1.0 TB) | 1 Datastore (2.0 TB) | 2 Datastores (2.0 TB)<br>2 Datastores (1.5 TB) | 1 Datastore (1.5 TB) |

| Virtual Machines | 500 Agent | 1000 Agent | 4000 Agent | 12000 Agent | Small Contact Center (Shared) |
|---|---|---|---|---|---|
| Total SAN Storage | 3.5 TB | 4.5 TB | 10 TB | 25TB | 9 TB |

## VM Specifications for HCS Core Components

The following table contains the VM specification for the HCS Core solution components.

**Note** The vCPU is oversubscribed, but the overall CPU MHz and memory is not oversubscribed for the blade.

***Table 42: VM Specifications for the Core Components***

| Components | Specifications | 500 Agents | 1000 Agents | 4000 Agents | Small Contact Center | | 12000 Agents |
|---|---|---|---|---|---|---|---|
| | | | | | 100 Agents | 500 Agents | |
| Unified CCE Call Server | vCPU | 2 | 4 | NA | NA | NA | NA |
| | Mhz Resv | 3300 | 5000 | | | | |
| | RAM | 4 | 8 | | | | |
| | MB Resv | 4096 | 8192 | | | | |
| | Disk C | 80 | 80 | | | | |
| Unified CCE Data Server | vCPU | 2 | 4 | NA | NA | NA | NA |
| | Mhz Resv | 3400 | 5100 | | | | |
| | RAM | 6 | 8 | | | | |
| | MB Resv | 6144 | 8192 | | | | |
| | Disk C | 80 | 80 | | | | |
| | Disk D | 512 | 750 | | | | |
| Unified CCE Logger | vCPU | NA | NA | NA | NA | NA | 4 |
| | Mhz Resv | | | | | | 3000 |
| | RAM | | | | | | 8 |
| | MB Resv | | | | | | 8192 |
| | Disk C | | | | | | 80 |
| | Disk D | | | | | | 500 |

| Components | Specifications | 500 Agents | 1000 Agents | 4000 Agents | Small Contact Center | | 12000 Agents |
|---|---|---|---|---|---|---|---|
| | | | | | 100 Agents | 500 Agents | |
| Unified CCE Router | vCPU | NA | NA | NA | NA | NA | 4 |
| | Mhz Resv | | | | | | 3000 |
| | RAM | | | | | | 8 |
| | MB Resv | | | | | | 8192 |
| | Disk C | | | | | | 80 |
| Unified CCE Rogger | vCPU | NA | NA | 4 | 4 | 4 | NA |
| | Mhz Resv | | | 5400 | 5400 | 5400 | |
| | RAM | | | 6 | 6 | 6 | |
| | MB Resv | | | 6144 | 6144 | 6144 | |
| | Disk C | | | 80 | 80 | 80 | |
| | Disk D | | | 150 | 150 | 150 | |
| Unified CCE AW-HDS-DDS / AW-HDS / HDS-DDS * | vCPU | NA | NA | 4 | 4 | 4 | 4 |
| | Mhz Resv | | | 3600 | 3600 | 3600 | 3600 |
| | RAM | | | 8 | 8 | 8 | 8 |
| | MB Resv | | | 8192 | 8192 | 8192 | 8192 |
| | Disk C | | | 80 | 80 | 80 | 80 |
| | Disk D | | | 500 | 500 | 500 | 500 |
| Unified CCE Agent PG | vCPU | NA | NA | 2 | 1 | 1 | 2 |
| | Mhz Resv | | | 3600 | 900 | 1800 | 3600 |
| | RAM | | | 6 | 4 | 4 | 6 |
| | MB Resv | | | 6144 | 4096 | 4096 | 6144 |
| | Disk C | | | 80 | 80 | 80 | 80 |
| Unified CCE VRU PG | vCPU | NA | NA | 2 | 2 | 2 | 2 |
| | Mhz Resv | | | 1800 | 1800 | 1800 | 1800 |
| | RAM | | | 2 | 2 | 2 | 2 |
| | MB Resv | | | 2048 | 2048 | 2048 | 2048 |
| | Disk C | | | 80 | 80 | 80 | 80 |

| Components | Specifications | 500 Agents | 1000 Agents | 4000 Agents | Small Contact Center | | 12000 Agents |
|---|---|---|---|---|---|---|---|
| | | | | | 100 Agents | 500 Agents | |
| Unified CVP Server | vCPU | 4 | 4 | 4 | 4 | 4 | 4 |
| | Mhz Resv | 1800 | 1800 | 1800 | 1800 | 1800 | 1800 |
| | RAM | 6 | 6 | 6 | 6 | 6 | 6 |
| | MB Resv | 6144 | 6144 | 6144 | 6144 | 6144 | 6144 |
| | Disk C | 150 | 150 | 150 | 150 | 150 | 150 |
| Unified CVP Reporting Server | vCPU | 4 | 4 | 4 | 4 | 4 | 4 |
| | Mhz Resv | 2500 | 2500 | 6600 | 6600 | 6600 | 6600 |
| | RAM | 4 | 4 | 4 | 4 | 4 | 4 |
| | MB Resv | 4096 | 4096 | 4096 | 4096 | 4096 | 4096 |
| | Disk C | 80 | 80 | 80 | 80 | 80 | 80 |
| | Disk D | 300 | 438 | 438 | 438 | 438 | 438 |
| Unified CVP OAMP | vCPU | 2 | 2 | 2 | 2 | 2 | 2 |
| | Mhz Resv | 400 | 400 | 400 | 400 | 400 | 400 |
| | RAM | 2 | 2 | 2 | 2 | 2 | 2 |
| | MB Resv | 2048 | 2048 | 2048 | 2048 | 2048 | 2048 |
| | Disk C | 80 | 80 | 80 | 80 | 80 | 80 |
| Unified Communications Manager | vCPU | 2 | 2 | 2 | 2 | 2 | 2 |
| | Mhz Resv | 800 | 3600 | 3600 | 800 | 3600 | 3600 |
| | RAM | 4 | 6 | 6 | 4 | 6 | 6 |
| | MB Resv | 3072 | 6144 | 6144 | 3072 | 6144 | 6144 |
| | Disk C | 80 | 110 | 110 | 80 | 110 | 110 |
| Unified Intelligence Center | vCPU | NA | NA | 4 | 4 | 4 | 4 |
| | Mhz Resv | | | 900 | 900 | 900 | 900 |
| | RAM | | | 10 | 10 | 10 | 10 |
| | MB Resv | | | 10240 | 10240 | 10240 | 10240 |
| | Disk C | | | 146 | 146 | 146 | 146 |

| Components | Specifications | 500 Agents | 1000 Agents | 4000 Agents | Small Contact Center | | 12000 Agents |
|---|---|---|---|---|---|---|---|
| | | | | | 100 Agents | 500 Agents | |
| Unified Intelligence Center with LiveData | vCPU | 2 | 4 | NA | NA | NA | NA |
| | Mhz Resv | 800 | 900 | | | | |
| | RAM | 10 | 10 | | | | |
| | MB Resv | 10240 | 10240 | | | | |
| | Disk C | 146 | 146 | | | | |
| Live Data Reporting System | vCPU | NA | NA | 4 | NA | 4 | 8 |
| | Mhz Resv | | | 3600 | | 3600 | 3600 |
| | RAM | | | 24 | | 24 | 24 |
| | MB Resv | | | 24576 | | 24576 | 24576 |
| | Disk C | | | 146 | | 146 | 146 |
| Cisco Finesse | vCPU | 4 | 4 | 4 | 1 | 4 | 4 |
| | Mhz Resv | 4000 | 8000 | 8000 | 1100 | 4000 | 8000 |
| | RAM | 8 | 8 | 8 | 4 | 8 | 8 |
| | MB Resv | 8192 | 8192 | 8192 | 4096 | 8192 | 8192 |
| | Disk C | 146 | 146 | 146 | 146 | 146 | 146 |

* The DB vDisk can be custom sized at OVA deployment based on solution sizing and customer retention requirements using the DB Estimator Tool.

## IOPS Requirement for HCS Core Components

The following tables contain the required lOPS (Input/Output Operations Per Second)). Use the lOPS 95th percentile value to design the SAN array and the lOPS average value to monitor the SAN array.

*Table 43: IOPS Requirement for HCS Core Components*

| Components | Specifications | | 500 Agent | 1000 Agent | 4000 Agent | Small Contact Center | | 12000 Agent |
|---|---|---|---|---|---|---|---|---|
| | | | | | | 100 Agents | 500 Agents | |
| Unified CCE Call Server | IOPS | Peak | 217.25 | 250.25 | NA | NA | NA | NA |
| | | 95 Percentile | 75.32 | 81.84 | | | | |
| | | Average | 58.48 | 71.58 | | | | |
| | Disk read (kbps) | Peak | 6592 | 9646.8 | | | | |
| | | 95 Percentile | 139.4 | 156.07 | | | | |
| | | Average | 75.86 | 106.292 | | | | |
| | Disk write (kbps) | Peak | 14160 | 28204.8 | | | | |
| | | 95 Percentile | 4054.4 | 10128.83 | | | | |
| | | Average | 2437.47 | 6366 | | | | |
| Unified CCE Data Server | IOPS | Peak | 2042.6 | 2244.98 | NA | NA | NA | NA |
| | | 95 Percentile | 978.26 | 1082.76 | | | | |
| | | Average | 268.45 | 312.4 | | | | |
| | Disk read (kbps) | Peak | 5581 | 56522.25 | | | | |
| | | 95 Percentile | 2891.3 | 18588.62 | | | | |
| | | Average | 731.79 | 4271.13 | | | | |
| | Disk write (kbps) | Peak | 27410 | 24515046 | | | | |
| | | 95 Percentile | 1184935 | 18371.31 | | | | |
| | | Average | 3007.67 | 6317.53 | | | | |
| Unified CCE Logger | IOPS | Peak | NA | NA | NA | NA | NA | 2365 |
| | | 95 Percentile | | | | | | 1582 |
| | | Average | | | | | | 2076 |
| | Disk read (kbps) | Peak | | | | | | 19603 |
| | | 95 Percentile | | | | | | 10846 |
| | | Average | | | | | | 16169 |
| | Disk write (kbps) | Peak | | | | | | 56969 |
| | | 95 Percentile | | | | | | 31443 |
| | | Average | | | | | | 47395 |

| Components | Specifications | | 500 Agent | 1000 Agent | 4000 Agent | Small Contact Center | | 12000 Agent |
|---|---|---|---|---|---|---|---|---|
| | | | | | | 100 Agents | 500 Agents | |
| Unified CCE Router | IOPS | Peak | NA | NA | NA | NA | NA | 9 |
| | | 95 Percentile | | | | | | 4 |
| | | Average | | | | | | 6 |
| | Disk read (kbps) | Peak | | | | | | 1 |
| | | 95 Percentile | | | | | | 0 |
| | | Average | | | | | | 0 |
| | Disk write (kbps) | Peak | | | | | | 143 |
| | | 95 Percentile | | | | | | 95 |
| | | Average | | | | | | 111 |
| Unified CCE Rogger | IOPS | Peak | NA | NA | 633.85 | 633.85 | 633.85 | NA |
| | | 95 Percentile | | | 580.02 | 580.02 | 580.02 | |
| | | Average | | | 203.02 | 203.02 | 203.02 | |
| | Disk read (kbps) | Peak | | | 3153 | 3153 | 3153 | |
| | | 95 Percentile | | | 626.25 | 626.25 | 626.25 | |
| | | Average | | | 328.81 | 328.81 | 328.81 | |
| | Disk write (kbps) | Peak | | | 40552 | 40552 | 40552 | |
| | | 95 Percentile | | | 9137.3 | 9137.3 | 9137.3 | |
| | | Average | | | 3722.76 | 3722.76 | 3722.76 | |
| Unified CCE AW-HDS-DDS / AW-HDS / HDS-DDS * | IOPS | Peak | NA | NA | 1115 | 1115 | 1115 | 1662 |
| | | 95 Percentile | | | 898.54 | 898.54 | 898.54 | 806 |
| | | Average | | | 428.94 | 428.94 | 428.94 | 1239 |
| | Disk read (kbps) | Peak | | | 2732 | 2732 | 2732 | 81429 |
| | | 95 Percentile | | | 781.65 | 781.65 | 781.65 | 13386 |
| | | Average | | | 485.68 | 485.68 | 485.68 | 35178 |
| | Disk write (kbps) | Peak | | | 30154 | 30154 | 30154 | 29406 |
| | | 95 Percentile | | | 7703.8 | 7703.8 | 7703.8 | 8101 |
| | | Average | | | 2905.42 | 2905.42 | 2905.42 | 22747 |

| Components | Specifications | | 500 Agent | 1000 Agent | 4000 Agent | Small Contact Center | | 12000 Agent |
|---|---|---|---|---|---|---|---|---|
| | | | | | | 100 Agents | 500 Agents | |
| Unified CCE Agent PG | IOPS | Peak | NA | NA | 908.5 | 72.05 | 94.15 | 908.5 |
| | | 95 Percentile | | | 106.45 | 40.74 | 43.67 | 106.45 |
| | | Average | | | 54.07 | 19.38 | 30.90 | 54.07 |
| | Disk read (kbps) | Peak | | | 35787 | 4499 | 114.00 | 35787 |
| | | 95 Percentile | | | 31.4 | 13.1 | 10.05 | 31.4 |
| | | Average | | | 484.83 | 38.01 | 2.27 | 484.83 |
| | Disk write (kbps) | Peak | | | 59250 | 2479 | 2309.00 | 59250 |
| | | 95 Percentile | | | 7405.6 | 1499 | 1730.20 | 7405.6 |
| | | Average | | | 2490.91 | 366.83 | 1037.89 | 2490.91 |
| Unified CCE VRU PG | IOPS | Peak | NA | NA | 130.65 | 130.65 | 130.65 | 130.65 |
| | | 95 Percentile | | | 106.35 | 106.35 | 106.35 | 106.35 |
| | | Average | | | 63.7 | 63.7 | 63.7 | 63.7 |
| | Disk read (kbps) | Peak | | | 2516 | 2516 | 2516 | 2516 |
| | | 95 Percentile | | | 800.95 | 800.95 | 800.95 | 800.95 |
| | | Average | | | 154.83 | 154.83 | 154.83 | 154.83 |
| | Disk write (kbps) | Peak | | | 4595 | 4595 | 4595 | 4595 |
| | | 95 Percentile | | | 4187.2 | 4187.2 | 4187.2 | 4187.2 |
| | | Average | | | 2432.77 | 2432.77 | 2432.77 | 2432.77 |
| Unified CVP Server | IOPS | Peak | 637 | 637 | 637 | 637 | 637 | 637 |
| | | 95 Percentile | 62 | 62 | 62 | 62 | 62 | 62 |
| | | Average | 25 | 25 | 25 | 25 | 25 | 25 |
| | Disk read (kbps) | Peak | 2450 | 2450 | 2450 | 2450 | 2450 | 2450 |
| | | 95 Percentile | 1401.7 | 1401.7 | 1401.7 | 1401.7 | 1401.7 | 1401.7 |
| | | Average | 582.12 | 582.12 | 582.12 | 582.12 | 582.12 | 582.12 |
| | Disk write (kbps) | Peak | 4433 | 4433 | 4433 | 4433 | 4433 | 4433 |
| | | 95 Percentile | 4354.1 | 4354.1 | 4354.1 | 4354.1 | 4354.1 | 4354.1 |
| | | Average | 2328.12 | 2328.12 | 2328.12 | 2328.12 | 2328.12 | 2328.12 |

| Components | Specifications | | 500 Agent | 1000 Agent | 4000 Agent | Small Contact Center | | 12000 Agent |
|---|---|---|---|---|---|---|---|---|
| | | | | | | 100 Agents | 500 Agents | |
| Unified CVP Reporting Server | IOPS | Peak | 1250 | 1250 | 1250 | 1250 | 1250 | 1250 |
| | | 95 Percentile | 984 | 984 | 984 | 984 | 984 | 984 |
| | | Average | 329 | 329 | 329 | 329 | 329 | 329 |
| | Disk read (kbps) | Peak | 3126 | 3126 | 3126 | 3126 | 3126 | 3126 |
| | | 95 Percentile | 2068.35 | 2068.35 | 2068.35 | 2068.35 | 2068.35 | 2068.35 |
| | | Average | 764.25 | 764.25 | 764.25 | 764.25 | 764.25 | 764.25 |
| | Disk write (kbps) | Peak | 9166 | 9166 | 9166 | 9166 | 9166 | 9166 |
| | | 95 Percentile | 5945.3 | 5945.3 | 5945.3 | 5945.3 | 5945.3 | 5945.3 |
| | | Average | 2210.38 | 2210.38 | 2210.38 | 2210.38 | 2210.38 | 2210.38 |
| Unified CVP OAMP | IOPS | Peak | 64.02 | 64.02 | 64.02 | 64.02 | 64.02 | 64.02 |
| | | 95 Percentile | 54.92 | 54.92 | 54.92 | 54.92 | 54.92 | 54.92 |
| | | Average | 42.99 | 42.99 | 42.99 | 42.99 | 42.99 | 42.99 |
| | Disk read (kbps) | Peak | 2426.4 | 2426.4 | 2426.4 | 2426.4 | 2426.4 | 2426.4 |
| | | 95 Percentile | 16.524 | 16.524 | 16.524 | 16.524 | 16.524 | 16.524 |
| | | Average | 5.02 | 5.02 | 5.02 | 5.02 | 5.02 | 5.02 |
| | Disk write (kbps) | Peak | 1254.2 | 1254.2 | 1254.2 | 1254.2 | 1254.2 | 1254.2 |
| | | 95 Percentile | 310.8 | 310.8 | 310.8 | 310.8 | 310.8 | 310.8 |
| | | Average | 287.23 | 287.23 | 287.23 | 287.23 | 287.23 | 287.23 |
| Unified Communications Manager | IOPS | Peak | 172.65 | 215 | 215 | 167.55 | 215 | 215 |
| | | 95 Percentile | 72.31 | 128 | 128 | 80.1 | 128 | 128 |
| | | Average | 58.32 | 107 | 107 | 70.97 | 107 | 107 |
| | Disk read (kbps) | Peak | 1068 | NA | NA | 1941 | NA | NA |
| | | 95 Percentile | 5 | | | 52 | | |
| | | Average | 9.11 | | | 29.89 | | |
| | Disk write (kbps) | Peak | 1860 | NA | NA | 1136 | NA | NA |
| | | 95 Percentile | 1775.1 | | | 737.7 | | |
| | | Average | 1218.23 | | | 460.02 | | |

| Components | Specifications | | 500 Agent | 1000 Agent | 4000 Agent | Small Contact Center | | 12000 Agent |
|---|---|---|---|---|---|---|---|---|
| | | | | | | 100 Agents | 500 Agents | |
| Unified Intelligence Center | IOPS | Peak | 781.4 | 781.4 | 781.4 | 781.4 | 781.4 | 781.4 |
| | | 95 Percentile | 628.34 | 628.34 | 628.34 | 628.34 | 628.34 | 628.34 |
| | | Average | 460.17 | 460.17 | 460.17 | 460.17 | 460.17 | 460.17 |
| | Disk read (kbps) | Peak | 466 | 466 | 466 | 466 | 466 | 466 |
| | | 95 Percentile | 433.1 | 433.1 | 433.1 | 433.1 | 433.1 | 433.1 |
| | | Average | 74.32 | 74.32 | 74.32 | 74.32 | 74.32 | 74.32 |
| | Disk write (kbps) | Peak | 7758 | 7758 | 7758 | 7758 | 7758 | 7758 |
| | | 95 Percentile | 6446.3 | 6446.3 | 6446.3 | 6446.3 | 6446.3 | 6446.3 |
| | | Average | 5727.44 | 5727.44 | 5727.44 | 5727.44 | 5727.44 | 5727.44 |
| Unified Intelligence Center with Live Data Reporting System | IOPS | Peak | 467 | 937 | NA | NA | NA | NA |
| | | 95 Percentile | 340 | 533 | | | | |
| | | Average | 109 | 436 | | | | |
| | Disk read (kbps) | Peak | 916 | NA | NA | NA | NA | NA |
| | | 95 Percentile | 378 | | | | | |
| | | Average | 114.86 | | | | | |
| | Disk write (kbps) | Peak | 9285 | NA | NA | NA | NA | NA |
| | | 95 Percentile | 7352.30 | | | | | |
| | | Average | 1656.77 | | | | | |
| Live Data Reporting System | IOPS | Peak | NA | NA | 36 | NA | 36 | 37 |
| | | 95 Percentile | | | 34 | | 34 | 35 |
| | | Average | | | 31 | | 31 | 33 |
| | Disk read (kbps) | Peak | NA | NA | 2 | NA | 2 | 42 |
| | | 95 Percentile | | | 0 | | 0 | 5 |
| | | Average | | | 0.01 | | 0.01 | 1 |
| | Disk write (kbps) | Peak | NA | NA | 419 | NA | 419 | 1132 |
| | | 95 Percentile | | | 386.10 | | 386.10 | 1058 |
| | | Average | | | 321.97 | | 321.97 | 952 |

| Components | Specifications | | 500 Agent | 1000 Agent | 4000 Agent | Small Contact Center | | 12000 Agent |
|---|---|---|---|---|---|---|---|---|
| | | | | | | 100 Agents | 500 Agents | |
| Cisco Finesse | IOPS | Peak | 53.55 | 53.55 | 53.55 | 53.55 | 53.55 | 53.55 |
| | | 95 Percentile | 48.21 | 48.21 | 48.21 | 19.95 | 48.21 | 48.21 |
| | | Average | 29.68 | 29.68 | 29.68 | 17.83 | 29.68 | 29.68 |
| | Disk read (kbps) | Peak | 4 | 4 | 4 | 4 | 4 | 4 |
| | | 95 Percentile | 0 | 0 | 0 | 2.2 | 0 | 0 |
| | | Average | 0.02 | 0.02 | 0.02 | 47.81 | 0.02 | 0.02 |
| | Disk write (kbps) | Peak | 1488 | 1488 | 1488 | 669 | 1488 | 1488 |
| | | 95 Percentile | 1429.15 | 1429.15 | 1429.15 | 211.3 | 1429.15 | 1429.15 |
| | | Average | 920.23 | 920.23 | 920.23 | 167.2 | 920.23 | 920.23 |

**Note**

1. Monitor SAN performance for lOPS and disk usage. lf usage exceeds thresholds, redeploy disk resources during the service window.
2. The lOPS values for Unified Communication Manager in the preceding table are based on the BHCA values. These values may differs for different scenarios. For more information, see IOPS values for Unified Communication Manager , on page 787

# Storage, VM Specifications, and IOPS Considerations for HCS Optional Components



## SAN Configuration for HCS Optional Components

The following table contains the SAN configuration for HCS optional components.

*Table 44: SAN Configuration for HCS Optional Components*

| RAID Group* | VM Datastore | Virtual Machines |
|---|---|---|
| RAID 5 | Datastore-100 GB | Cisco Remote Silent Monitoring |
| | Datastore-900 GB | Cisco MediaSense (Small/Medium) |
| | Datastore-2000 GB | Cisco MediaSense (Large) |
| | Datastore-400 GB | Cisco MediaSense (Expansion) |
| | Datastore-80 GB | Avaya PG |
| | Datastore-300 GB | Cisco Virtualized Voice Browser |

## VM Specifications for HCS Optional Components

The following tables contain the VM specifications for Cisco optional components.

*Table 45: VM Specifications for the Optional Components*

| Virtual Machine | vCPU | RAM (GB) | Disk C (GB) | Disk D (GB) | Disk E (GB) | CPU Reservation (MHz) | RAM Reservation (MB) |
|---|---|---|---|---|---|---|---|
| Cisco Remote Silent Monitoring | 2 | 4 | 100 | - | - | 2130 | 4096 |
| Cisco MediaSense (Small) | 2 | 6 | 80 | 80 | 210 | 2200 | 5460 |
| Cisco MediaSense (Medium) | 4 | 8 | 80 | 80 | 210 | 3200 | 8192 |
| Cisco MediaSense (Large) | 7 | 16 | 80 | 600 | 210 | 15000 | 16384 |
| Cisco MediaSense (Expansion node) | 7 | 16 | 80 | 80 | 210 | 10000 | 16384 |
| Avaya PG | 2 | 6 | 80 | - | - | 3600 | 6144 |
| Cisco Virtualized Voice Browser | 4 | 8 | 146 | 146 | - | 900 | 8192 |

## IOPS Requirement for HCS Optional Components

The following tables contain the lOPS(Input/Output Operations Per Second) 95th percentile value to design the SAN array and the lOPS average value to monitor the SAN array.

| Virtual Machine | IOPS | | | Disk Read (kbps) | | | Disk Write (kbps) | | |
|---|---|---|---|---|---|---|---|---|---|
| | Peak | 95 Percentile | Average | Peak | 95 Percentile | Average | Peak | 95 Percentile | Average |
| Cisco Remote Silent Monitoring | 32 | 4.25 | 2.38 | 1054 | 0 | 8.63 | 718 | 18 | 14.44 |
| Avaya PG | 215 | 128 | 107 | 0 | 0 | 0 | 0 | 0 | 0 |
| Cisco Virtualized Voice Browser | 138.15 | 55.76 | 46.01 | | | | | | |

For Cisco MediaSense IOPS. see IOPS and Storage System Performance Requirement

# Congestion Control Considerations

The Congestion Control feature provides protection to the Central Controller Router from overload conditions, due to high call rates. The main objective of congestion control is to keep the system running close to its rated capacity, when faced with extreme overload. The goal is to give satisfactory service to a smaller percentage of calls (your capacity) rather than a highly degraded service to all the calls, during an overloaded condition. This is achieved by restricting capacity on the system by rejecting calls by the Routing Clients at the call entry point. Throttling the capacities ensures the service of those calls routed is successful, meaning no delays or timeouts.

The measured CPS at router is the trigger for identifying congestion in the system. For a given deployment, the supported capacity is set when the deployment type is selected. The router measures the new incoming call requests from all the routing clients and computes moving weighted average over sample duration. If the average CPS exceeds beyond the thresholds for each level, the congestion levels are changed along with the reduction percentage. The congestion control algorithm utilizes 3 congestion levels and rejects/treats the incoming calls as per the reduction percentage for that level. The change in congestion level is notified to the routing clients. The routing clients start rejecting/treating calls based on reduction percentage

In a Small Contact Center deployment model, where a single instance of CCE central controller is common for multiple sub-customers (PG's), the congestion control would evenly reject calls across all the routing clients in the SCC deployment. The service provider should consider the congestion control while designing and planning the call rates in SCC deployment.

# Deployment Types

After upgrading or installing the system, configure the system to a valid deployment type. If the supported deployment type is not set, the PGs and NICs cannot connect to the Central Controller and process the call.

The following table lists the supported deployment types with guidelines for selecting a valid deployment type.

*Table 46: Supported Congestion Control Deployment Types*

| Deployment Type Code | Deployment Name | Guidelines for Selection |
|---|---|---|
| 15 | HCS-CC 12000 Agents | This deployment should be selected for Unified CCE Enterprise system where only Unified CCE PGs are deployed. The system should be distributed deployment with Router and Logger installed on different servers meets the requirements for 12000 Unified CCE agents. |
| 14 | HCS-CC 4000 Agents | This deployment should be selected for Unified CCE Enterprise system where only Unified CCE PGs are deployed. The system should be distributed deployment with Router and Logger installed on different servers meets the requirements for 4000 Unified CCE agents. |
| 11 | HCS-CC 1000 Agents | This deployment type is automatically set as part of the install for the HCS-CC 1000 agents deployment type and is unavailable for user selection. |
| 12 | HCS-CC 500 Agents | This deployment type is automatically set as part of the install for the HCS-CC 500 agents deployment type and is unavailable for user selection. |

**Note**

- For Small Contact Center deployment model follow the **Deployment Type Code** and **Guidelines** as that of 4000 agent deployment model.
- Configuring the system to a valid HCS deployment type is mandatory to integrate and provision through Unified CCDM.

# Congestion Treatment Mode

There are five options available to handle the calls that are rejected or treated due to congestion in the system. Contact center administrators can choose any of the following options to handle the calls:

- Treat call with Dialed Number Default Label - The calls to be rejected due to congestion are treated with the default label of the dialed number on which the new call has arrived.
- Treat call with Routing Client Default Label - The calls to be rejected due to congestion are treated with the default label of the routing client on which the new call arrived.
- Treat call with System Default Label - The calls to be rejected due to congestion are treated with the system default label set in Congestion Control settings.
- Terminate call with a Dialog Fail or Route End - Terminates the new call dialog with a dialog failure.
- Treat call with a Release Message to the Routing Client - Terminates the new call dialog with release message.

The treatment options are set either at the routing client or at global level system congestion settings. If the treatment mode is not selected at the routing client, then the system congestion settings are applied for treating the calls.

# Congestion Control Levels and Thresholds

Congestion Control algorithm works in three levels; each level has an onset and an abatement value. Rising to higher congestion can happen from any level to any level. However reducing the congestion level occurs one level at a time.

The following table shows the percentage of the CPS capacity for different congestion levels.

***Table 47: Congestion levels and capacities***

| Congestion Levels | Congestion Level Threshold (Percent of Capacity) |
|---|---|
| Level1Onset | 110% |
| Level1Abate | 90% |
| L1Reduction | 10% |
| Level2Onset | 130% |
| Level2Abate | 100% |
| Level2Reduction | 30% |
| Level3Onset | 150% |
| Level3Abate | 100% |
| Level3Redution | Variable reduction from 100% to 10% |

## Congestion Control Configuration

Configure the congestion control settings using the Congestion Settings Gadget and the Routing Client Explorer tool. Use the Congestion Settings Gadget to set the system level congestion control. Use the Routing Client Explorer tool to select the Routing Client level treatment options.

After you select the deployment type, the system starts computing the various metrics related to the congestion control and system capacity, and generates the real time report. However, the system cannot reject or treat the calls until you turn on the Congestion Enabled option in the Congestion Control Setting Gadget.

## Real Time Capacity Monitoring

System Capacity Real Time provides congestion level information to the user. The report provides the following views:

- Congestion Information View
- Rejection Percentage View
- Key Performance Indicators View
- System Capacity View

# UCS Network Considerations

This section provides guidance on performing the network configuration needed to deploy HCS-CC on UCS. It includes information on fault tolerance and redundancy:

- Network Requirements for Cisco UCS B-Series Servers, on page 186
- Network Requirements for Cisco UCS C-Series Servers, on page 189
- VMware High Availability, on page 190
- Network Link High Availability, on page 191

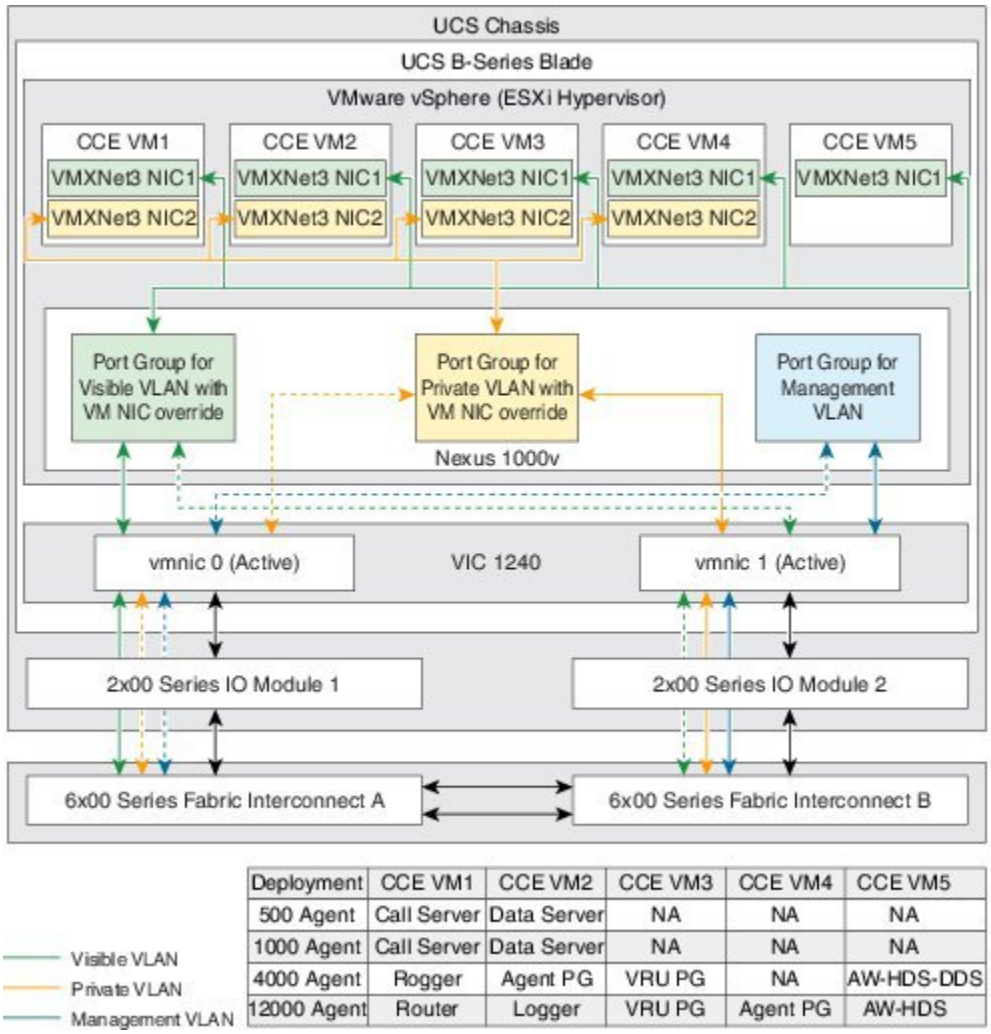
## Network Requirements for Cisco UCS B-Series Servers

The illustration below shows the virtual to physical HCS-CC communications path from application local OS NICs to the data center network switching infrastructure.

The reference design depicted uses a single virtual switch with two vmnics in Active/Active mode, with Visible and Private network path diversity aligned through the Fabric Interconnects using the Port Group vmnic override mechanism of the VMware vSwitch. Path diversity of the Visible and Private networks must

be maintained so that both networks do not fail in the event of a single path loss through the Fabric Interconnects.

***Figure 50: Network Requirements for Cisco UCS B-Series Servers***




| Deployment | CCE VM1 | CCE VM2 | CCE VM3 | CCE VM4 | CCE VM5 |
|---|---|---|---|---|---|
| 500 Agent | Call Server | Data Server | NA | NA | NA |
| 1000 Agent | Call Server | Data Server | NA | NA | NA |
| 4000 Agent | Rogger | Agent PG | VRU PG | NA | AW-HDS-DDS |
| 12000 Agent | Router | Logger | VRU PG | Agent PG | AW-HDS |

- Design of connecting Cisco UCS to Cisco Nexus 7000 Series is available at http://www.cisco.com/c/en/us/products/switches/nexus-7000-series-switches/white-paper-listing.html
- SAN solution (SAN controller and switches) used for HCS-CC on the UCS Storage Interoperability Matrix for the version of UCSM to be deployed http://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/interoperability/matrix/intmatrx.html
- Contact Center with UCS B Fabric Interconnect supports the following:
  - Fabric in end-host Mode
  - No split L2 direct connected to Fabrics prior to UCSM 2.0(2)
  - No Fabric Failover enabled for vNICs in UCS Manager

## Nexus1000v Switch Configurations

The blades use a Cisco Nexus 1000v switch, a vSwitch, and an Active/Active VMNIC. The Cisco Nexus 1000v is the switching platform that provides connectivity of the private VLAN to the virtual machine. The vSwitch controls the traffic for the private and public VLANs. A single vSwitch is used with two VMNICs in Active/Active state.

Ensure that the Visible and Private networks Active and Standby vmnics are alternated through Fabric Interconnects so that no single path failure will result in a failover of both network communication paths at one time. In order to check this, you may need to compare the MAC addresses of the vmnics in vSphere to the MAC addresses assigned to the blade in UCS Manager to determine the Fabric Interconnect to which each vmnic is aligned.

## Data Center Switch Configurations

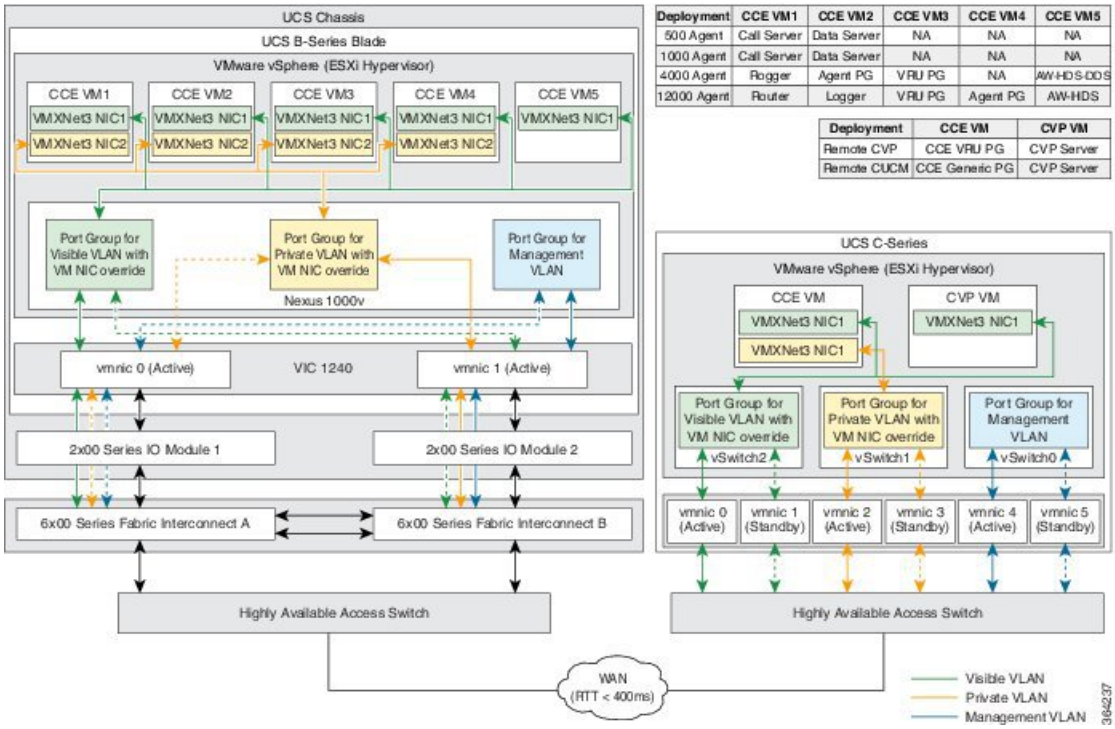
There are several supported designs for configuring Ethernet uplinks from UCS B-Series Fabric Interconnects to the data center switches. Virtual Switch VLAN Tagging is required, with EtherChannel / Link Aggregation Control Protocol (LACP) and Virtual PortChannel (vPC) being options depending on data center switch capabilities.

The required and reference design for Visible and Private network uplinks from UCS Fabric Interconnects uses a Common-L2 design, where both VLANs are trunked to a pair of data center switches. Service Provider also may choose to trunk other management (including VMware) and enterprise networks on these same links, or use a Disjoint-L2 model to separate these networks. Both designs are supported, though only the Common-L2 model is used here.

# Network Requirements for Cisco UCS C-Series Servers

The illustration below shows the reference design for all HCS-CC deployments on UCS C-series servers and the network implementation of the vSphere vSwitch design.

***Figure 51: Network Requirements for Cisco UCS C-Series Servers***




This design calls for using the VMware NIC Teaming (without load balancing) of virtual machine network interface controller (vmnic) interfaces in an Active/Standby configuration through alternate and redundant hardware paths to the network.

The network side implementation does not have to exactly match this illustration, but it must allow for redundancy and must not allow for single points of failure affecting both Visible and Private network communications.

Requirements:

- Ethernet interfaces must be Gigabit speed and connected to Gigabit Ethernet switches. 10/100 Ethernet is not supported
- No single point of failure is allowed for visible and private networks.
- Network switches must be configured properly for connection to VMware

# VMware High Availability

High availability (HA) provides failover protection against hardware and operating system failures within your virtualized Cisco HCS for Contact Center environment.

The following lists the VMware HA considerations for deploying Cisco HCS for Contact Center with VMware HA enabled:

- Cisco HCS does not support VMware Distributed Resource Scheduler (DRS).
- Select the Admission Control Policy: **Specify a failover host**. When an ESXi host fails, all of the VMs on this host fail over to the reserved HA backup host. The failover host Admission Control Policy avoids resource fragmentation. The Cisco HCS for Contact Center deployment models assume a specific VM colocation within a Cisco HCS for Contact Center instance deployment. This VM colocation requirement guarantees system performance, and it is tested for specific Cisco HCS for Contact Center application capacity requirements.
- Select VM monitoring status options: **VM Monitoring Only**.
- Select Host Isolation response: **Shut down** for all the virtual machines.
- Configure the Cisco HCS for Contact Center virtual machines with the VM restart priority shown in the following table.

***Table 48: Virtual Machine Settings***

| Virtual Machine | VM Restart Priority |
|---|---|
| Cisco Unified Intelligence Center | Low |
| Contact Center Domain Manager | Low |
| Unified CVP Reporting Server | Low |
| Unified CCE Call Server | Medium |
| Cisco Finesse | Medium |
| Unified CVP Servers | High |
| Unified CCE Database Server | High |

- HA is not required because the Cisco HCS for Contact Center applications are highly available by design.
- HA Backup Hosts must be in the same cluster, but not in the same physical chassis as the Contact Center blades.
- For more information about high availability see the *VMware vSphere Availability Guide ESXi 5.1, 5.5*.

**Note** Because the Router and PGs are co-located in 500 and 1000 agent deployment model, an unlikely dual (Public and Private) network failure could result in serious routing degradation. The Cisco Hosted Collaboration Solution for Contact Center does not tolerate a dual concurrent network failure, so you may need to intervene to restore the system's full functionality.

## Network Link High Availability

The following lists considerations when the network link fails between Cisco HCS for Contact Center setup and Active Directory:

- Call traffic is not impacted during the link failure.
- The virtual machines in the domain restrict sign in using the domain controller credentials. You can sign in using cached credentials.
- If you stop Unified CCE services before the link fails, you must restore the link before starting the Unified CCE components.
- You will not be able to access the local PG Setup or sign in to the Unified CCE Web Setup.
- If the link fails while the Cisco HCS services are active, access to Unified CCE Web Setup, configuration tools, and Script Editor fails.
- Although the Unified CCDM allows login to the portal, access to the reporting page fails.
- The administrator and superusers can access or configure any attribute except the Reporting Configuration in Cisco Unified Intelligence Center OAMP portal.
- Agent supervisors cannot sign in to the Cisco Unified Intelligence Center Reporting portal, however supervisors already signed in can access the reports.

# Firewall Hardening Considerations

This section describes the specific ports required, which should be allowed from the Contact Center and customer networks, but are restricted only to the ports required for the services that need to be exposed, as well as from specific hosts or networks wherever possible. For an inventory of the ports used across the Hosted Collaboration Solutions for Contact Center applications, see the following documentation:

**Note** Refer to Step 2 in section Configure NAT in the Customer Instance Context, on page 480 for configuring required ports in ASA.

- Port Utilization Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted
- Cisco Unified Customer Voice Portal (CVP) Solution Reference Network Design (SRND) . See section 'TCP/UDP ports used by Unified CVP, voice, and VoiceXML gateways in the *Network infrastructure considerations* chapter.
- TCP and UDP Port Usage Guide for Cisco Unified Communications Manager

- Cisco Unified Intelligence Center TCP and UDP Port Usage
- Installation and Getting Started Guide for Cisco Finesse. See the 'Ports used for Cisco Finesse' section in the *Frequently Asked Questions*. See chapter *Cisco Finesse port utilization* section in the *APPENDIX C*.
- Cisco Unified Web and E-Mail Interaction Manager Solution Reference Network Design Guide. See the 'Port Number Configuration Between Components' in the *System Architecture* chapter.
- Cisco Remote Silent Monitor Installation and Administration Guide. See the 'Port Numbers Used' section in the *Installation* chapter.
- Cisco MediaSense User Guide . See the 'Port Usage' section in the *MediaSense Features and Services* chapter.
- TCP and UDP Port Usage for Active Directory Domain Controller, on page 192

# TCP and UDP Port Usage for Active Directory Domain Controller

Below are ports that needs to be opened in the ASA firewall for the DNS clients to join the Domain Controller.

| Protocol | TCP port | UDP port |
|---|---|---|
| DNS | 53 | 53 |
| Active Directory Domain Controller - LDAP for Global Catalog | 3268 | |
| Active Directory Domain Controller - Secure LDAP for Global Catalog | 3269 | |
| Active Directory Domain Controller - Kerberos | 88 | 88 |
| Active Directory Domain Controller - LDAP | 389 | 389 |
| Active Directory Domain Controller -NetBIOS name resolution services | | 137 |
| Active Directory Domain Controller -NetBIOS Datagram services | | 138 |
| Active Directory Domain Controller - W32Time | | 123 |
| Active Directory Domain Controller (RPC-EPMAP) | 135 | 135 |
| Active Directory Domain Controller -RPC | 49152-65535 | 49152-65535 |

| Protocol | TCP port | UDP port |
|---|---|---|
| Active Directory Domain Controller - SAM/LSA | 445 | 445 |
| Active Directory Domain Controller - Secure LDAP | 636 | |

# License Considerations

Each Cisco HCS for Contact Center license includes:

- Premium agent capabilities
- Cisco Unified Intelligence Center Premium
- One Unified CVP IVR or queuing treatment
- One Unified CVP redundant IVR or queuing treatment

One Unified CVP IVR or queuing treatment license is defined as a call that receives treatment at a VoiceXML browser for queuing or self service by a Unified CVP call server.

One Unified CVP redundant IVR or queuing treatment license is defined as a call that receives treatment on the secondary Unified CVP call server residing on the secondary side for redundancy purposes.

**Note** Both Unified CVP call servers are active and can process calls. This implies that there could be times when you can handle more calls, however, Cisco supports a maximum of 1 IVR or queue treatment port per agent license.

While each HCS for Contact Center license provides a Unified CVP port for self-service or redundancy, current deployment limitations result in slightly lower capacity when running at 100% licensing capacity. For example, 500 agents licensed on a 500 agent deployment model or 1000 agents licensed on a 1000 agent deployment model.

For example, a 500 agent deployment model with 500 agent licenses includes:

- 500 calls receiving IVR or queue treatment and 400 callers talking to agents
- 400 calls in queue receiving IVR or queue treatment and at the same time another 500 callers talking to 500 agents
- 450 calls receiving IVR or queue treatment at 450 agents talking

For example, a 1000 agent deployment model with 1000 agent licenses includes:

- 1000 calls receiving IVR or queue treatment and 800 callers talking to agents
- 800 calls in queue receiving IVR and at the same time another 1000 callers talking to 1000 agents
- 900 agents talking and 900 agents receiving IVR or call treatment

For example, a 4000 agent deployment model with 4000 agent licenses includes:

- 4000 calls receiving IVR or queue treatment and 3200 callers talking to agents
- 3200 calls in queue receiving IVR and at the same time another 4000 callers talking to 4000 agents
- 3600 agents talking and 3600 agents receiving IVR or call treatment

For example, a 12000 agent deployment model with 12000 agent licenses includes:

- 10000 calls receiving IVR or queue treatment and 11600 callers talking to agents
- 9600 calls in queue receiving IVR and at the same time another 12000 callers talking to 12000 agents

**Note** The maximum of 10000 IVR calls is supported by the system.

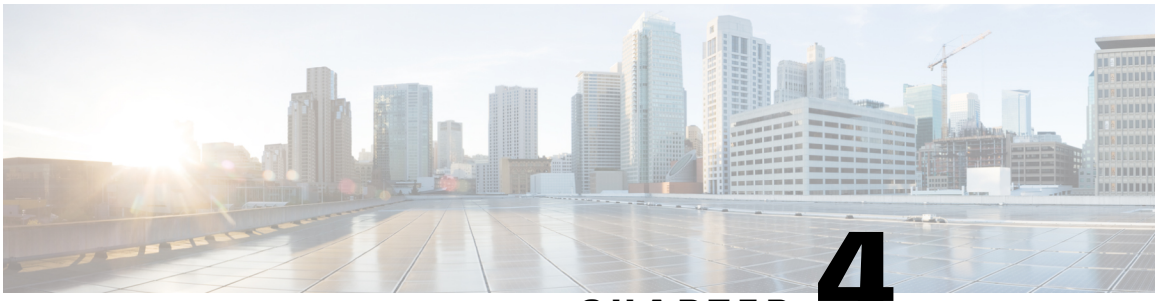
# Billing Considerations

Complete the following procedure to determine the number of phones registered to Cisco HCS for Contact Center for billing purposes.

### Procedure

From the CLI of the Call Manager Publisher virtual machine, run the following query exactly as shown with no new line characters:
**run sql select count(*) from applicationuserdevicemap as appuserdev, applicationuser appuser, device dev where appuserdev.fkapplicationuser = appuser.pkid appuserdev.fkdevice = dev.pkid tkmodel != 73 appuser.name = "pguser"**

**Note** If you configured the application username to a name other than pguser, you must update appuser.name in the above query. This query is based on the supported Cisco HCS for Contact Center deployment, which only requires that you add CTI route points and phones to the application user. If this is not the case, you may need to modify the query.



CHAPTER 4

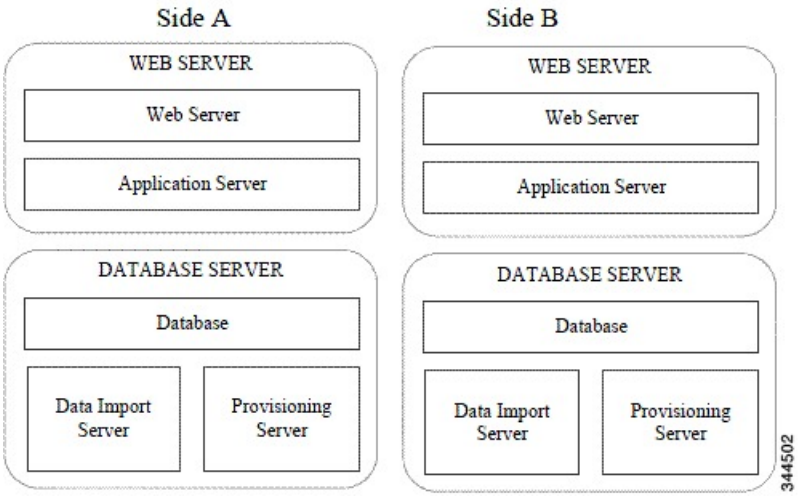
# Shared Management and Aggregation



# Install and Configure Unified CCDM

For Cisco HCS for Contact Center, implement a dual-tier (distributed) system as shown in the following figure. This involves separating the web and application components (App/Web Server) of the Unified CCDM from the database server components.

***Figure 52: Unified CCDM Dual-Tier Deployment***



For dual-sided systems, perform a complete installation on the Side A servers, and then a complete installation on the Side B servers.

- Deploy Unified CCDM Database Server, on page 196
- Deploy Unified CCDM Web Server, on page 205
- Unified CCDM Configuration, on page 209

# Deploy Unified CCDM Database Server

**Note** Before you install CCDM Database server, ensure that you have a naming convention ready for the CCDM Web server, as the host name of CCDM Web server is required during the installation and configuration of CCDM Database server. Do not use hyphens in the server name. Hyphens are not supported.

Follow this sequence of tasks to install Unified CCDM database server on Side A and Side B.

After each task, return to this page to mark the task "done" and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova | Hosted Collaboration Solution for Contact Center OVA, on page 54 |
| 2 | | Create the virtual machine for the Unified CCDM Database Server | Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server | Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252 |
| 4 | | Configure Windows | Configure Windows, on page 197 |
| 5 | | Associate Unified CCDM Component servers with Service Provider AD Domain | Associate Unified CCDM Component servers with Service Provider AD Domain, on page 199 |
| 6 | | Configure Secondary Drive | Configure Secondary Drive, on page 341 |
| 7 | | Install Microsoft SQL Server | Install Microsoft SQL Server 2014 Standard Edition , on page 257 |
| 8 | | Configure Post-Install | Configure Post-Install SQL, on page 199 |
| 9 | | Install Service Pack 1 for the SQL server | Run Service Pack 1 for SQL server |

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 10 | | Install Unified CCDM Database Server | Install Unified CCDM Database Server on Side A and Side B, on page 201<br>**Note** It is required to complete CCDM Web server Side A installation before installing the CCDM Database server on Side B. |
| 11 | | Install the Diagnostic Framework for System CLI | Install the Diagnostic Framework for System CLI , on page 202 |
| 12 | | Install Unified CCDM portal Database | Install Unified CCDM Portal Database on Side A and Side B, on page 202 |
| 13 | | Add SQL Login for Unified CCDM web server | Add SQL Login for Unified CCDM Web Server, on page 204 |
| 14 | | Configuring SNMP Traps | Configure SNMP Traps, on page 207 |

## Configure Windows

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

- Configure Windows Feature Requirements, on page 197
- Turn Off FIPS Compliance, on page 198
- Disable UAC, on page 198

### Configure Windows Feature Requirements

#### Procedure

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

**Step 2** In **Before you begin** page, click **Next**.

**Step 3** In **Installation Type** page, select **Role-based or feature-based installation** option and click **Next**.

**Step 4** In **Select destination server** page, ensure **Select a server from the server pool** option is selected and click **Next**.

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

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

**Step 6** Click **Next**

**Step 7** In **Select features** page, check **.Net Framework 3.5 Features** check-box and click **Next**.

**Step 8** In **Application server** page, click **Next**.

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

- .NET Framework 4.5
- COM+ Network Access
- Incoming Network Transactions
- Outgoing Networking Transactions
- TCP Port Sharing
- Web Server (IIS) Support
- Message Queuing Activation
- Named Pipes Activation
- TCP Activation

**Step 10** Click **Next**.

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

**Step 12** In **Select role services** page, ensure that required role services are selected and click **Next**.

## Turn Off FIPS Compliance

Complete the following procedure to turn off the FIPS compliance checking:

### Procedure

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

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

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

## Disable UAC

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

### Procedure

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

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

**Step 3** Click **OK**.

**Step 4** Restart your machine to commit the new UAC settings.
You have now disabled UAC and are ready to install the Unified CCDM.

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

## Associate Unified CCDM Component servers with Service Provider AD Domain

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

### Procedure

**Step 1** Log in to the machine using local administrator account.

**Step 2** Choose **Start** > **Administrative Tools** > **Server Manager**.

**Step 3** Click **Local Server** in the left panel and click **WORKGROUP** to change system properties.

**Step 4** In **Computer Name** tab, click **Change**.

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

**Step 6** Enter fully qualified Service Provider domain name and Click **OK**.

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

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

**Step 9** Reboot the server and login with domain credentials.

## Configure Post-Install SQL

Complete the following procedures for post-install for SQL configuration:

- Configure DTC, on page 199
- Configure Windows Server 2012 R2 Firewall for SQL Server, on page 200

### Configure DTC

Complete the following procedure to configure Distributed Transaction Coordinator (DTC):

### Procedure

**Step 1** Open **Component Services** application.
**Step 2** Expand **Component Services** > **Computers** > **My Computer** > **Distributed Transaction Coordinator**.
**Step 3** Right-click **Local DTC** and select **Properties**.
**Step 4** Choose **Security** tab.
**Step 5** In **Security** tab, configure the following:

- Ensure that **Security Settings** has **Network DTC Access** selected, and **Transaction Manager Communication** has **Allow Inbound** and **Allow Outbound** selected.
- Set **Transaction Manager Communication** to **No Authentication Required**.
- Click **OK**.

## Configure Windows Server 2012 R2 Firewall for SQL Server

Complete the following procedure to configure Windows server 2012 R2 firewall for SQL server

### Procedure

**Step 1** Open **Server Manager** application.
**Step 2** Select **Tools** > **Windows Firewall with Advanced Security** and click **Inbound Rules**.
**Step 3** In the Actions pane, click **New Rule**.
**Step 4** Select **Port** as the rule type and click **Next**.
**Step 5** Select **TCP** as the protocol and enter 1433 as the Specific local ports. Click **Next**.
**Step 6** Select Allow the connection. Click **Next**.
**Step 7** Select the profile options that are appropriate to your deployment and click **Next**.
**Step 8** Enter a name for the rule and click **Finish** to create the rule.
**Step 9** Close the Server Manager window.

## SQL Server Backup Guidelines

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

## Install Unified CCDM Database Server on Side A and Side B

For dual-tier systems, perform a complete installation on the Side A servers, and then perform a complete installation on the Side B servers.Make sure that the prerequisites are met before you perform these installations. For more information on the prerequisites, see Configure Windows Feature Requirements, on page 197.

Complete the following procedure to install the Unified CCDM Database server:

**Note** It is required to complete CCDM Web server Side A installation before installing the CCDM Database server on Side B.

### Procedure

**Step 1** Mount the correct version of the Unified CCDM ISO image to the virtual machine's CD/DVD drive. For more information, see Mount and Unmount ISO Files, on page 787.

**Step 2** Double-click the mounted ISO image.

**Step 3** In **Cisco Unified CCDM Installation** window, choose the component **Database server** under Server Installation and wait till it completes prerequisite checks, click **Install**.

**Step 4** In **Domain Manager: Database Components - InstallShield wizard** window, click **Next**.

**Step 5** Select **I accept the terms in the license agreement** in **License Agreement** window. Click **Next**.

**Step 6** Enter and confirm the passphrase using 6 to 35 characters in the **Cryptography Configuration** window, click **Next**.
This passphrase is used for encrypting and decrypting system passwords and must be the same for all the servers in the cluster. The contents in the Confirm Passphrase must be identical to the passphrase entered above.

**Step 7** Configure the following in the **Configure Database** window and click **Next**:

- **Catalog Name —** Enter a name for the database catalog that is used for Unified CCDM. It is required that you use the default name. Default name is Portal.
- **Connect Using —** Select this option to use the login credentials to connect.
  - **Windows authentication —** This is a mandatory option.
  - **SQL Server authentication —** Enter the SQL Server Login ID and Password. Use this option only if you are using a database catalog on a different domain.

**Step 8** In the **Destination Folder** window, accept the default location for the Database Server installation. Click **Next**.

**Step 9** In **Ready to Install Program** window, click **Install**.

**Step 10** After the installation, ensure **Launch Database Management Utility** check-box is unchecked. You can later set up the database manually.

**Step 11** Click **Finish**.

**Note** Repeat the above steps to setup CCDM Database Server on Side B.

## Install the Diagnostic Framework for System CLI

### Procedure

**Step 1** To install the Diagnostic Framework component, start the Unified CCDM Installer, click **Support Tools** and select **Diagnostic Framework** .
The **Domain Manager: Diagnostic Framework Install Shield Wizard** window displays.

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

**Step 3** In the **License Agreement** window, select **I accept the terms in the license agreement** and click **Next** .

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

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

**Step 5** Click **Next**.

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

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

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

**Step 9** Unmount the ISO image

## Install Unified CCDM Portal Database on Side A and Side B

Complete the following procedure to setup the database server:

### Procedure

**Step 1** Open **Database Installer**.

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

**Step 3** Choose **Install a new database** from the Database setup page.

**Step 4** Click **Next**.

**Step 5** Enter the following details in the SQL Server Connection Details page:

- **Server Name**

  The name defaults to the Database Server machine name. Accept the default (local).

- **Database Name**

  Enter or select the name of the database catalog to use for Unified CCDM. It is necessary that you use the default name of Portal. This should match the database catalog name specified during Database Server installation.

- **Connect Using—**Select this option to use the login credentials to connect.
  - **Windows authentication—**Select this option to use the windows account information to log in to your computer. This is a mandatory option.
  - **SQL Server authentication—**Select this option only if you are using a database catalog on a different domain. Enter your SQL Server Login Name and Password in the fields provided.

**Step 6** Click **Test Connection** to make sure the connection to the SQL Server is established. Click **OK**.

**Step 7** Click **Next**.

**Step 8** In **Optimize System Databases**, click **Next**.

**Step 9** Check **Replicated Configuration** if the installation is on the Side B server.

a) In **Setup Replication** window, select Replicated Configuration and set up the replication folder share as follows:

- **Share Name** The name of the share for the ReplData folder. By default this is ReplData.
- **Folder Path** The path of the ReplData folder. This is configured in SQL Server, and is by default C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\repldata.

b) Click **Next**.

**Step 10** In the Configure the Location of Data Files window, if you are not using a custom installation of SQL Server, accept the defaults and click **Next**. If you are using a custom installation of SQL Server, configure the data files as follows:

- Select the check box or boxes beside the file group or file groups you want to change.
- To change the Location, browse to the new location.
- To change the Max Size, specify the amount of space that should be allocated for the chosen file group or file groups.
- To specify a different Initial Size, first uncheck Set Initial Size to Max Size.
- You can also choose an unlimited file size by selecting Unrestricted Size, but this is not supported.
- Click **Update** to save your changes.
- Click **Default** to restore the settings for all file groups to their default.
- Click **Next** when you have finished.

**Step 11** Configure the following in the Configure SQL Server Agent Service Identity window:

- **Account Type** - The type of user account that will be used. For a distributed installation, this must be a domain user account.
- **User Name** - Enter the name of the user account. Default value is sql_agent_user. If you selected the Account Type as Domain, enter the domain user account name instead. If you have specified a domain user, you will need to prefix the user name with the domain name, followed by a backslash.
- **Automatically create the user account if missing** - For a single-sided single server system, it is possible to create a local user automatically by selecting this check box.

- **Password** - Create a password for the new user, conforming to your individual system's complexity requirements.
- **Confirm Password** - You will not be able to continue until the contents of this field are identical to the password entered above.
- Click **Next**.

**Step 12** In Ready to Install the database page, Click **Next**.

**Step 13** Click **Close**.

**Step 14** Start the following Unified CCDM services under the Windows services:

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

**Step 15** Repeat the above steps to setup database for Unified CCDM Data Server Side B.

## Add SQL Login for Unified CCDM Web Server

You must create SQL logins so that the Unified CCDM web server can connect to the database server in distributed deployment.

Complete the following procedure to configure Unified CCDM database for Side A and B:

### Procedure

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

**Step 2** Open the **SQL Server 2014 Management Studio**.

**Step 3** Expand **Security > Logins**.

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

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

1. In the **Login Name** field, enter the name for the machine as <DOMAIN>\<Unified CCDM-WEB SERVER HOSTNAME>$.
2. Choose **Windows Authentication** unless you are connecting to a server on another domain.
3. Select Default language as **English**.

**Step 6** Configure the following settings on the **User Mapping** page:

1. In the **Users Mapped to this Login** field, check the **Portal** check box.
2. To grant the Portal login, check the **portalapp_role** , **portalreporting_role**, **portalrs_role**, and **public** check boxes in the **Database role membership for Portal** field.

**Step 7** Click **OK**.

**Step 8** Repeat steps 1 to 7 to add SQL login for Unified CCDM Web Servers in Unified CCDM Database Server for Side B.

# Deploy Unified CCDM Web Server

**Note** Do not use hyphens in the server name. Hyphens are not supported.

Follow this sequence of tasks to install Unified CCDM Web server on Side A and Side B.

After each task, return to this page to mark the task "done" and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova | Hosted Collaboration Solution for Contact Center OVA, on page 54 |
| 2 | | Create the virtual machine for the Unified CCDM Web Server | Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server | Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252 |
| 4 | | Configure Windows | Configure Windows, on page 197 |
| 5 | | Associate Unified CCDM Component servers with Service Provider AD Domain | Associate Unified CCDM Component servers with Service Provider AD Domain, on page 199 |
| 6 | | Configure Secondary Drive | Configure Secondary Drive, on page 341 |
| 7 | | Install Unified CCDM Web Server | Install Unified CCDM Web Server on Side A and Side B, on page 206<br>**Note** It is required to complete CCDM Data server Side B installation before installing CCDM Web server on Side B. |
| 8 | | Install the Diagnostic Framework for System CLI | Install the Diagnostic Framework for System CLI , on page 202 |
| 9 | | Configuring SNMP Traps | Configure SNMP Traps, on page 207 |

# Install Unified CCDM Web Server on Side A and Side B

**Note** It is required to complete CCDM Data server Side B installation before installing CCDM Web server on Side B.

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

### Procedure

**Step 1** Mount the correct version of the Unified CCDM ISO image to the virtual machine's CD/DVD drive. For more information, see Mount and Unmount ISO Files, on page 787.

**Step 2** Double-click the mounted ISO image.

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

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

**Step 5** Select **I accept the terms in the license agreement** in **License agreement** window, and click **Next**.

**Step 6** Enter and confirm the passphrase using 6 to 35 characters in **Cryptography Configuration** window, and click **Next**.
This passphrase is used for encrypting and decrypting system passwords and must be the same for all the servers in the cluster. The contents in the Confirm Passphrase must be identical to the passphrase entered above.

**Step 7** In **Destination Folder** window, accept the default location for the App/Web Server installation. Click **Next**.

**Step 8** Configure the following in the **Configure Database** window and click **Next**:

- **SQLServer Name -** Enter the Side A database server host name. The default option is valid only for the All-in-One deployment type.

  **Note** When you install the app/web server on Side B, enter the Side B database server host name.

- **Catalog Name -** Enter or select the name you selected while installing the Database Server component. The default value is Portal.
- **Connect Using -** Select the radio button of the login credentials you wish to apply.
  - **Windows authentication -** This is a mandatory option.
  - **SQL Server authentication -** Select this option only if you are using a database catalog on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.

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

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

**Note** In a dual-sided Unified CCDM deployment setup, for replicating systems, repeat this installation for side B. It is required that you complete the side A installation of all components before installing side B.

## Configure SNMP Traps

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

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

- Enable Windows SNMP Feature, on page 207
- Configure SNMP Service for Trap Forwarding, on page 207
- Configure Windows Events to Forward to SNMP, on page 208

### Enable Windows SNMP Feature

To configure Windows event forwarding to SNMP, the SNMP feature in Windows must be enabled. To do this, on the Unified CCDM server containing the component for which traps are required:

#### Procedure

**Step 1** Open **Server Manager**.
**Step 2** Click **Dashboard** in the left pane and select **Add Roles and Features** option.
**Step 3** Check **SNMP Services** check-box and ensure whether **SNMP WMI** provider is also checked.
**Step 4** Click **Next** and then click **Install** to complete the deployment of SNMP.
**Step 5** Close **Server Manager**.

### Configure SNMP Service for Trap Forwarding

The SNMP Service must be configured to forward traps to the management tool that is being used for reporting and alerting.

### Procedure

**Step 1** From the Start menu, select **All Programs** > **Administrative Tools** > **Services**.

**Step 2** In the list of services, locate the **SNMP Service**, right-click and select **Properties**.

**Step 3** In **Traps** tab, enter public in **Community Name** field and click **Add to List**.

**Step 4** Click **Add** below the Trap destinations field and in the SNMP Service Configuration dialog box, enter the host name or IP address of the system that will be receiving the trap information (that is, the server hosting the management agents or reporting and alerting tools). Click **Add** to add the trap destination.

**Step 5** If there is more than one system that needs to receive the trap information, repeat step 4 for each of the other servers.

**Step 6** Click **OK**, then close the Services window.

## Configure Windows Events to Forward to SNMP

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

### Procedure

**Step 1** From the **Start** menu, select **Run**, and enter **evntwin.exe**.

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

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

| Event Source | Description |
|---|---|
| UCCDM Application Server Monitoring | The core monitoring service for the application server. This posts connection change events to the event log. |
| UCCDM Data Import Server Monitoring | The data import service used for importing data from CCE etc. |
| UCCDM Partition Table Manager Monitoring | Connection monitoring for the partition manager service (which creates partitioning tables in the database). |
| UCCDM Provisioning Server Monitoring | Service used for provisioning changes on remote equipment, for example, CCE etc. |
| UCCDM: Partition Table Manager | Core application service for creating partitioning tables in the database. |

| Event Source | Description |
|---|---|
| X_ANALYTICALDATA, X_HIERARCHY, X_IMPORTER etc. | These are the individual services configured in Windows for Unified CCDM. These applications can be used for subscribing to standard service events, for example, start/stop events etc. |

**Step 4** To configure an event source to generate SNMP traps, select the event source, wait a few moments, then click **Add** once it is enabled. In the Properties dialog, specify the trap properties required, then click **OK**.

**Step 5** When you have finished setting the SNMP traps you require, click **Apply**.

# Unified CCDM Configuration

For the Unified CCDM to operate correctly, establish communications channels between the different Unified CCDM components so that each individual Unified CCDM component connects to the appropriate channels in the event of a failure.

Complete the procedures in the following order for Unified CCDM cluster configuration:

| Sequence | Done ? | Task | Notes |
|---|---|---|---|
| 1 | | Launch the Integrated Configuration Environment, on page 209 | |
| 2 | | Set Up Unified CCDM Servers , on page 210 | |
| 3 | | Configure Replication, on page 211 | |
| 4 | | Login to Unified CCDM, on page 212 | |
| 5 | | Configure Single Sign-On, on page 212 | |

## Launch the Integrated Configuration Environment

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

### Procedure

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

**Step 2** Enter the following details in the Database Connection page:

a) The Server Name field default value is the 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 loaded as the default tool. You can use the Tool drop-down in the toolbar to switch to other ICE tools.

## Set Up Unified CCDM Servers

Complete the following procedure to set up Unified CCDM servers.

### Procedure

**Step 1** Launch **Integrated Configuration Environment** on Unified CCDM Database Server Side A, see Launch the Integrated Configuration Environment, on page 209.

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

**Step 3** In **Configure Redundancy** select a Dual-Sided system and click **Next**.

**Step 4** For the two-tier deployment, enter the number of web servers for each side. For dual-sided configurations, you must configure an equal number of app/web servers on each side of the system and click **Next**.

**Step 5** In the **Configure Servers** page, configure the following:

a) Enter the name and IP address of the primary database server.
b) Enter the name and IP address of the secondary database server.

**Step 6** Click **Next**.

**Step 7** In the **Configure Application Servers (1)** page, configure the following:

a) Enter the name and IP address of the primary web server.
b) Enter the name and IP address of the secondary web server.
c) Click **Next**.

**Step 8** In the **Configure Database Connection** page, enter the following details:

a) **Catalog** - Enter the name of the Unified CCDM Relational database. The default is Portal.
b) **Authentication** - Select the authentication mode to connect to Unified CCDM relational database.

- **Windows Authentication** - The default required authentication mode.
- **SQL Authentication**- Select this option only if you are using a database server on a different domain. For this option you must enter your SQL Server Login Name and Password in the fields provided.

**Step 9** Click **Next**.

**Step 10** If you want to print the deployment summary, click **Print** below the summary list

**Step 11** Verify the deployment details, and click **Next**.

A confirmation message appears to indicate that the wizard has completed successfully.

**Step 12** Click **Exit** to close the wizard.

**Step 13** Click **Save** on ICE window.

## Configure Replication

In a dual-sided Unified CCDM deployment setup, use the SQL Server Replication to replicate Unified CCDM databases. Replication between these databases is set up and monitored using the Replication Manager application which is available in the Unified CCDM Integrated Configuration Environment (ICE).

Complete the procedures to configure replication in a dual-sided Unified CCDM deployment setup.

### Procedure

**Step 1** Launch the Integrated Configuration Environment on Unified CCDM Database Server Side A. For more information, see Launch the Integrated Configuration Environment, on page 209.

**Step 2** In the left pane, select **Tool** and select **Replication Manager** from the drop-down list.

**Step 3** Configure setup to enable SQL Server Replication for the Unified CCDM databases in a dual-sided environment. For more information, see Setup, on page 211.

**Step 4** Configure monitor to check the general health of SQL Server Replication between Unified CCDM databases. For more information, see Monitor, on page 212.

### Setup

The Setup option configures or disables SQL Server Replication for the Unified CCDM databases in a dual-sided environment.

#### Procedure

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

**Step 2** In the CCDM Database Server Properties, the Server Name and Catalog Name for each are defaulted to the values used when the Unified CCDM servers were configured with the ICE Cluster Configuration tool.

**Step 3** In Distributor Properties, by default, the Distributor is created on the Unified CCDM Database Subscriber Server.

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

**Note** After replication, all options are greyed out except **Disable** button.

### Monitor

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

#### Procedure

**Step 1** Select **Monitor** tab.

**Step 2** After Unified CCDM is replicated, top-left pane shows the list of **Publishers** and Publications of each Publisher.

**Step 3** Select publications to see either **Subscriptions** or **Agents** details.
**Agents** tab lists **Snapshot Agent**, **Log Reader Agent** and **Queue Reader Agent**, if available for the selected publication.

**Step 4** Select subscriptions or agents to see their session details in the bottom left pane.
This pane lists all the agent sessions in the last 24 hours. Click each session to see the performed actions during the session. It also provides information about agents failure.

**Note** To start or stop the replication agents, select **Agents** tab, right-click **Status** of the agent and select **Start** or **Stop** replication agents.

## Login to Unified CCDM

#### Procedure

**Step 1** In the App/Web server, open **Domain Manager** application or enter *https://<webserver FQDN>/Portal* in browser.
Displays Unified CCDM web page.

**Step 2** For login to a new system, use the username 'Administrator' and a blank password. You are prompted to change the administrator password. If you logged into an upgraded system, enter the password that you created when you first logged in. Re-enter the password to confirm.

## Configure Single Sign-On

By default, users must log in to Unified CCDM every time they connect. You can optionally configure Unified CCDM to use Single Sign-On (SSO), which allows users to connect to Unified CCDM without logging in by linking their Unified CCDM user accounts with their Active Directory user accounts.

**Note** Users cannot use SSO over a proxy connection. Setting up SSO disables any existing Unified CCDM users that are not in domain login format. You must set up new Unified CCDM user accounts for all existing users.

## Setup Administrator Account

It is important to set up the new SSO administrator account correctly, because the Unified CCDM administrator account is disabled when SSO is configured. Complete the following procedure to administrator account setup.

### Before You Begin

Create users in active directory, see Create Users in Active Directory, on page 463.

### Procedure

**Step 1** In the CCDM Web Server, open the Domain Manager. Log in to Unified CCDM as Administrator.

**Step 2** In **Security** > **Users**, create a user account to be the new administrator account.

**Note** For the login name, use the format <DOMAIN>\<your domain login>, for example, ACMEDOM\jsmith.

**Step 3** Enter the password, re-enter and confirm the password.

**Step 4** Check the **Advanced** mode check box.

**Step 5** Click **Save**.

**Step 6** Click on the newly created user and choose **Groups** tab.

**Step 7** Click **Add to Group**.

**Step 8** Check the **Administrators** group check box and click **Ok**.

**Step 9** Click **Save**.

## Configure SSO Authentication for Unified CCDM

Complete the following procedure to configure SSO authentication for Unified CCDM.

### Procedure

**Step 1** Launch **Integrated Configuration Environment** on CCDM Database Server Side A, see Launch the Integrated Configuration Environment, on page 209.

**Step 2** Select **System Properties** in the Tools drop-down list in the Integrated Configuration Environment.

**Step 3** In the Global properties tab, navigate to **Login Authentication Configuration group** > **Login Authentication Mode property**.

**Step 4** Using the drop-down against the property value, change the value from **Portal** to **Active Directory**.

**Step 5** Save the configuration changes, and click **Exit**.

**Step 6** On the Application and Web server, navigate to the location where Unified CCDM is installed (usually C:\Program Files\Domain manager ). Right-click the Web folder and click **Properties**.

**Step 7** Select the Security tab and ensure that all the domain users have both Read, Read and Execute permissions on this folder.

**Step 8** Click **Advanced** settings. Ensure that **Replace all child object-permission entries with inheritable permission entries from this object** is selected. If not, click **Change Permissions**, select the option and click **OK**.

**Step 9** Click **OK** to close the properties dialog.

**Step 10** Run `iisreset` command, from a command window for all CCDM servers.

**Note** Users will now be able to access Unified CCDM directly from their domain account without logging in again.

## Manage Users with Single Sign-On

After you set up, assign all the Unified CCDM users with a Unified CCDM login in the format <DOMAIN>\<Windows domain login>. This implies that you must re-create the previously existing Unified CCDM user accounts in the new format before any users can log in.

Each time you give a new user a Unified CCDM account, you must give Read/Read & Execute properties on the Web directory, or you must add that user to a user group that has those permissions.

The first time a user access Unified CCDM using SSO, a dialog box may appear requesting for Windows username and password. To sign in automatically, the user will have to add the Unified CCDM website to the list of local intranet sites in their browser.

Administrator can create Users for the tenant that is created. See, Configure User, on page 504.

### What to Do Next

- Obtaining Digital Certificate, on page 214
- Installing the Security Certificate in the User Certificate Store , on page 220
- Installing the Security Certificate in the Computer Certificate Store, on page 220

### *Obtaining Digital Certificate*

Perform the following procedures to obtain the digital certificate.

- Install Active Directory Certificate on Domain Controller Box, on page 215
- Install Active Directory Certificate on CCDM Web Server and Data Server, on page 215

• Install Active Directory Certificate on CCDM Web Server., on page 216

Install Active Directory Certificate on Domain Controller Box

### Before You Begin

Select **Start** > **Administrative Tools** > **Server Manager** > **Roles** and expand, if the Active Directory Certificate services are present, see Installing the Security Certificate in the User Certificate Store , on page 220

If the Active Directory Certificate is not present then perform the following steps to install the Active Directory Certificate Services.

### Procedure

**Step 1** Select **Server Manager** > **Roles** > **Summary** and click **Add Roles** and click **Next**.

**Step 2** Check **Active Directory Certificate Services** check-box on **Select Service Roles** page and click **Next**.

**Step 3** Check **Certification Authority** check-box and click **Next**.

**Step 4** Select **Enterprise Type** in Specify Set Up type page and click **Next**.

**Step 5** Select **Create New Private Key** in Set Up Private Key page and click **Next** until the installation begins

**Note** CA Name is the Name of the Certificate i.e its the Name of the Domain Controller box.

**Step 6** Click **Close**.

**Step 7** In the command prompt, type **mmc** in the command box to open Microsoft Management Console (MMC).

**Step 8** Click **File** > **Add/Remove Snap-in** > **Certificates** > **Add** .

**Step 9** In the Certificates Snap-in dialogue box, select **Computer Account** and click **Next**.

**Step 10** In the Select Computer dialogue box, select **Local Computer** option and click **Finish** and click **OK**.

**Step 11** Expand the Certificates node and Trusted Root Certificate node, click **Certificates** to see the available certificates. Right-click on the certificate that you created through Creating the Active Directory Certificate Services.

**Step 12** Right-Click on selected Certificate and click **All Tasks** and click **Export** .

**Step 13** Accept the default format and click **Next**.

**Step 14** Specify a file name and click **Next** and click **Finish**.

**Step 15** Copy the Certificate that you have exported into CCDM web Servers and Data Servers box.

Install Active Directory Certificate on CCDM Web Server and Data Server

### Procedure

**Step 1** In command prompt type **mmc** and open the MMC.

**Step 2** Click **File** > **Add/Remove Snap-in** > **Certificates** > **Add**.

**Step 3** Select Computer Account and click **Next**.

**Step 4** Select Local computer and click **Finish** and click **OK**.

Certificates snap-in will be added to MMC

**Step 5** Expand the Certificates (Local Computer) node Trusted Root Certificate Authorities node, right-click **Certificates** and select **All Tasks** > **Import**.

**Step 6** In the Certificate Import Wizard, click **Next**.

**Step 7** Browse to the certificate file you copied from Domain Controller and click **Open** and then click **Next** .

**Step 8** Select **Place all certificates in the following store** and then browse and locate the Trusted, click **Next** and click **Finish**

**Step 9** Reboot the server.

Install Active Directory Certificate on CCDM Web Server.

### Procedure

**Step 1** Open Internet Information Services (IIS) Manager and select the web server in the folder hierarchy.

**Step 2** Select the **Features View** tab, click **Server Certificates**.

**Step 3** Create a digital certificate in one of the following ways:

a) Select Create Domain Certificate in the Actions pane to display the Distinguished Name Properties dialog box.

b) In the Common Name field, enter the fully qualified domain name of the web server. For example, if your your web server is WEBSERVER and your domain name is UCCDMDOM.LOCAL, enter WEBSERVER.UCCDMDOM.LOCAL. If you have a loadbalancedsystem, this must be the domain name of the load balanced node, not the domain name of any of the individual servers.

c) Complete the other fields as appropriate, and click **Next**.

d) In the Online Certification Authority dialog box specify the Online Authority and a Friendly Name. Click **Finish**.

### What to Do Next

- Configure SSL for Unified CCDM, on page 216
- Grant Network Service Rights to the Certificate, on page 217
- Obtain the Certificate Thumbprint, on page 217
- Configure Web Services to Use the Certificate, on page 218
- Test the Certificate Installation, on page 219

Configure SSL for Unified CCDM

After you have a suitable digital certificate, configure SSL for Unified CCDM. On the App/Web Server

### Procedure

**Step 1** Open Internet Information Services (IIS) Manager , expand the folder tree below the web server and select the web site that the Unified CCDM web application resides on.

**Step 2** In the Actions pane, select **Edit Site** > **Bindings** to display the Site Bindings dialog box.

**Step 3** If there is no existing binding for https, click **Add** to display the Add Site Binding dialog box.

a) Set the IP Address to All Unassigned , and Port to 443 , unless your system has been set up differently. If you are note sure, contact your system administrator.

b) Set SSL Certificate to point to your certificate and click **OK**.

**Step 4** If there is an existing binding for https, select it and click Edit to display the Edit Site Binding dialog box, edit the settings to the values in step 3. above and click **OK** .

**Step 5** In the folder tree, select the **Portal Application**.

**Step 6** Select the **Features View** tab, and click on **SSL Settings in the IIS group**.

**Step 7** Select the Require SSL, and retain the default Ignore for Client Settings

**Step 8** In the Actions pane, click **Apply** to apply these settings.

**Step 9** Close IIS Manager.

## Grant Network Service Rights to the Certificate

Grant Network Service Rights to the Certificate to grant network service rights to the certificate, on the App/Web Server:

### Procedure

**Step 1** In the Start menu, type mmc in the command box to open Microsoft Management Console (MMC).

**Step 2** Click **File** > **Add/Remove Snap-in** > **Certificates** , then **Add** .

**Step 3** In the Certificates Snap-in dialog box, select Computer Account and click **Next** .

**Step 4** In the Select Computer dialog box, select **Local Computer** and click **Finish** to add the Certificates snap-in to MMC. Click **OK** .

**Step 5** In MMC, expand the Certificates node and the Personal node, then click **Certificates** to see the available certificates.

**Step 6** Right-click on the certificate you want to use, select **All Tasks** > **Manage Private Keys** .

**Step 7** In the Permissions for Private Keys dialog box, click **Add**.

**Step 8** In the Select Users, Computers, Service or Groups dialog box, type NETWORK SERVICE , then click **Check Names**. The name will be underlined if it has been entered correctly. Click **OK** .

**Step 9** In the Permissions for Private Keys dialog box, select the NETWORK SERVICE user, then in the Full Control row, select the check box in the Allow column. Click **OK** .

## Obtain the Certificate Thumbprint

To obtain the certificate thumbprint, on the App/Web Server:

### Procedure

**Step 1** In MMC, expand the Certificates node and the Personal node to see the available certificates and select the certificate you want to use.

**Step 2** Double-click on the **Certificate**.

**Step 3** In the Certificate dialog box, select the Details tab, and click **Thumbprint**.
The thumbprint for this certificate is displayed on the lower part of the screen as a text string.

**Step 4** Select the thumbprint text string, copy it and paste it into a text editor. Edit the string to remove all the spaces. For example, if the thumbprint text string you copied was: c3 34 9a 43 28 d3 a7 75 a9 93 eb 31 5c bf e0 62 51 6d b8 18 you need to edit it to become: c3349a4328d3a775a993eb315cbfe062516db818
Save this thumbprint value as you will need it several times in the next step.

## Configure Web Services to Use the Certificate

To configure Web Services to use the certificate, on the App/Web Server:

### Procedure

**Step 1** Use Windows Services or the Service Manager in the ICE tool (see the *Administration Guide for Cisco Unified Contact Center Domain Manager* ) to stop all Unified CCDM services.

**Step 2** Enter the following commands to remove the existing localhost certificates for each Web Services:

- **subscription manager**

  **netsh http delete sslcert ipport**=*0.0.0.0:8083*

- **resource manager**

  **netsh http delete sslcert ipport**=*0.0.0.0:8085*

- **analytic data**

  **netsh http delete sslcert ipport**=*0.0.0.0:8087*

**Step 3** Enter the following commands to add the new certificates for each Web Services:

- **subscription manager**

  **netsh http add sslcert ipport**=*0.0.0.0:8083* **certhash**=<*thumbprint*> **appid**=*{16dde36c-787e-4dc7-bdc0-fd4ae0eb189a}*

- **resource manager**

  **netsh http add sslcert ipport**=*0.0.0.0:8085* **certhash**=<*thumbprint*> **appid**=*{16dde36c-787e-4dc7-bdc0-fd4ae0eb189a}*

- **analytic data**

  **netsh http add sslcert ipport**=*0.0.0.0:8087* **certhash**=<*thumbprint*> **appid**=*{16dde36c-787e-4dc7-bdc0-fd4ae0eb189a}*

**Example:**
Consider thumbprint value from the section 6.2.5 and obtain the certificate thumbprint to update subscription manager certificate, enter the following command:

**netsh http add sslcert ipport**=*0.0.0.0:8083* **certhash**=*c3349a4328d3a775a993eb315cbfe062516db818* **appid**=*{ 16dde36c-787e-4dc7-bdc0-fd4ae0eb189a}*

**Note** Do not alter the appid value in the commands above.

Test the Certificate Installation

On the local Machine, copy the Certificate that you have exported from Domain Controller box and perform the following procedure.

### Before You Begin

To test the certificate installation, in Internet Explorer, navigate to each of the locations below, where <Server> is the name of the App/Web Server.

Check that the page opens without a certificate warning, and that the address bar shows a green safe status.

```
https://<Server>:8083/SubscriptionManager?wsdl
https://<Server>:8085/ResourceManagement?wsdl
https://<Server>:8086/HierarchyManagement?wsdl
https://<Server>:8087/AnalyticData?wsdl
```

### Procedure

**Step 1** Enter mmc in the command box to open MMC.

**Step 2** Click **File** > **Add/Remove Snap-in** > **Certificates** > **Add**.

**Step 3** In the Certificates Snap-in dialogue box, select Computer account and click **Next**.

**Step 4** In the Select Computer dialogue box, select Local computer and click Finish to add the Certificates snap-in to MMC. Click **OK**.

**Step 5** In MMC, expand the Certificates (Local Computer) node Trusted Root Certificate Authorities node, then right-click **Certificates** and select **AllTasks** > **Import**.

**Step 6** In the Certificate Import Wizard, click **Next**.

**Step 7** In the File to Import dialogue box, browse to the certificate file you copied from DC and click Open and then click **Next**.

**Step 8** In the Certificate Store dialogue box, select the option, Place all certificates in the following store, then Browse and locate the Trusted Root Certificate Authorities store and click OK.

**Step 9** In the Certificate Store dialogue box, click **Next**. Review the settings and click **Finish**.
Repeat the steps given in section Test the Certificate Installation.

### *Installing the Security Certificate in the User Certificate Store*

To install the Unified CCE ConfigWebService security certificate in the user certificate store, you need to locate the certificate and import it into your certificate store on each Unified CCDM database server.

#### Procedure

**Step 1** Choose **Start** > **All Programs** > **Domain Manager** > **Configuration Tools** > **Integrated Configuration Environment** to start ICE.

**Step 2** Enter the credentials for your database. Click **OK** if there is any warning or error message displayed.

**Step 3** In the ICE Cluster Configuration tool, select the **Resources** tab and navigate to the Unified CCE instance. Select the **Components** tab. From this you can determine the URL of the Unified CCE ConfigWebService.

**Step 4** In Internet Explorer, navigate to the URL you found above. If the certificate has not been installed on this server, you will see a certificate error.

**Step 5** Click **Certificate Error** in the top right hand corner of the window.

**Step 6** In the Untrusted Certificate dialog box, select **View Certificates**.

**Step 7** In the Certificate dialog, note the "Issued to:" name (you will need this name to locate the certificate again below) and click **Install Certificate**.

**Step 8** In the Certificate Import Wizard, click **Next**.

**Step 9** In the Certificate Store dialog box, select **Place all certificates in the following store**, and click **Browse**. Choose **Trusted Root Certificate Authorities** and click **OK** to return to the Certificate Store dialog box.

**Step 10** In the Certificate Store dialog box, click **Next.** Review the settings and click **Finish**.

**Step 11** Click **OK** if there is any warning or error message displayed. When the import completes, click **OK**.

### *Installing the Security Certificate in the Computer Certificate Store*

To install the Unified CCE ConfigWebService Security Certificate in the computer's certificate store, you need to export the security certificate from the user certificate store that you saved and import it into the computer certificate store.

- To Export the Certificate, on each CCDM database server , on page 220
- To Import the Certificate, on each CCDM database server, on page 221

To Export the Certificate, on each CCDM database server

### Procedure

**Step 1** Enter **mmc** in the command box to open Microsoft Management Console (MMC).

**Step 2** Click **File** > **Add/Remove Snap-in**>**Certificates**> **Add**.

**Step 3** In the Certificates Snap-in dialog box, select **My user account** and click **Finish** and Click **OK**.

**Step 4** In MMC, expand the Certificates - Current User node, Trusted Root Certificate Authorities node, then click **Certificates** to see the available certificates.

**Step 5** Locate the certificate you imported in the section above, right-click on it, and select **All Tasks** > **Export** .

**Step 6** In the Certificate Export Wizard, select **Next**.

**Step 7** In the Export File Format dialog box, accept the default format and click **Next**.

**Step 8** In the File to Export dialog box, specify a file name and click **Next**. Review the settings and click **Finish**.

To Import the Certificate, on each CCDM database server

### Procedure

**Step 1** Enter **mmc** in the command box to open MMC.

**Step 2** Click **File** > **Add/Remove Snap-in** > **Certificates**>**Add**.

**Step 3** In the Certificates Snap-in dialog box, select **Computer account** and click **Next**.

**Step 4** In the Select Computer dialog box, select **Local computer** and click **Finish** to add the Certificates snap-in to MMC. Click **OK**.

**Step 5** In MMC, expand the Certificates (Local Computer) node Trusted Root Certificate Authorities node, then right-click **Certificates** and select **All Tasks** > **Import**.

**Step 6** In the Certificate Import Wizard, click **Next**.

**Step 7** In the File to Import dialog box, browse to the certificate file you exported and click **Open** and then click **Next**.

**Step 8** In the Certificate Store dialog box, select the option, **Place all certificates in the following store**, then **Browse** and locate the Trusted Root Certificate Authorities store and click **OK**.

**Step 9** In the Certificate Store dialog box, click **Next.** Review the settings and click **Finish**.

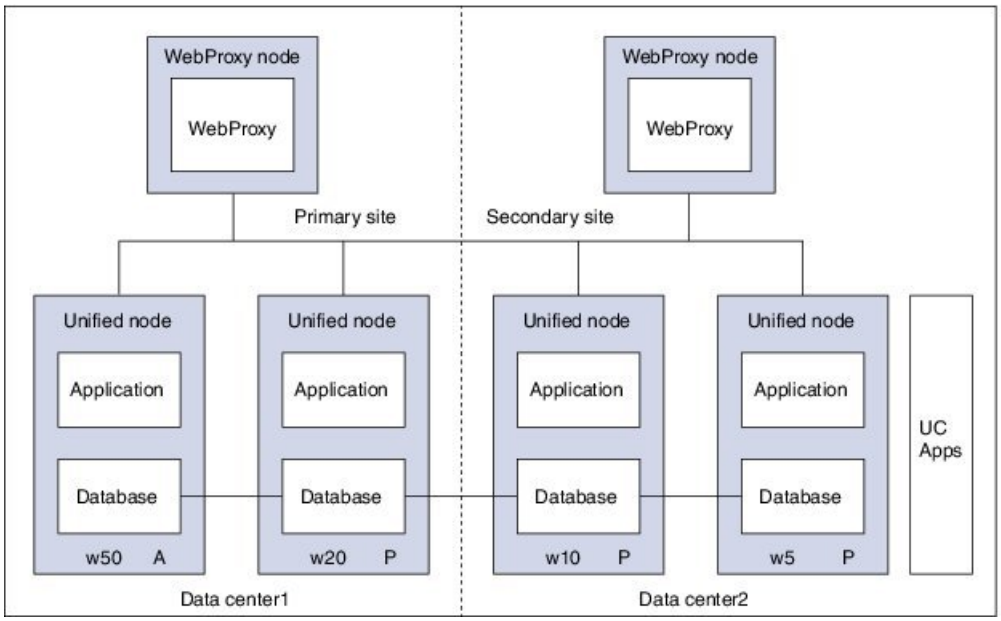
# Install and Configure Unified Communication Domain Manager

For Cisco HCS for contact center, implements a multinode deployment as shown in the following figure. This deployment VOSS recommends to install four (or more) Unified instances and two (or more) WebProxy instances are clustered and split over two different geographical locations to provide high availability and disaster recovery.

- A WebProxy role installs only the front-end web sever together with ability to distribute load among multiple middleware nodes
- A Unified node comprises Application and Database roles on a single node

- WebProxy and Unified nodes can be contained in separate firewalled networks
- Database synchronization takes places between all Database roles, thereby offering Disaster Recovery and High Availability
- All nodes in the cluster are active

***Figure 59: Graphical Representation of Geo-redundant cluster***




Following are the functional roles of each node:

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

Following are the procedures to install and configure Unified Communication Domain Manager:

- Install Unified Communication Domain Manager, on page 223
- Post Installation , on page 223
- Install Hosted Collaboration Mediation-Fulfilment, on page 225
- Prerequisites to Configure Unified Communication Domain Manager, on page 226

# Install Unified Communication Domain Manager

### Procedure

**Step 1** After obtaining the OVA file from Cisco.com, deploy the OVF template from the vSphere Client. The setup file contains the OVA file along with software and platform upgrade files.

**Step 2** Power on the virtual machine (VM).
The Setup wizard starts to configure the system.

**Step 3** Choose each options and provide the necessary details:

a) Choose **ip** and enter the IP address.
b) Choose **netmask** and enter the network mask for the Cisco Unified Communications Domain Manager.
c) Choose **gateway** and enter the IP address of the Gateway.
d) Choose **dns** and enter the Dns server address.
e) Choose **ntp** and enter the ntp server address.
f) Choose **hostname** and enter the hostname.
g) Choose **role** and choose the required option. Choose **Unified** to unified instances. Choose **WebProxy** to Webproxy instances.
h) Choose **datacentre** and enter the name of datacentre.
i) Choose **platform** and enter the password.

**Note** Platform password must be at least 8 characters long and must contain both upper and lowercase letters and at least one numeric or special character.

**Step 4** Choose **install**.

# Post Installation

### Procedure

**Step 1** Login to each node and update security.

a) execute: security check
b) execute: security update

**Example:**

```
platform@cucdm-tb3-un-01:~$ security check
There are 181 security updates available
Please install them with: security update
platform@cucdm-tb3-un-01:~$ security update
```

**Note** Enter the command `system reboot` to restart all the nodes after security patches are installed.

**Step 2** To open ports for Cluster Communication:

a) Enter `cluster prepnode` command on all unified nodes.

```
platform@tesla-cucdm-u3:~$ cluster prepnode
You are about to add this node to a cluster as a web proxy
```

```
Do you wish to continue? y
platform@tesla-cucdm-u3:~$
```

b) Enter `web cluster prepnode` command on all webproxy nodes.

```
platform@tesla-cucdm-u3:~$ web cluster prepnode
You are about to add this node to a cluster.
Do you wish to continue? y
platform@tesla-cucdm-u3:~$
```

**Step 3** Add nodes to Cluster. Perform the following on one of the node:

a) Login to one of the unified node.

b) Enter `cluster add <ip address>` command to add other nodes including WebProxy.

c) Enter `cluster list` command. Displays a list of nodes in the cluster.

**Step 4** Add Network Domain:

a) Enter `cluster run all network domain <domain-name>` command to configure domain.

**Note** Skip this step if already configured during installation.

b) Enter `cluster run all network domain` command to check configured network domain.

c) Enter `cluster run all network dns` command to check the status of DNS config.

d) Enter `cluster run all diag ping <ip address of each node>` command to check reachability of all nodes.

e) Optional, enter `cluster run all system shutdown` command to shut all the nodes down gracefully and take a snapshot.

**Step 5** Provision cluster:

**Note** Provision takes long time depending on number of nodes since VOSS provisions each one sequentially. Approximately 4-5 hours for 2 WebProxy and 4 Unified nodes.

a) Enter `database weight add <database-ip> <priority>` command to add weight to all database servers.

**Note** Higher the value, more the priority. Weights of 4, 3, 2, and 1 are recommended for the 4 Unified nodes.

b) Enter `cluster provision primary <ip of primary database node> fast` command to provision all the nodes.

**Note** Make sure to run above command only when all the nodes are added to the cluster.

c) Enter `cluster status` command to view the status of the cluster. If any of the services are down, enter `cluster run all app start all` command to restart the service on the problematic node.

d) Optional, enter `cluster run all system shutdown` command shut all the nodes down gracefully and take a snapshot.

**Step 6** Enter `voss cleardown` command to initialize and clear the cache.

**Step 7** Import template:

a) Access any unified node using SFTP to copy <template-file> to media.

b) Login to node and enter `app template media/<template-file>` command to import the template.

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

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

# Install Hosted Collaboration Mediation-Fulfilment

The Fulfillment service responds to data changes in the Shared Data Repository related to the Cisco Unified Communication Manager.

The Cisco HCM-F administrative interface is the user interface to the Cisco HCM-F services. It allows you to perform management and configuration tasks on the Cisco HCM-F services.

### Procedure

**Step 1** After obtaining the OVA file from Cisco.com, deploy the OVF template from the vSphere Client. The setup file contains the OVA file along with software and platform upgrade files.

**Step 2** Choose **HCM-F APP** from **Configuration** drop-down list.

**Step 3** Power on the virtual machine (VM) and open the console.
The Setup wizard starts to configure the system.

**Step 4** On **Media Check** screen, click **OK** to perform a check of the media, or click **Skip** to proceed to the installation.

**Step 5** On **Product Deployment Selection** screen, choose **HCS Application Suite** and then click **OK**.

**Step 6** On **Proceed with Install** screen, verify that you are installing the version you want, and click **Yes** to overwrite the hard drive.

**Step 7** On **Platform Installation Wizard** screen, choose **Proceed**.

**Step 8** On **Basic Install** screen, click **Continue**.

**Step 9** On **Timezone Configuration** screen, choose your time zone from the list, and then click **OK**.

**Step 10** On **Auto Negotiation Configuration** screen, click **Continue**.

**Step 11** On **MTU Configuration screen**, click **No** to leave the MTU size at the OS default, or click **Yes** and enter new values.

**Step 12** On **DHCP Configuration** screen, click **No** to use a static IP address. On **Static Network Configuration** page, enter **Host Name**, **IP Address**, **IP Mask**, **GW Address** and click **Ok**.

**Note** The virtual machine must be able to reach the gateway that is entered for the static configuration, or else the installation will give an error and not proceed.

**Step 13** On **DNS Client Configuration** screen:

a) Click **Yes** to use DNS. Enter values for **Primary DNS**, **Secondary DNS** (optional), and **Domain**.

b) Click **No** to not use DNS.

**Note** If the hostname of the Cisco HCM-F server is not resolvable using the specified DNS server because, the virtual machine cannot reach the DNS server, then the installation gives an error and does not proceed.

**Step 14** On **Administrator Login Configuration** screen, set up **Administrator ID** and **Password** for the AppNode. Then click **OK**.

**Step 15** On **Certificate Information** screen, enter values for Organization, **Unit**, **Location**, and **State**. Choose **Country** from the menu. Then click **OK**.

**Step 16** On **Network Time Protocol Client Configuration** screen, enter hostname or IP address for one to five NTP Servers. Then click **OK**.

**Step 17** On **Security Configuration screen** set the **system security password** for the App Node. Then click **OK**.

**Step 18** On **Platform Configuration Confirmation** screen, click **OK**.
After installation, it displays login console.

# Prerequisites to Configure Unified Communication Domain Manager



## Add HCM-F Device

### Procedure

**Step 1** Login to Cisco Unified Communications Domain Manager as admin.

**Step 2** Create a new HCM-F instance:

a) Navigate to **Device Management** > **HCM-F** and click **Add**.
b) Enter **HCM-F Host IP Address**.
c) Enter **HCM-F Admin Username**.
d) Enter **HCM-F Admin Password**.
e) Re-enter the admin password.
f) Retain the default base URL.
g) Choose **v10_6 from HCM-F Version** from the drop-down list.
h) Click **Save**.

**Step 3** Verify the connection:

a) Navigate to **Device Management** > **Advanced** > **HCM-F Network Device**.
b) Click **HCM-F instance**.
c) Navigate to **Action** > **Test Connection**.

## Add Provider

### Procedure

**Step 1** Login to Cisco Unified Communication Domain Manager as admin.

**Step 2** Navigate to **Provider Management** > **Providers**.

**Step 3** Click **Add**.

**Step 4** Provide necessary details in the following:

a) Enter **Name**.
b) Enter **Description**.
c) Enter **Domain Name**.

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

**Step 5** Click **Save**.

## Add Reseller

### Procedure

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

**Example:**
<provider_name>Admin@<domain_name>.

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

**Step 3** Click **Add**.

**Step 4** Provide necessary details in the following:

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

**Step 5** Click **Save**.

### What to Do Next

To integrate Unified Communication Domain Manager with the customer instance, see Cisco UCDM Integration, on page 473.

# Install and Configure ASA Firewall and NAT

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

# Setup ASA

Complete the following procedure to initiate the basic setup in Cisco ASA.


- Access Command-line Interface, on page 228
- Configure Hostname and Password, on page 228


## Access Command-line Interface

### Procedure

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

**Step 2** Press Enter.

Displays the following prompt:

```
hostname>
```

This indicates you are in user EXEC mode.

## Configure Hostname and Password

### Procedure

**Step 1** Enter the following commands to access privileged EXEC mode:

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

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

**Step 2** Enter the following commands to access the global configuration mode:

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

**Step 3** Enter `hostname` command to configure the hostname:

**Example:**

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

**Step 4** Enter `enable passsword` command to configure the password:

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

**Example:**

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

**Step 5** Enter the following commands to save configuration:

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

# Configure Multiple Context Modes

Complete the following procedures to configure multiple context modes on ASA Firewall:

- Enable Multiple Context Modes, on page 229
- Enable Interfaces in the System Execution Space, on page 229
- Configure Security Contexts in System Execution Space, on page 230
- Assign MAC Addresses to Context Interfaces Automatically (Optional), on page 230
- Configure Interfaces in the Context, on page 230

## Enable Multiple Context Modes

### Procedure

Enter the following commands:

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

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

## Enable Interfaces in the System Execution Space

Complete the following procedure to configure interfaces in the system execution space:

### Procedure

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

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

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

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

## Configure Security Contexts in System Execution Space

Complete the following procedure to configure security contexts:

### Procedure

**Step 1** Configure the admin context name in the global configuration mode:
```
hostname(config)#admin-context admin
```

**Step 2** Navigate to the context admin:
```
hostname(config)#context admin
```

**Step 3** Configure the admin context definitions:
```
hostname(config-ctx)#description admin Context for admin purposes
```
a) Allocate interface management 0/0 for admin context.
```
hostname(config-ctx)#allocate-interface management0/0 invisible
```
b) Create `admin.cfg` in disk 0.
```
hostname(config-ctx)#config-url disk0:/admin.cfg
```

## Assign MAC Addresses to Context Interfaces Automatically (Optional)

Complete the following procedure to automatically assign MAC addresses to context interfaces:

### Procedure

Enter the following command in configure mode to automatically assign MAC addresses to context interfaces:
```
hostname(config)#mac-address auto
```

## Configure Interfaces in the Context

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

### Procedure

**Step 1** Navigate to admin context in configure mode:
```
hostname#changeto context admin
```

**Step 2** Navigate to the interface management:
```
hostname/admin#configure terminal
hostname/admin(config)#interface management 0/0
```

**Step 3** Enter a name for management interface of the admin context:
```
hostname/admin(config-if)#nameif management
```
Enter the IP address of the management interface:
```
hostname/admin(config-if)#ip address ip_address subnet_mask
hostname/admin(config-if)#exit
```

**Example:**

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

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

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

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

b) Save the RSA keys to persistent flash memory.

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

c) Enables local authentication for SSH access.

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

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

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

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

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

**Example:**

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

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

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

g) Enable HTTPS server and default port is 443.

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

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

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

i) Enter Default Static Route.

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

**Example:**

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

### What to Do Next

To integrate Cisco ASA with the customer instance, see ASA Integration, on page 476.

# Install and Configure Perimeta SBC

This section describes the steps to deploy Perimeta SBC for HCS deployment model. For HCS, it is validated on C-Series platform.

Perimeta SBC performs address translation and the media anchor role for inter-enterprise and off net Calls. Each sub customer CUCMs forward inter-enterprise and off-net calls to Perimeta SBC over SIP trunks, which in turn forward the calls to Carrier-Network. Perimeta SBC also receives calls from Carrier-Network and forwards the calls to each sub customer CUCM's. Routing decisions inside Perimeta SBC are based on source adjacency (to the SIP trunk from which the call was received), so Perimeta SBC maintains adjacency relationships to all sub customer components (CUCM, MediaSense), shared core components (CUBE (E), CVP Server's) and Carrier-Network. Perimeta SBC is manually provisioned using IOS CLI.

# Hardware Specification

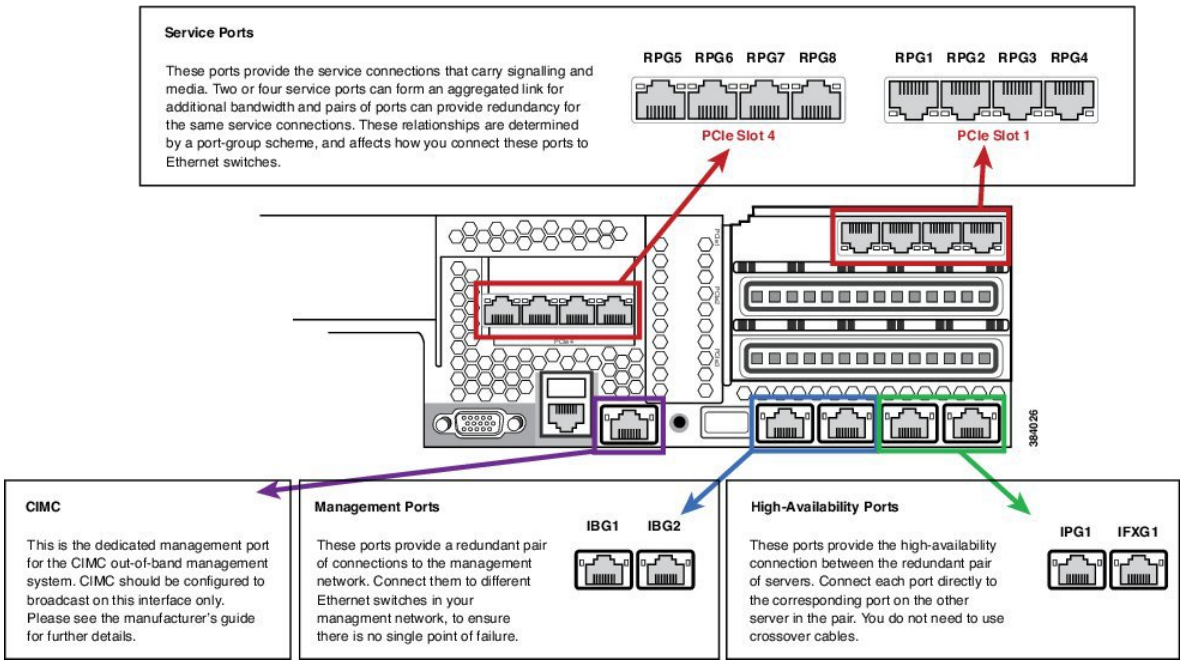
This section provides an information on how to get the Cisco C240 M3 platform ready to install with Perimeta. It covers the Perimeta-specific cabling and the BIOS settings required by Perimeta.

Cisco C240 M3 Network interfaces should have a total of 13 NICs. This includes:

- Four embedded 1Gb Ethernet ports
- CIMC out-of-band hardware management port
- Eight 1 Gb Ethernet ports, made available from two PCIe cards
  - 4 ports on a card installed in PCIe slot 1
  - 4 ports on a card installed in PCIe slot 4

The below figure shows the locations of the network interfaces on a Cisco C240 M3 blade, and how Perimeta labels and uses them.

***Figure 60: Cisco C240 M3 Network Interface Port Layout***



# CIMC Setup

Use a VGA monitor and a USB keyboard to get direct console access, and use this to configure CIMC. On system boot select CIMC configuration (press F8 at the relevantprompt).

Configure CIMC with a dedicated IP address and subnet configuration, and with a user/password. It also should be configured to be accessible through only the dedicated management port. For more information, see the Cisco CIMC documentation.

# Advanced BIOS Configuration

Set the advanced BIOS configuration to match that specified in table below. This is required to ensure that the Perimeta system performs at full capacity at all times.

Advanced BIOS configuration can be set in the CIMC over HTTPS.

| Field | Value |
|---|---|
| ASPM Support | Disabled |
| Intel(R) VT-d ATS Support | Enabled |
| Adjacent Cache Line Prefetcher | Enabled |
| NUMA | Enabled |
| Power Technology | Energy Efficient |
| Channel Interleaving | Auto |
| Intel(R) VT-d Coherency Support | Disabled |
| Number of Enabled Cores | All |
| Energy Performance | Performance |
| Frequency Floor Override | Enabled |
| CPU Performance | HPC |
| DRAM Clock Throttling | Performance |
| DCU IP Prefetch | Enabled |
| DCU Streamer Prefetch | Enabled |
| Demand Scrub | Enabled |
| Direct Cache Access Support | Enabled |
| Onboard SCU Storage Support | Disabled |
| DRAM Refresh Rate | 2x |
| Enhanced Intel Speedstep(R) Tec | Enabled |

# Install Perimeta SBC

This section provides a brief overview and describes the minimal steps to deploy Perimeta SBC for HCS deployment models.

| Sequence | Task | Done |
|---|---|---|
| 1 | Mount Perimeta ISO, on page 234 | |
| 2 | Configure the Management Network, on page 235 | |
| 3 | Configure DNS Servers, on page 235 | |
| 4 | Unpack the Software, on page 236 | |
| 5 | Configure System, Node, and Remote Node Names, on page 236 | |
| 6 | Managing Local Timezone, Time and Date, and NTP Server, on page 236 | |
| 7 | Commissioning and Partnering the System, on page 237 | |
| 8 | Apply Licenses, on page 237 | |

## Mount Perimeta ISO

### Procedure

**Step 1** Log in to **Cisco Integrated Management Controller**.
**Step 2** Click **Power on** to turn on the server.
**Step 3** Select **Virtual Media** > **Activate Virtual Devices**.
**Step 4** Select **Accept this Session** option and click **Apply**.
**Step 5** Select **Virtual Media** > **Map CD/DVD**.
**Step 6** Click **Browse** and select the ISO location.
**Step 7** Click **Map Device**.
**Step 8** Press Enter to boot from the mapped ISO.
Installation begins.
**Step 9** After the installation, restart the server.

## Configure the Management Network

### Procedure

**Step 1** Login to Craft Console using the default username and password.
The default username is defcraft and password is !defcraft.

**Step 2** Choose **Admin** > **Management** > **Set IP**.

**Step 3** Enter the Management IP address and Subnet mask, Press **Enter**.

**Step 4** Enter the Processor A management IP address, Processor A probing IP address for management port 1, Processor A probing IP address for management port 2.

**Step 5** If your Session Controller has two processors, enter the Processor B management IP address, Processor B probing IP address for management port 1, Processor B probing IP address for management port 2.

**Step 6** Enter the management network default gateway IP address, then press **Enter**.

**Step 7** The following are optional configurations, if you have chosen not to configure a value for this address then press **Enter**.

a) Enter the first connectivity test IP address
**Note** We suggest that you do configure at least one connectivity test IP address.

b) Enter the second connectivity test IP address
c) Enter the third connectivity test IP address

**Step 8** The Craft terminal shows a summary of your selections, choose **OK**.

## Configure DNS Servers

### Procedure

**Step 1** Select **DNS**.

**Step 2** Select **Set DNS info**.

**Step 3** Enter the IP address of primary DNS Server, secondary server.

**Step 4** Choose **OK**.

## Unpack the Software

### Procedure

**Step 1** Download the software and upload it to /ftp/software/ path on the C240 server.

**Step 2** Choose **Software** > **Manage versions** > **Verify/unpack** and choose **Ok**.

**Step 3** Select the software to be unpacked from the list and choose **Ok**.

## Install Software

### Procedure

**Step 1** Choose **software** > **upgrade** > **start upgrade** and choose **OK**.

**Step 2** Select an appropriate version.

**Step 3** Press **Enter**.

**Step 4** Choose **yes**.

## Configure System, Node, and Remote Node Names

### Procedure

**Step 1** Choose **Admin** > **System config** > **System info** > **Set System name** and enter the appropriate system name..

**Step 2** Choose **Set node name** and enter the node name.

**Step 3** Choose **Set remote node name** and enter the remote node name.

## Managing Local Timezone, Time and Date, and NTP Server

### Procedure

**Step 1** Choose **Admin** > **System Config** > **Timezone**, select the View options and enter the appropriate time zone.

**Step 2** Choose **Admin** > **System Config** > **Time** > **Set Date and Time**, enter date and time.

**Note** Date format is YYYY MM DD and time format is HH MM [SS].

**Step 3** Choose **Admin** > **System Config** > **Update NTP**, enter the IP address of the NTP and choose **OK**.

## Commissioning and Partnering the System

### Procedure

**Step 1** Choose **Admin** > **Commisions**, select **Commisions for Commisioning** and choose **Ok**.

**Step 2** Choose **Admin** > **Partnering**, select **Propose** and Choose **Ok**.

**Step 3** To confirm the changes, select **Yes**.

## Apply Licenses

### Before You Begin

Both physical USB token and license key are required for license activation.

### Procedure

**Step 1** Choose **CLI** and enter the following commands.

```
my-SC# actions
my-SC# system
my-SC# apply-license
```

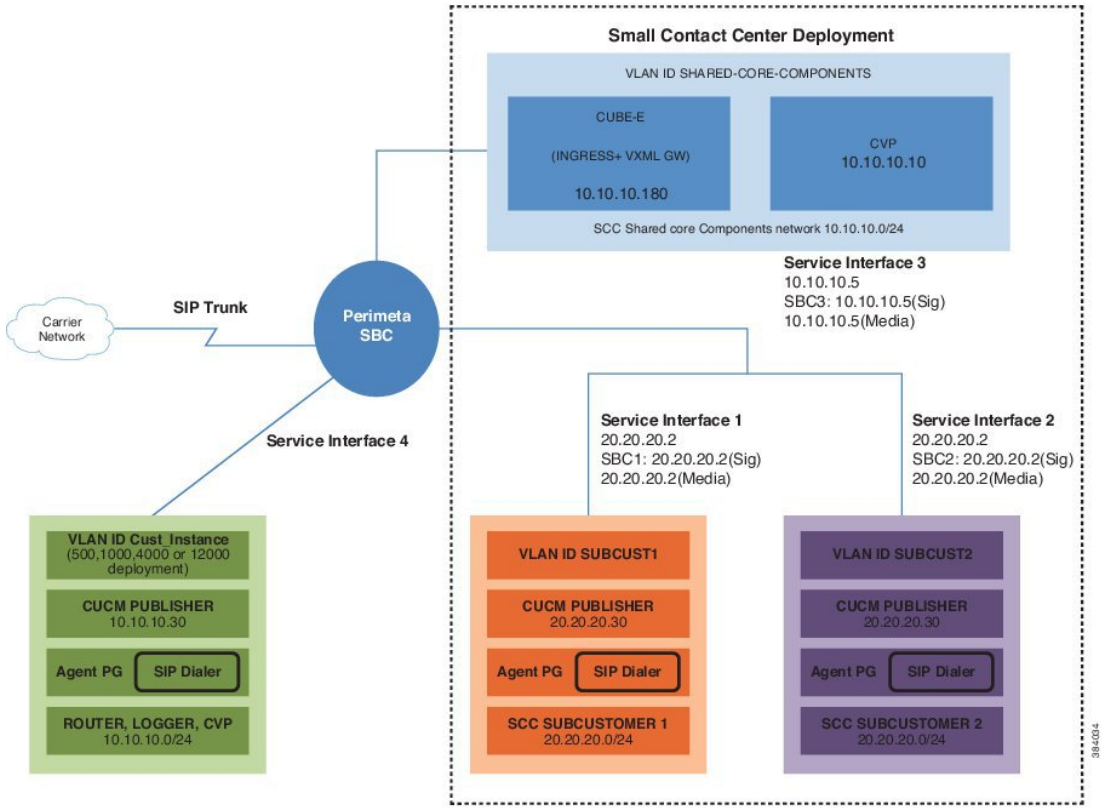
**Step 2** Enter the license key.
Session controller displays the details of the license.

**Step 3** Check the details and enter **Y**.

# Configure Perimeta SBC

Following figure shows Perimeta SBC topology for HCS deployment models.

***Figure 61: Perimeta SBC Topology for HCS Deployment Models***




## Configuration of C-Series Perimeta SBC for all HCS Deployment models

This section includes all the configurations for all HCS deployment models in Perimeta SBC.

- Configure Service Interface for Carrier Network, on page 238
- Configure Codec List, on page 239
- Configure Media Address, on page 239
- Create Account, on page 239

### Configure Service Interface for Carrier Network

To create the service interface for carrier network perform the following instructions. This is used for vPGW and for other applications which are in HCS aggregation layer.

```
config
 system
```

```
service-interface serv5
 description CarrierNetwork
 service-network 5
  port-group-name CoreNetwork
 ipv4
   subnet-prefix-length 24
   gateway-ip-address 192.168.10.1
   local-ip-address 192.168.10.2
    service-address Extra
   probes-source-style specific-source
   activate
  vlan-id 5
  network-security trusted
```

### Configure Codec List

To configure codec list, perform the following instructions.

```
sbc
    codec list codec-list-1
      description codeclist
      codec-entry G729 3
      codec-entry PCMA 2
      codec-entry PCMU 1
      codec-entry telephone-event 9
```

### Configure Media Address

For each network, mention the IP address to be used for media. Media IP addresses is required for Carrier Network - 5:

**Note** Same IP address is used for both signaling and media, as HCS deployment model use Integrated Session Controller (ISC).

Enter the following commands to add media address:

```
sbc
    media
      media-address ipv4 192.168.10.2 service-network 5
        port-range 16384 65535
```

To define media address for newly added sub-customers see, Configure Media Address for Sub-customer, on page 489

### Create Account

Enter the following commands to create an account:

```
config
 sbc
  signaling
      account carrier 5
```

To integrate Perimeta SBC with customer instance see, Perimeta SBC Integration , on page 486.

# Install and Configure Prime Collaboration Assurance

Installing Prime Collaboration Assurance encompasses:

- Deploying Prime Collaboration Assurance, on page 240
- Configuring the Prime Collaboration Assurance Virtual Appliance, on page 242
- SSL Certificate Installation, on page 245


Software Download Link:

Prime Collaboration Assurance Software download

You can install the Prime Collaboration Assurance application, based on the OVA downloaded:

- For small, medium, and large deployment models requires only one virtual machine to install and configure Prime Collaboration Assurance. To learn about configuring these deployment models, see Simple Deployment section in the prime document
- For very large deployment models: You must configure Prime Collaboration Assurance OVA for database and application on separate virtual machines. To learn about configuring these deployment models, see Advance Deployment section in the prime document

During the installation of Prime Collaboration Assurance, if there are multiple networks in UCS, ensure that the virtual machine network you select belongs to Prime Collaboration is reachable.

For information on Requirements for Prime Collaboration Assurance (includes Analytics) refer the link Prime Collaboration Assurance

# Deploying Prime Collaboration Assurance

Based on the OVA you downloaded, you can deploy Prime Collaboration Assurance as follows:


- Simple Prime Collaboration Assurance Deployment, on page 240
- Advanced Prime Collaboration Assurance Deployment, on page 241


Ensure that the requirements listed in Installation Requirements and System Requirements have been met as per the Prime document.

## Simple Prime Collaboration Assurance Deployment

You can deploy Prime Collaboration Assurance OVA for small, medium, and large deployment models:

### Procedure

**Step 1** Launch your VMWare vSphere client and choose **File** > **Deploy OVF Template**.

**Step 2** Click Browse and navigate to the location where you saved the **Prime Collaboration Assurance** OVA file. Click **Next**.

**Step 3** In the **OVF Template Details** window, verify the details about the OVA file, including the product name, version, and size, then click **Next**.

**Step 4** Click **Accept** to accept the end-user license agreement. Click **Next**.

**Step 5** In the **Name** window, specify a name for the template that you are deploying. The name must be unique within the inventory folder and can contain up to 80 characters. In the **Inventory Location** window, select the folder where you want to deploy the file, and click **Next**.

**Step 6** In the **Disk Format** window, select **Thick provisioned format** to store on the virtual disks, then click **Next**.

**Step 7** Verify the options in the **Ready to Complete** window, then click **Finish** to start the deployment.

The deployment takes about 30 minutes to complete. Check the progress bar in the **Deploying Virtual Appliance** window to monitor the task status.

**Step 8** After the deployment task is complete, click **Close** in the confirmation message box.

The virtual appliance that you deployed appears in the left pane of the vSphere client, under the host. As a part of the next process, follow Configuring the Prime Collaboration Assurance Virtual Appliance, on page 242.

## Advanced Prime Collaboration Assurance Deployment

Following is the procedure to deploy Prime Collaboration Assurance very large OVA deployment model.

### Procedure

**Step 1** Launch your VMWare vSphere client and choose **File** > **Deploy OVF Template**.

**Step 2** Click Browse and navigate to the location where you saved the **Prime Collaboration Assurance** OVA file. Click **Next**

**Step 3** In the **OVF Template Details** window, verify the details about the OVA file, including the product name, version, and size, and then click **Next**.

**Step 4** Click **Accept** to accept the end-user license agreement. Click **Next**.

**Step 5** In the **Name** window, specify a name for the template. The name must be unique within the inventory folder and can contain up to 80 characters. In the I**nventory Location** window, select the folder where you want to deploy the file and click **Next**.

**Step 6** If you choose to enable **Prime Collaboration Analytics** in very large OVA deployment of **Prime Collaboration Assurance**, you require two virtual machines - **database** and **application**. Recommended, install the **database** server first so that you can have the database server IP address, this is required while installing application server. Configure the database server before to application server. To configure the database server.

a) In the **Host/Cluster** window, select the **Host** or **Cluster** on which you want to run the deployed template and click **Next**.

b) In the **Storage** window, select a destination for the virtual machine files and click **Next**.
c) In the **Disk Format** window, select the **Thick Provision Lazy Zeroed** format to store on the virtual disks, then click **Next**.
d) Verify the options in the **Ready to Complete** window, then click **Finish** to start the deployment. The deployment takes about 30 minutes to complete. Check the progress bar in the **Deploying Virtual Appliance** window to monitor the task status.
e) After the deployment task is complete, click **Close** in the confirmation message box. The virtual appliance that you deployed appears in the left pane of the vSphere client, under the host.
f) (Optional) Before you proceed with configuring **Prime Collaboration Assurance**, right-click the database server and select **Edit** Settings to change the server configurations. The recommended CPU for database server configuration is 8 and Memory is 16 GB.

**Note** If you reduce the CPU to 8, from the default value of 24, you should also reduce the corresponding CPU Reservation frequency to 16 Ghz from the default value of 48 Ghz.

To configure application server.

g) In **Disk Format** window, select the **Thick Provision Lazy Zeroed** format to store on the virtual disks, then click **Next**.
h) In the **Network Mapping** page, select a network and click **Next**.
i) Verify the options in the **Ready to Complete** window, then click **Finish** to start the deployment. The deployment takes about 30 minutes to complete. Check the progress bar in the **Deploying Virtual Appliance** window to monitor the task status.
j) After the deployment task is complete, click **Close** in the confirmation message box. The virtual appliance that you deployed appears in the left pane of the vSphere client, under the host.

As a part of the next process, follow Configuring the Prime Collaboration Assurance Virtual Appliance, on page 242.

# Configuring the Prime Collaboration Assurance Virtual Appliance

After you deploy the Prime Collaboration Assurance OVA, you must configure the virtual appliance.

Based on the OVA you have downloaded, you can configure the Prime Collaboration Assurance virtual appliance as follows:



## Simple Prime Collaboration Assurance Configuration

You can configure Prime Collaboration Assurance OVA for small, medium, and large deployment models:

### Procedure

**Step 1** Right-click the virtual appliance and choose **Power** > **Power ON** to start the virtual machine.

**Step 2** In the virtual appliance console, enter **setup** at the localhost login prompt.

**Step 3** Enter the required parameters at the console prompts. Press Enter to bring up the next parameter. For the Installation Mode prompt, enter **1** to select **Standard Prime Collaboration Assurance**, or **2** to select **Advanced Prime Collaboration Assurance Evaluation**. The Default value is **1**.

The virtual machine will reboot.

**Note** Time zone-The timestamp that is displayed on the UI is the server time. By default, the configured time zone is UTC. For a list of supported time zones, see Supported Timezones for Prime Collaboration.

**Step 4** If you have selected the **Advanced Prime Collaboration Assurance Evaluation** option, select the **Managed Service Provider (MSP)** mode of deployment. Enter **M** to deploy Prime Collaboration Assurance in the MSP mode.

Each mode provides a different customer view option. For more information, see Overview of Cisco Prime Collaboration - Assurance section in the Cisco Prime Collaboration Assurance Guide - Advanced, 10.5.

**Note** If you have selected the **Standard Prime Collaboration Assurance** option, it is directly deployed in the **Enterprise mode**.

**Step 5** After installation (when you see the login prompt in the console), wait for approximately 20 minutes for the **Prime Collaboration Assurance** processes to be listed on the console, and then log in to the **Prime Collaboration Assurance** UI.

**Step 6** Log in to the **Prime Collaboration Assurance** server to verify the installation. See the How to verify the Cisco Prime Collaboration Assurance Standard installation and How to verify the Cisco Prime Collaboration Assurance Advanced installation sections in Troubleshooting Cisco Prime Collaboration.

## Advanced Prime Collaboration Assurance Configuration

You can configure Prime Collaboration Assurance OVA for very large deployment model.

### Procedure

**Step 1** Right-click **virtual appliance** and choose **Power** > **Power ON** to start the virtual machine.

**Step 2** In the virtual appliance console, enter **setup** at the localhost login prompt.

**Step 3** Enter the required parameters at the console prompts.

- **Hostname:** Enter the Hostname for the VM deployed
- **IP Address:** The IP address of the virtual appliance
- **IP default netmask:** The default subnet mask for the IP address
- **IP default gateway:** The IP address of the default gateway
- **Default DNS domain:** The default Domain Name
- **Primary name server (Optional):** The primary name server, to configure several name servers, enter **Y**

- **Primary NTP server[time.nist.gov]:** The primary NTP server. To enter a secondary NTP server, enter **Y** at the next prompt

  **Note** To configure a tertiary NTP server enter **Y** at the next prompt, after you specify a secondary NTP server. Prime Collaboration supports three NTP servers.
- **Timezone:** The timestamp that is displayed on the UI is the server time. By default, the configured timezone is UTC. For a list of supported timezones, see Supported Timezones for Prime Collaboration.
- **Username:** CLI Admin user name. Default user name is admin. However, you can specify the user name of your choice
- **Password:** CLI Admin password. This password is used to log in to CLI to check the application status and perform back up and restore
- **IPv6 configuration (Optional):** If you want to configure IPv6 when prompted, specify **Y**, and then enter the IPv6 address and route to proceed. If not, you can proceed with the installation by providing your inputs for the next prompt
- **Root password:** Specify a password for the root user
- **globaladmin password:** Specify a password for the globaladmin

**Step 4** After entering each parameter, press Enter to bring up the next parameter. For the Installation Mode prompt, enter **1** to select **Standard Prime Collaboration Assurance**, or **2** to select **Advanced Prime Collaboration Assurance Evaluation**. The default value is **1**.

The virtual machine will reboot.

**Note** Time zone-The timestamp that is displayed on the UI is the server time. By default, the configured time zone is UTC. For a list of supported time zones, see Supported Timezones for Prime Collaboration.

**Step 5** If you have selected the **Advanced Prime Collaboration Assurance Evaluation** option, select the the **Managed Service Provider (MSP)** mode of deployment. Enter **M** to deploy Prime Collaboration Assurance in the MSP mode.

Each mode provides a different customer **view** option. For more information, see section "Overview of Cisco Prime Collaboration - Assurance" in the Cisco Prime Collaboration Assurance Guide - Advanced, 10.5 .

**Note** If you have selected the Standard Prime Collaboration Assurance option, it is directly deployed in the Enterprise mode.

**Step 6** If you have downloaded the very large OVA deployment model, you are prompted to enter the type of server to be configured.

**Note** You can choose to enable Prime Collaboration Assurance only or both Prime Collaboration Assurance and Prime Collaboration Analytics. If you choose to enable Prime Collaboration Analytics, you need to deploy the database server before you deploy the application server. See Deploying Prime Collaboration Assurance.

a) For the server configuration prompt, enter **Y** to configure the server as an analytics database server.

b) After the analytics database server installation, you are prompted to enter the analytics database server IP address.

c) Enter **Y** and enter the database server IP address to complete the Prime Collaboration Assurance and Prime Collaboration Analytics installation.

**Note** If you enter **N** in the server configuration prompt, the steps to install Prime Collaboration Analytics at a later point of time is displayed. See, Enabling Prime Collaboration Analytics After Prime Collaboration Assurance Installation.

**Step 7** After the installation (when you see the login prompt in the console), wait for approximately 20 minutes for the **Prime Collaboration Assurance** processes to be listed on the console, and then log in to the **Prime Collaboration Assurance UI**.

**Step 8** Log in to the Prime Collaboration Assurance server to verify the installation. See the "How to verify the Cisco Prime Collaboration Assurance Standard installation" and "How to verify the Cisco Prime Collaboration Assurance Advanced installation" sections in Troubleshooting Cisco Prime Collaboration.

# SSL Certificate Installation

- **Windows Internet Explorer:** You can permanently remove the SSL certificate warning by installing the Prime Collaboration self-signed certificate. See, Removing SSL Certificate Warning from Windows Internet Explorer, on page 245
- **Mozilla Firefox:** You can remove the SSL certificate warning only by adding an exception. See, Removing SSL Certificate Warning from Mozilla Firefox, on page 246

## Removing SSL Certificate Warning from Windows Internet Explorer

Perform the following procedure to remove the SSL Certificate warning from Windows Internet Explorer.

### Procedure

**Step 1** Choose **Continue to this website (not recommended)**.

**Step 2** Choose **Tools** > **Internet Options**.

**Step 3** In **Internet Options** dialog box, click the **Security** tab, choose **Trusted sites**, and then click **Sites**.

**Step 4** Confirm that the URL that appears in the field and matches the application URL, and then click **Add**.

**Step 5** Close all dialog boxes and refresh the browser.

**Step 6** Choose **Certificate Error** to the right of the address bar, and then click **View certificates**.

**Step 7** In the **Certificate** dialog box, click **Install Certificate**.

**Step 8** In the **Certificate Import Wizard** dialog box, click **Next**.

**Step 9** Click the **Place all certificates in the following store** radio button, and then click **Browse**.

**Step 10** In the **Select Certificate Store** dialog box, choose **Trusted Root Certification Authorities**, and then click **OK**.

**Step 11** Click **Next** > **Finish**.

**Step 12** In the **Security Warning** message box, click **Yes**.

**Step 13** In the **Certificate Import Wizard** message box, click **OK**.

**Step 14** In the **Certificate** dialog box, click **OK**.

**Step 15** Repeat Step 2 and Step 3.

**Step 16** Select the URL in the **Websites** section, and then click **Remove**.

**Step 17** Close all dialog boxes, restart the browser, and invoke Prime Collaboration. See the "Getting Started" chapter of Prime Collaboration 9.0 Administration Guide for information about invoking Prime Collaboration.

**Step 18** If you have a safe URL implemented, do the following:

a) Choose **Tools** > **Internet Options**.

b) In the **Internet Options** dialog box, click the **Advanced** tab.

c) In the **Security** section, uncheck the **Warn about certificate address mismatch** check box.

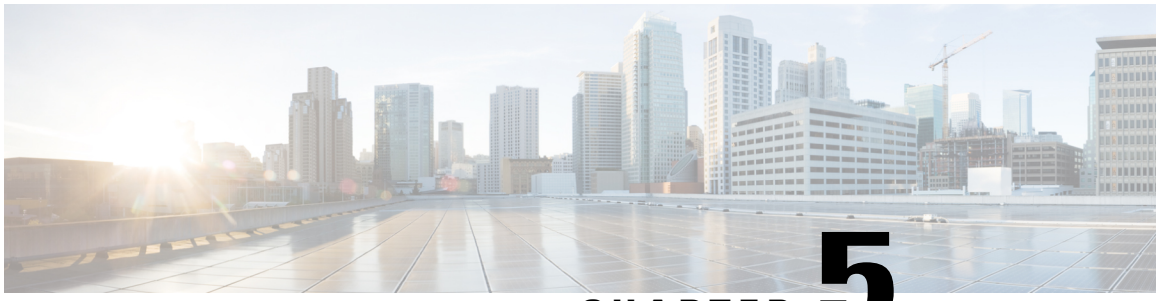
## Removing SSL Certificate Warning from Mozilla Firefox

Perform the following procedure to remove SSL Certificate Warning from Mozilla Firefox.

### Procedure

**Step 1** Check **I Understand the Risks** check box and click **Add Exception**.

**Step 2** In the **Add Security Exception** dialog box, click **Confirm Security Exception**.



CHAPTER 5

# Golden Template Process

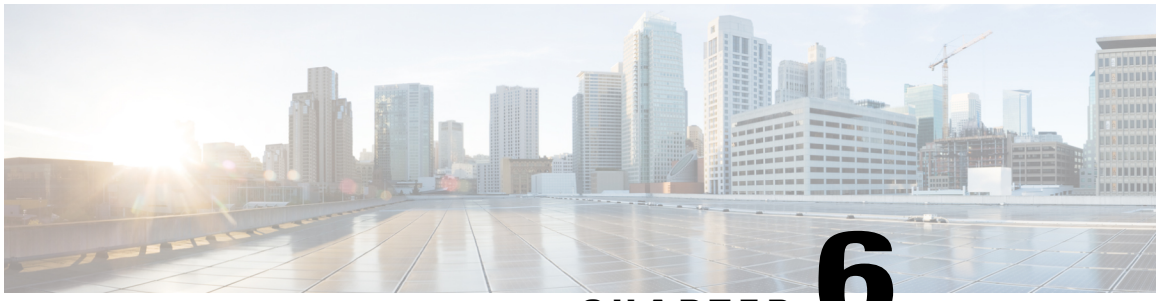


## Sequence for Golden Template Process

The Golden Template process is a three step configuration process that clones and deploys the Golden templates as Virtual machines (VMs) on the destination servers deployed for the customer after the Golden templates are built. The administrative tasks for the contact center VM applications on destinations servers are initiated only after the Golden template process.

The sequence is:

- Create Golden Template, on page 249
- Clone and OS Customization, on page 299
- Configure Customer Instance, on page 319



CHAPTER 6

# Create Golden Template



## Create Golden Template for 500 Agent Deployment

Follow this sequence of tasks to create the golden template for 500 agent deployment for Cisco HCS for Contact Center.

After each task, return to this page to mark the task “done” and continue the sequence.

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 1 | | Create Golden Template for Unified CCE Call Server, on page 250 | HCS Core Component |
| 2 | | Create Golden Template for Unified CCE Data Server, on page 255 | HCS Core Component |
| 3 | | Create Golden Template for Unified CVP Server, on page 259 | HCS Core Component |
| 4 | | Create Golden Template for Unified CVP OAMP Server, on page 261 | HCS Core Component |
| 5 | | Create Golden Template for Unified CVP Reporting Server, on page 262 | HCS Core Component |
| 6 | | Create Golden Template for Cisco Finesse, on page 264 | HCS Core Component |

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 7 | | Create Golden Template for Cisco Unified Intelligence Center with Live Data, on page 265 | HCS Core Component |
| 8 | | Create Golden Template for Cisco Unified Communications Manager, on page 266 | HCS Core Component |

# Create Golden Template for Unified CCE Call Server

Follow this sequence of tasks to create the golden template for Unified CCE Call Server.

After each task, return to this page to mark the task “done” and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova` | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Unified CCE Call Server OVA. | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install anti-virus software. | Follow the procedure Install Antivirus Software, on page 253. |
| 5 | | Install the Unified Contact Center Enterprise. | Follow the procedure Install Unified Contact Center Enterprise, on page 254. |
| 6 | | Convert the virtual machine to a template. | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Unified CCE Call Server on the destination system. See Configure Cisco Unified CCE Call Server, on page 323.

# Create Virtual Machines

## Procedure

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

**Step 2** Browse to the location on your local drive where you 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 **Name** field, enter the Virtual Machine name. 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. Skip this step if you do not have a resource pool allocated in the host server, and click **Next**.

**Step 7** On the **Storage** page, select a datastore that you want to deploy the new virtual machine. See Storage, VM Specifications, and IOPS Considerations, on page 168. Click **Next**.

**Step 8** On the **Disk Format** page, select **Thin provision format**. Click **Next**.

**Note** For CCDM and Unified EIM and WIM, keep the virtual disk format **Thick provisioned Lazy Zeroed**.

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

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

- Public to Visible Network
- Private to Private Network

**Step 10** Click **Finish**.

**Step 11** Right-click on the VM, edit the **CPU** and increase the number of virtual sockets to 2.

## Install Microsoft Windows Server 2012 R2 Standard Edition

### Procedure

**Step 1** Mount the Microsoft Windows Server ISO image to 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 **Windows Server 2012 R2 Standard(Server with GUI)**, 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** Install 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 **Preffered DNS Server** address, then click **OK**.

**Note** All network configurations are overwritten with new settings.

**Step 14** Run a Microsoft Windows update.
After the update is complete, check **Do not enable automatic updates**.

## Install VMware Tools

VMware Tools is a suite of utilities that enhance the performance of the virtual machine guest operating system. It also aids virtual machine management.

### Procedure

**Step 1** Switch on the virtual machine.
**Step 2** When the Guest Operating starts, prepare your virtual machine to install VMware tools.
**Step 3** Choose **VM** > **Guest** > **Install VMware Tools**.
**Step 4** Double-click your CD-ROM drive to open the installation wizard. Click **OK** in the warning message.
**Step 5** Choose the **Typical** option, then click **Next** to begin installation.
**Step 6** Click **Install**.
**Step 7** Click **Finish**.
**Step 8** Restart your system.

## Install Antivirus Software

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

This procedure is required for the applications that use the Windows 2012 Operating System.

Install one of the following anti-virus software products for Unified CCE Call Server, Unified CCE Data Server, Unified CVP server, Unified CVP OAMP server, and Unified Reporting server.

- McAfee® VirusScan® Enterprise 8.7i / 8.8i
- Symantec® Endpoint Protection 11.0 / 12.1
- Trend Micro Server Protect Version 5.7 / 5.8

Install one of the following anti-virus software products for Unified WIM and EIM.

- McAfee® VirusScan® Enterprise version 8.7
- Symantec® AntiVirus® Corporate Edition 10.1

**Important** Update anti-virus software, manually - do not enable automatic updates.

**Tip** To allow required access to installation program files or folders, perform file-blocking exclusions in the anti-virus 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 Contact Center supports Symantec Endpoint Protection 12.1.

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.

### Disabling Port Blocking

On computers that run Unified CVP Server components, such as Call Server and Reporting server, which has an anti-virus software configured to block ports, exclude Unified CVP processes and `tomcat6.exe`. In addition, exclude Voice Browser.exe for the call server process.

**Note** If you use an anti-virus software other than McAfee Virus Scan, perform the equivalent exclusions in port blocking rules for that software.

#### Procedure

**Step 1** Select **Start** > **All Programs** > **McAfee** > **VirusScan Console**.

**Step 2** Double-click **Access Protection**, then choose **Anti-virus Standard Protection**.

**Step 3** Choose **Prevent IRC communication** from the list, then click **Edit**.

**Step 4** Add `tomcat6.exe`, `tomcat5.exe`, `VoiceBrowser.exe` to the **Processes to Exclude** , then click **Ok**.

**Step 5** Click **Ok**.

## Install Unified Contact Center Enterprise

Complete the following procedure to install the Unified Contact Center Enterprise.

### Procedure

**Step 1** Add the template virtual machine into the domain.

**Step 2** Mount the correct version of the Unified Contact Center Enterprise ISO image to the virtual machine's CD/DVD drive.

**Step 3** Run setup.exe from the ICM-CCE-CCH Installer directory on the CD/DVD drive and follow the InstallShield procedures to install Unified Contact Center Enterprise.

**Step 4** In the **Select the installation method** window, click **Fresh Install**. Click **Next**.

**Step 5** In the **Maintenance Release (MR)** window, leave the Maintenance Release Location field blank. Click **Next**.

**Step 6** In the **Installation Location** window, select the drive C from the drop-down list. 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**. 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 template virtual machine back to the workgroup.

## 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 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**.

# Create Golden Template for Unified CCE Data Server

Follow this sequence of tasks to create the golden template for Unified CCE Data Server.

After each task, return to this page to mark the task "done" and continue the sequence.

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 1 | | Download HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova. | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Unified CCE Data Server. | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server. | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install antivirus software. | Follow the procedure Install Antivirus Software, on page 253. |
| 5 | | Enable .Net Framework 3.5 SP1 | Follow the procedure Enable Microsoft .Net Framework 3.5 SP1, on page 256 |
| 6 | | Install Microsoft SQL Server. | Follow the procedure Install Microsoft SQL Server 2014 Standard Edition , on page 257. |
| 7 | | Install the Unified Contact Center Enterprise. | Follow the procedure Install Unified Contact Center Enterprise, on page 254. |
| 8 | | Convert the virtual machine to a template. | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Unified CCE Data server on the destination system. See Create Golden Template for Unified CCE Data Server, on page 255.

## Enable Microsoft .Net Framework 3.5 SP1

### Procedure

**Step 1** Open **Server Manager**.

**Step 2** Click **Manage** and choose **Add Roles and Features**.

Opens **Add Roles and Features wizard**.

**Step 3** On **Select Installation Type** window, click **Next**.

**Step 4** Choose **Role-based or feature-based installation** option.

**Step 5** Choose **Select a server from server pool** option.

**Step 6** Choose appropriate server from **Server Pool** drop-down list and click **Next**.

**Step 7** On **Server Roles** window click **Next**.

**Step 8** Check **.Net Framework 3.5 Features** check box in **Features** list and click **Next**.

**Step 9** Click **Specify an alternate source path** and enter the path `\sources\sxs` which is available in Microsoft 2012 OS Installer DVD or ISO. Click **OK**.

**Step 10** Click **Install**.

**Step 11** After installation, restart the server.

## Install Microsoft SQL Server 2014 Standard Edition

Install Microsoft SQL Server 2014 x64 and store the SQL Server log and temporary files on the same physical disk as the operating system (typically the C drive).

For Unified CCE components, use the secondary drive to store the database (typically the D drive).

### Before You Begin

Ensure Microsoft .Net framework 3.5 is enabled. See, Enable Microsoft .Net Framework 3.5 SP1, on page 256.

### Procedure

**Step 1** Mount the Microsoft SQL Server 2014 ISO image to the virtual machine. For more information, see Mount and Unmount ISO Files, on page 787.

**Step 2** Run setup.exe.

**Step 3** Click **Installation** on the left pane and then click **New SQL Server stand-alone installation or add features to an existing installation** link.
The SQL Server 2014 Setup wizard opens. Click **Next**.

**Step 4** Accept the Licence Terms and click **Next**.

**Step 5** On **Microsoft Update** page, click **Next**.

**Step 6** On **Product Updates** page, click **Next**.

**Step 7** On **Install Rules** page, click **Next**.

**Step 8** On **Setup Role** page, select **SQL Server Feature Installation**, and click **Next**.

**Step 9** On **Feature Selection** page, choose all the features except below:

- **Analysis Services**
- **Reporting Services-Native**
- **Reporting Services - SharePoint**
- **Reporting Services Add-in for SharePoint Products**

- **Distributed Replay Controller**
- **Distributed Replay Client**

Click **Next**.

**Step 10** On **Instance Configuration** page, select **Default Instance**. Click **Next**.

**Step 11** On **Server Configuration** page, click **Services Account** tab:
You must associate the SQL Services with the Account Name.

- For SQL Server Database Engine, choose **NT Service\MSSQLSERVER** from **Account Name** drop-down list and choose **Automatic** in **Startup Type** column.
- For SQL Server Agent, choose **NT Service\SQLSERVERAGENT** from **Account Name** drop-down list and choose **Automatic** in **Startup Type** column.
- For the remaining services, accept the default values.

**Step 12** On **Server Configuration** page, select **Collation** tab.

**Note** Collation configuration is different for both CCE and CCDM servers. Follow the appropriate procedures to configure collation.

- Configure the collation for CCE servers as follows:

  1. Click **Customize** for **Database Engine**.
  2. Choose **Windows Collation designator and sort order** option.
  3. Choose appropriate collation from **Collation Designator** drop-down list. For more information http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCE

     **Example:** For **English** language choose **Latin1_General**.
  4. Check **Binary** check-box and click **OK**.
  5. Click **Next**.

- Configure the collation for CCDM servers as follows:

  1. Click **Customize** for **Database Engine**.
  2. Choose **Windows Collation designator and sort order** option.
  3. Choose **Latin1_General** from **Collation designator** drop-down list.
  4. Check **Accent Sensitive** check-box and click **OK**.
  5. Click **Next**.

**Step 13** On the **Database Engine Configuration** page, perform the following:

a) In **Server Configuration** tab, choose **Mixed Mode** option.
b) Enter your password and confirm by reentering it.
c) Click **Add Current User**.
d) Select **Data Directories** tab, it is strongly recommended that **Temp DB** and **Temp DB log** directories should be in different drives.

e) Click **Next**.

**Step 14** Click **Install** on the **Ready to Install** page.

**Step 15** Click **Close** on the **Complete** page.

**Step 16** Enable Named Pipes and set the sort order as follows:

a) Open **SQL Server 2014 Configuration Manager**.
b) In the left pane, navigate to **SQL NativeClient 11.0 Configuration (32bit)** > **Client Protocols**.
c) In the right pane, right-click **Named Pipes**, and ensure **Enable** option is selected.
d) In the Client Protocols Properties window, right-click **Named Pipes** and select the order, click **Move Up** or **Move Down** to change the order of the protocols as follows: Shared Memory, Named Pipes, TCP/IP, then click **OK**.
e) In the left pane, expand **SQL Server Network Configuration**, and select **Protocols for MSSQLSERVER**.
f) In the right pane, right-click **Named Pipes**, and select **Enable**, and click **OK**.
g) In the right pane, right-click **TCP/IP**, and select **Enable**.

**Step 17** Enable **Autogrowth** as follows:

a) Open **SQL Server 2014 Management Studio**.
b) Click **Connect**. In the left pane, expand **Databases > System Databases**.
c) Right-click **tempdb** and select **Properties**.
d) In the left pane, select **Files**. Ensure that **AutoGrowth** is enabled for both **tempdev** and **templog**.
e) For **Maximum File Size**, select **Unlimited** option, applicable for both tempdev and templog.
f) For **File Growth**, enter 10 **In Percent** field, applicable for both tempdev and templog.
g) Set **initial size (MB)** as **1400** for tempdev and **1024** for templog and click **OK**.

**Step 18** Set the SQL Server's default language to **English** as follows:

a) On **SQL Server Management Studio** page, right-click on the server and choose **Properties**.
b) Click **Advanced**.
c) In **Miscellaneous** section, choose **English** from **Default Language** drop-down list.

**Important** You must set the SQL Server default language to English because Unified CCE requires a US date format (MDY). Many European languages use the European date format (DMY) instead. This mismatch causes queries such as `select * from table where date = '2012-04-08 00:00:00'` to return data for the wrong date.

**Step 19** Restart the SQL Server service.

# Create Golden Template for Unified CVP Server

Follow this sequence of tasks to create the golden template for Cisco Unified CVP Server.

After each task, return to this page to mark the task “done” and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova`. | See Open Virtualization Format Files, on page 54. |

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 2 | | Create the virtual machine for the Cisco Unified CVP Server. | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install antivirus software. | Follow the procedure Install Antivirus Software, on page 253. |
| 5 | | Install the Unified CVP Server. | Follow the procedure Install Unified CVP Server, on page 260. |
| 6 | | Convert the virtual machine to a template. | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Unified CVP Server on the destination system. See Configure Unified CVP, on page 347.

## Install Unified CVP Server

Complete the following procedure to install the Unified CVP Server.

### Procedure

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

**Step 2** Copy the current Engineering Specials to the local drive.

**Note** Ignore this step if there are no Engineering Specials.

**Step 3** Select the ISO file on the `CD/DVD` drive `D`. Run `setup.exe` from the `D:\ CVP\Installer_Windows` directory.

**Step 4** Follow the InstallShield wizard:

a) Accept the license agreement and click **Next**.

b) In the **Select Packages** window, select **CVP Server** and click **Next**.

c) In the **Voice Prompt Encode Format Type** window, select **U-Law Encoded Wave Format** and Click **Next**.

d) In the **Choose Destination Location** window, select the folder locations for the CVP Installation Folder and the Media Files Installation Folder, and click **Next**.

e) In the **X.509 Certificate** window, enter the information that you want to include in the certificate.
f) In the **Ready to Install the Program** window, click **Install**.
g) In the **Installation Complete** window, click **Yes, I want to restart my computer now**. Click **Finish**.

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

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

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

**Step 8** Unmount the ISO image.

# Create Golden Template for Unified CVP OAMP Server

Follow this sequence of tasks to create the golden template for Cisco Unified CVP OAMP Server.

After each task, return to this page to mark the task "done" and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova`. | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Cisco Unified CVP OAMP Server. | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install antivirus software. | Follow the procedure Install Antivirus Software, on page 253. |
| 5 | | Install the Cisco Unified CVP OAMP Server. | Follow the procedure Install Unified CVP OAMP Server, on page 262. |
| 6 | | Convert the virtual machine to a template. | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Unified CVP OAMP Server on the destination system. See Configure Cisco Unified CVP Operations Console, on page 359.

## Install Unified CVP OAMP Server

### Procedure

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

**Step 2** Run setup.exe from the `CVP\Installer_Windows` directory on the CD/DVD drive.

**Step 3** Click **I accept the terms of the License Agreement** from the License Agreement and Copyright screen.

**Step 4** On the **Select Package** window, select the Unified CVP component **Operations Console**, and click **Next**.

**Step 5** In the **Voice Prompt Encode Format Type** window, select **U-Law Encoded Wave Format** and click **Next**.

**Step 6** On the **Choose Destination Location** window, accept the default locations, and click **Next**.

**Step 7** In the **X.509 certificate** window, enter the information that you want to include in the certificate, and click **Next**.

**Step 8** In the **Ready to Install** window, click **Install**.

**Step 9** Enter the operations console password that meets the criteria detailed on the **Operations Console Password** window, and click **Next**.

**Step 10** Click **Yes, I want to restart my computer**, and click **Finish**.

**Step 11** Unmount the Unified CVP ISO image.

# Create Golden Template for Unified CVP Reporting Server

Follow this sequence of tasks to create the golden template for Cisco Unified CVP Reporting Server.

After each task, return to this page to mark the task “done” and continue the sequence.

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova`. | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Unified CVP Reporting Server | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install antivirus software | Follow the procedure Install Antivirus Software, on page 253. |

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 5 | | Convert the virtual machine to a template | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the CVP Reporting Server on the destination system. See Configure Unified CVP Reporting Server, on page 351

## Install Unified CVP Reporting Server

Complete the following procedure to install the Unified CVP Reporting Server.

### Procedure

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

**Step 2** Copy the current Engineering Specials to the local drive.

**Note** Ignore this step if there are no Engineering Specials.

**Step 3** Select the ISO file on the CD/DVD drive. Run *setup.exe* from the DVD drive located at `CVP\Installer_Windows` directory.

**Step 4** Follow the Install Shield wizard:

a) Check **I accept the terms of the License Agreement from the License Agreement and Copyright** and click **Next**.

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

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

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

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

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

**Note** Select **Standard** for 500 agent deployment and **Premium** for other HCS agent deployments.

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

h) Enter the Reporting Server password when prompted.
It can take some time for the database to install.

i) Restart the server after installation.

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

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

**Step 7** Unmount the ISO image.

# Create Golden Template for Cisco Finesse

Follow this sequence of tasks to create the golden template for Cisco Finesse.

After each task, return to this page to mark the task "done" and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_Finesse_vmv8_v1.0.ova` | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for Cisco Finesse | See, Create Virtual Machines, on page 251. |
| 3 | | Install Cisco Finesse | Follow the procedure for installing VOS applications for golden templates. See Install Unified Communications Voice OS based Applications, on page 264 . |
| 4 | | Convert the virtual machine to a template | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process Automated Cloning and OS Customization, on page 300. After you run the automation process, you can configure Cisco Finesse on the destination system. See Configure Cisco Finesse, on page 392.

## Install Unified Communications Voice OS based Applications

Use the following procedures to install Unified Communications Voice OS based applications:

- Cisco Unified Communications Manager
- Cisco Unified Intelligence Center
- Live Data
- Cisco Unified Intelligence Center with Live Data
- Cisco Finesse
- Cisco MediaSense
- Cisco Virtualized Voice Browser

### Procedure

**Step 1** Mount the ISO file to the CD/DVD drive of the virtual machine and power it on.

**Step 2** Follow the Install wizard:

a) On **Disk found** page, click **OK** to check the media before installation.
b) Click **OK** on the success message.
c) On **Product Deployment Selection** page, select the required product and click **OK**.
d) On **Proceed with Install** page, click **Yes**.
e) On **Platform Installation Wizard** page, select **Skip** option.
After installation it displays **Pre-existing Configuration Information** page.
f) Press Ctrl+Alt to free your cursor.

**Step 3** Shutdown the Virtual Machine.

**Step 4** Unmount the ISO image.

# Create Golden Template for Cisco Unified Intelligence Center with Live Data

Follow this sequence of tasks to create the golden template for Cisco Unified Intelligence Center with Live Data.

After each task, return to this page to mark the task "done" and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download `UCCELD_11.0_CVOS_vmv8_v1.0.ova`. | See Create Virtual Machines, on page 251 |
| 2 | | Create the virtual machine for Live Data | See Create Virtual Machines, on page 251. |
| 3 | | Install Cisco Unified Intelligence Center with Live Data | Follow the procedure for installing VOS applications for golden templates. See Install Unified Communications Voice OS based Applications, on page 264. |
| 4 | | Install VMware Tools | Follow the procedure Install VMware Tools, on page 252 |
| 5 | | Convert the virtual machine to a Golden Template | See Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Cisco Unified Intelligence Center VMs on the destination system. See Configure Unified Intelligence Center with Live Data, on page 380.

# Create Golden Template for Cisco Unified Communications Manager

Follow this sequence of tasks to create the golden template for Cisco Unified Communications Manager. After each task, return to this page to mark the task "done" and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download `cucm_10.5_vmv8_v1.9.ova` | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for Unified Communications Manager | Follow the procedure that is documented in, Create Virtual Machines, on page 251. |
| 3 | | Install Cisco Unified Communications Manager | Follow the procedure for installing VOS applications for golden templates. See Install Unified Communications Voice OS based Applications, on page 264 . |
| 4 | | Convert the virtual machine to a template | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255 |

After you create all golden templates, you can run the automation process Automated Cloning and OS Customization, on page 300. After you run the automation process, you can configure the Unified Communications Manager publisher and subscriber VM on the destination system. See Configure Unified Communications Manager, on page 375.

# Create Golden Template for 1000 Agent Deployment

Follow this sequence of tasks to create the golden template for 1000 agent deployment for Cisco HCS for Contact Center.

After each task, return to this page to mark the task “done” and continue the sequence.

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 1 | | Create Golden Template for Unified CCE Call Server, on page 250 | HCS Core Component |

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 2 | | Create Golden Template for Unified CCE Data Server, on page 255 | HCS Core Component |
| 3 | | Create Golden Template for Unified CVP Server, on page 259 | HCS Core Component |
| 4 | | Create Golden Template for Unified CVP OAMP Server, on page 261 | HCS Core Component |
| 5 | | Create Golden Template for Unified CVP Reporting Server, on page 262 | HCS Core Component |
| 6 | | Create Golden Template for Cisco Finesse, on page 264 | HCS Core Component |
| 7 | | Create Golden Template for Cisco Unified Intelligence Center with Live Data, on page 265 | HCS Core Component |
| 8 | | Create Golden Template for Cisco Unified Communications Manager, on page 266 | HCS Core Component |

# Create Golden Template for 4000 Agent Deployment

Follow this sequence of tasks to create the golden template for 4000 agent deployment for Cisco HCS for Contact Center.

After each task, return to this page to mark the task “done” and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Create Golden Template for Unified CCE Rogger, on page 268 | HCS Core Component |
| 2 | | Create Golden Template for Unified CCE AW-HDS-DDS, on page 269 | HCS Core Component |
| 3 | | Create Golden Template for Unified CCE Agent Peripheral Gateway, on page 270 | HCS Core Component |
| 4 | | Create Golden Template for Unified CCE VRU Peripheral Gateway, on page 271 | HCS Core Component |
| 5 | | Create Golden Template for Unified CVP Server, on page 259 | HCS Core Component |
| 6 | | Create Golden Template for Unified CVP OAMP Server, on page 261 | HCS Core Component |

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 7 | | Create Golden Template for Unified CVP Reporting Server, on page 262 | HCS Core Component |
| 8 | | Create Golden Template for Cisco Finesse, on page 264 | HCS Core Component |
| 9 | | Create Golden Template for Cisco Unified Intelligence Center , on page 272 | HCS Core Component |
| 10 | | Create Golden Template for Cisco Unified Communications Manager, on page 266 | HCS Core Component |
| 11 | | Create Golden Template for Live Data Reporting System, on page 272 | HCS Core Component |

# Create Golden Template for Unified CCE Rogger

Follow this sequence of tasks to create the golden template for Cisco Unified CCE Rogger.

After each task, return to this page to mark the task “done” and continue the sequence.

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova` | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Unified CCE Rogger | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server. | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install Anti-Virus software | Follow the procedure Install Antivirus Software, on page 253. |
| 5 | | Enable .Net Framework 3.5 SP1 | Follow the procedure Enable Microsoft .Net Framework 3.5 SP1, on page 256 |

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 6 | | Install Microsoft SQL Server. | Follow the procedure Install Microsoft SQL Server 2014 Standard Edition , on page 257. |
| 7 | | Install the Unified CCE | Follow the procedure Install Unified Contact Center Enterprise, on page 254. |
| 8 | | Convert the virtual machine to a template | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Unified CCE Rogger on the destination system. See Configure Cisco Unified CCE Rogger, on page 404 for 4000 agent deployment model and Configure Unified CCE Rogger for Small Contact Center Agent Deployment , on page 425 for small contact center agent deployment model.

# Create Golden Template for Unified CCE AW-HDS-DDS

Follow this sequence of tasks to create the golden template for Cisco Unified CCE AW-HDS-DDS.

After each task, return to this page to mark the task “done” and continue the sequence.

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova`. | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Unified CCE AW-HDS-DDS | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server. | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install antivirus software | Follow the procedure Install Antivirus Software, on page 253. |

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 5 | | Enable .Net Framework 3.5 SP1 | Follow the procedure Enable Microsoft .Net Framework 3.5 SP1, on page 256 |
| 6 | | Install Microsoft SQL Server | Follow the procedure Install Microsoft SQL Server 2014 Standard Edition , on page 257 |
| 7 | | Install the Unified CCE | Follow the procedure Install Unified Contact Center Enterprise, on page 254. |
| 8 | | Convert the virtual machine to a template | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Unified CCE AW-HDS-DDS on the destination system. See Configure Unified CCE AW-HDS-DDS, on page 409 .

# Create Golden Template for Unified CCE Agent Peripheral Gateway

Follow this sequence of tasks to create the golden template for Cisco Unified CCE Agent Peripheral Gateway(PG).

After each task, return to this page to mark the task “done” and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova`. | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Unified CCE Agent PG | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install antivirus software | Follow the procedure Install Antivirus Software, on page 253. |

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 5 | | Install the Unified Contact Center Enterprise | Follow the procedure Install Unified Contact Center Enterprise, on page 254. |
| 6 | | Convert the virtual machine to a template | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Unified CCE Agent PG 1 Configure Unified CCE Agent PG 1, on page 412 and Agent PG 2 Configure Unified CCE Agent PG 2, on page 418 on the destination system for 4000 agent deployment. and see Configure Unified CCE Agent PG's for 12000 Agent Deployment, on page 445 for 12000 agent deployment model.

# Create Golden Template for Unified CCE VRU Peripheral Gateway

Follow this sequence of tasks to create the golden template for Cisco Unified CCE VRU PG.

After each task, return to this page to mark the task "done" and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova`. | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Unified CCE VRU PG. | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install antivirus software. | Follow the procedure Install Antivirus Software, on page 253. |
| 5 | | Install the Unified CCE. | Follow the procedure Install Unified Contact Center Enterprise, on page 254. |
| 6 | | Convert the virtual machine to a template. | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Unified CCE VRU PG on the destination system. See Configure Unified CCE VRU PG, on page 420 for 4000 agent deployment model and Configure Unified CCE VRU PG's for 12000 Agent Deployment, on page 447 for 12000 agent deployment model.

# Create Golden Template for Cisco Unified Intelligence Center

Follow this sequence of tasks to create the golden template for Cisco Unified Intelligence Center.

After each task, return to this page to mark the task "done" and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CUIC_vmv8_v2.3.ova` | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for Cisco Unified Intelligence Center | See Create Virtual Machines, on page 251. |
| 3 | | Install Cisco Unified Intelligence Center | Follow the procedure for installing VOS applications for golden templates. See Install Unified Communications Voice OS based Applications, on page 264 . |
| 4 | | Convert the virtual machine to a Golden Template | See Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process Automated Cloning and OS Customization, on page 300. After you run the automation process, you can configure the Cisco Unified Intelligence Center VMs on the destination system. See Configure Unified Intelligence Center , on page 423.

# Create Golden Template for Live Data Reporting System

Follow this sequence of tasks to create the golden template for Live Data.

After each task, return to this page to mark the task "done" and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download `UCCELD_11.0_CVOS_vmv8_v1.0.ova` | See Create Virtual Machines, on page 251 |

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 2 | | Create the virtual machine for Live Data | See Create Virtual Machines, on page 251. |
| 3 | | Install Live Data Reporting Server. | Follow the procedure for installing VOS applications for golden templates. See Install Unified Communications Voice OS based Applications, on page 264. |
| 4 | | Install VMware Tools | Follow the procedure Install VMware Tools, on page 252 |
| 5 | | Convert the virtual machine to a Golden Template | See Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Live Data VMs on the destination system. See Configure Live Data Reporting System, on page 423.

# Create Golden Template for Small Contact Center Agent Deployment

Follow this sequence of tasks to create the golden template for small contact center agent deployment for Cisco HCS for Contact Center.

After each task, return to this page to mark the task “done” and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Create Golden Template for Unified CCE Rogger, on page 268 | HCS Shared Core Component |
| 2 | | Create Golden Template for Unified CCE AW-HDS-DDS, on page 269 | HCS Shared Core Component |
| 3 | | Create Golden Template for Unified CCE Agent Peripheral Gateway, on page 270 | HCS Sub Customer Component |
| 4 | | Create Golden Template for Unified CCE VRU Peripheral Gateway, on page 271 | HCS Shared Core Component |

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 5 | | Create Golden Template for Unified CVP Server, on page 259 | HCS Shared Core Component |
| 6 | | Create Golden Template for Unified CVP OAMP Server, on page 261 | HCS Shared Core Component |
| 7 | | Create Golden Template for Unified CVP Reporting Server, on page 262 | HCS Shared Core Component |
| 8 | | Create Golden Template for Cisco Finesse, on page 264 | HCS Sub Customer Component |
| 9 | | Create Golden Template for Cisco Unified Intelligence Center , on page 272 | HCS Shared Core Component |
| 10 | | Create Golden Template for Cisco Unified Communications Manager, on page 266 | HCS Sub Customer Component |
| 11 | | Create Golden Template for Live Data Reporting System, on page 272 | HCS Core Component |

# Create Golden Template for 12000 Agent Deployment

Follow this sequence of tasks to create the golden template for 12000 agent deployment for Cisco HCS for Contact Center.

After each task, return to this page to mark the task “done” and continue the sequence.

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 1 | | Create Golden Template for Unified CCE Router, on page 275 | HCS Core Component |
| 2 | | Create Golden Template for Unified CCE Logger, on page 276 | HCS Core Component |
| 3 | | Create Golden template for Unified CCE AW-HDS, on page 277 | HCS Core Component |
| 4 | | Create Golden Template for Unified CCE HDS-DDS, on page 278 | HCS Core Component |
| 5 | | Create Golden Template for Unified CCE Agent Peripheral Gateway, on page 270 | HCS Core Component |
| 6 | | Create Golden Template for Unified CCE VRU Peripheral Gateway, on page 271 | HCS Core Component |

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 7 | | Create Golden Template for Unified CVP Server, on page 259 | HCS Core Component |
| 8 | | Create Golden Template for Unified CVP OAMP Server, on page 261 | HCS Core Component |
| 9 | | Create Golden Template for Unified CVP Reporting Server, on page 262 | HCS Core Component |
| 10 | | Create Golden Template for Cisco Finesse, on page 264 | HCS Core Component |
| 11 | | Create Golden Template for Cisco Unified Intelligence Center , on page 272 | HCS Core Component |
| 12 | | Create Golden Template for Cisco Unified Communications Manager, on page 266 | HCS Core Component |
| 13 | | Create Golden Template for Live Data Reporting System, on page 272 | HCS Core Component |

# Create Golden Template for Unified CCE Router

Follow this sequence of tasks to create the golden template for Cisco Unified CCE Router.

After each task, return to this page to mark the task " done " and continue the sequence.

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova`. | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Unified CCE Router. | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install Anti-Virus software. | Follow the procedure Install Antivirus Software, on page 253. |

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 5 | | Install the Unified CCE. | Follow the procedure Install Unified Contact Center Enterprise, on page 254. |
| 6 | | Convert the virtual machine to a template | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Unified CCE Router on the destination system. See Configure the Unified CCE Router, on page 405.

# Create Golden Template for Unified CCE Logger

Follow this sequence of tasks to create the golden template for Cisco Unified CCE Logger.

After each task, return to this page to mark the task " done " and continue the sequence.

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova`. | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Unified CCE Logger | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server. | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install Anti-Virus software | Follow the procedure Install Antivirus Software, on page 253. |
| 5 | | Enable .Net Framework 3.5 SP1 | Follow the procedure Enable Microsoft .Net Framework 3.5 SP1, on page 256 |
| 6 | | Install Microsoft SQL Server. | Follow the procedure Install Microsoft SQL Server 2014 Standard Edition , on page 257. |

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 7 | | Install the Unified CCE | Follow the procedure Install Unified Contact Center Enterprise, on page 254. |
| 8 | | Convert the virtual machine to a template | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Unified CCE Logger on the destination system. See Configure Unified CCE Logger , on page 439.

# Create Golden template for Unified CCE AW-HDS

Follow this sequence of tasks to create the golden template for Cisco CCE Unified AW-HDS.

After each task, return to this page to mark the task " done " and continue the sequence.

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 1 | | Download HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova. | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Unified CCE AW-HDS. | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server. | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install Anti-Virus software | Follow the procedure Install Antivirus Software, on page 253. |
| 5 | | Enable .Net Framework 3.5 SP1 | Follow the procedure Enable Microsoft .Net Framework 3.5 SP1, on page 256 |
| 6 | | Install Microsoft SQL Server. | Follow the procedure Install Microsoft SQL Server 2014 Standard Edition , on page 257. |

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 7 | | Install the Unified CCE | Follow the procedure Install Unified Contact Center Enterprise, on page 254. |
| 8 | | Convert the virtual machine to a template | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Unified CCE AW-HDS on the destination system. See Configure Unified CCE AW-HDS, on page 441.

# Create Golden Template for Unified CCE HDS-DDS

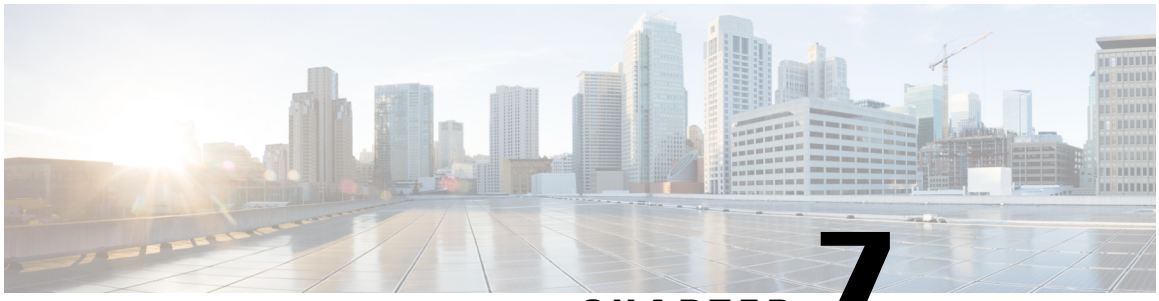
Follow this sequence of tasks to create the golden template for Cisco Unified CCE HDS-DDS.

After each task, return to this page to mark the task " done " and continue the sequence.

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova`. | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Unified CCE HDS-DDS. | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server. | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install Anti-Virus software | Follow the procedure Install Antivirus Software, on page 253. |
| 5 | | Enable .Net Framework 3.5 SP1 | Follow the procedure Enable Microsoft .Net Framework 3.5 SP1, on page 256 |
| 6 | | Install Microsoft SQL Server. | Follow the procedure Install Microsoft SQL Server 2014 Standard Edition , on page 257. |

| Sequence | Done? | Task | Notes |
|---|---|---|---|
| 7 | | Install the Unified CCE | Follow the procedure Install Unified Contact Center Enterprise, on page 254. |
| 8 | | Convert the virtual machine to a template | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Unified CCE HDS-DDS on the destination system. See Configure Unified CCE HDS-DDS, on page 443.



CHAPTER 7

# Configure Customer Instance for Network Infrastructure



## Implement UCS Platform

In HCS for Contact Center, virtualization of all Unified Computing (UC) applications and key third-party components use Cisco Unified Computing System (UCS) hardware as the platform. The HCS virtualization integrates the UCS platform and SAN, and virtualizes the target UC applications. The following sections describes the deployment of the Service Provider (SP) virtualization infrastructure.



### Set Up Basic UCS Connectivity

Cisco UCS 6100 Series Fabric Interconnects is a core part of UCS that provides network connectivity and management capabilities for attached blades and chassis. The Cisco UCS 6100 Series offers line-rate, low-latency, lossless 10 Gigabit Ethernet, and Fibre Channel over Ethernet (FCoE) functions.

The Interconnects provide the management and communication support for the Cisco UCS B-Series blades and the UCS 5100 Series blade server chassis. All chassis and all blades attached to the interconnects becomes part of a single, high availability management domain. By supporting a unified fabric, the Cisco UCS 6100 Series provides LAN and SAN connectivity for all blades in its domain.

You will require the following connections for a working UCS:

- Console connection on the 6100 Series switch.
- At least one 10 Gbps connection between the 6100 Series switch and the Fabric Extender 2104 on the chassis.
- At least one 10 Gbps connection on the 6100 Series switch for the northbound interface to a core router or switch (could be a port-channel connection).
- At least one FCoE connection between the 6100 Series switch and a Multilayer Director Switch (MDS) switch.
- Cluster link ports connected between the 6100 Series switches in a high availability deployment.

# Basic Configuration for UCS

Unified Computing System Manager (UCSM) provides centralized management capabilities, creates a unified management domain, and serves as the central nervous system of the UCS. UCSM delivers embedded device-management software that manages the system from end to end as a single logical entity through a GUI, a CLI, or, an XML API.

UCS Manager resides on a pair of Cisco UCS 6100 Series fabric interconnects using a clustered, active-standby configuration for High Availability (HA). The software participates in server provisioning, device discovery, inventory, configuration, diagnostics, monitoring, fault detection, auditing, and statistics collection.

After 6100 Series initial configuration, you can configure UCS from the GUI. You can launch the GUI from a URL that is reachable to the configured 6100 Management IP address.

- Configure UCS 6100 Server Ports, on page 282
- Configure UCS 6100 Uplink Ethernet Ports, on page 283
- Configure Uplink FC Ports, on page 283
- Acknowledge Chassis, on page 283
- Configure Server Management IP Address Pool, on page 283

## Configure UCS 6100 Server Ports

Complete the following procedure to configure UCS 6100 server ports on UCS Manager.

### Procedure

**Step 1** Choose **Equipment** > **Fabric Interconnect A(B)** > **Fixed Module** > **Unconfigured Ports** > **Port #**.

**Step 2** Click the **General** tab.

**Step 3** Click the **Configure as Server Port** option.

## Configure UCS 6100 Uplink Ethernet Ports

Complete the following procedure to configure UCS 6100 uplink ethernet ports.

### Procedure

**Step 1** Choose **Equipment** > **Fabric Interconnect A(B)** > **Fixed Module** > **unconfigured Ports** > **Port #**.

**Step 2** Click **General** tab.

**Step 3** Click **Configure as Uplink Port** option.

## Configure Uplink FC Ports

You must define the ports that are capable of passing Fibre Channel (FC) traffic as Fibre Channel uplink ports using the SAN configuration tab of the UCS Manager.

## Acknowledge Chassis

Any time there is a change in the number of links between the 6100 series switch and the blade server chassis, you must perform a chassis acknowledgment to make the UCS Manager aware of the link change which causes a rebuild of its connectivity data.

## Configure Server Management IP Address Pool

The UCSM server management IP address pool assigns an external IP addresses for each of the blade servers installed. UCS Manager uses the IP addresses in a management IP pool for external access to a server through the following:

- KVM Console
- Serial over LAN
- IPMI

Complete the following procedure to configure server management IP address pool.

### Procedure

**Step 1** Choose **Administration > Communication Management > Management IP Pool**.

**Step 2** Right-click and select **Create Block of IP Addresses**.

# Configure UCS LAN

The enabled Uplink Ethernet ports in UCS 6100 series switch forwards traffic to the next layer in the network. You can configure the LAN properties such as VLANs, MAC Pools, and vNIC templates within the LAN view in the UCS Manager.

Complete the following procedures to create VLANs and MAC pools.


- Add VLANs, on page 284
- Create MAC Pools, on page 284


## Add VLANs

In the Cisco UCS, a named VLAN creates a connection to a specific external LAN. The VLAN isolates traffic to that external LAN, which includes broadcast traffic. The name that you assign to a VLAN ID adds a layer of abstraction that you can use to globally update all servers associated with service profiles that use the named VLAN. You do not need to reconfigure servers individually to maintain communication with the external LAN. Complete the following procedure to add VLANs.

### Procedure

**Step 1** Click the **LAN** tab and then right-click the VLANs.

**Step 2** Enter the name or designation of the VLANs being added and the VLAN IDs to use.
A decision on how the named VLAN is accessible by the 6100 Series switches completes the UCS VLAN additions.

## Create MAC Pools

A MAC pool is a collection of network identities, or MAC addresses, that are unique in Layer 2 (L2) and available to be assigned to a vNIC on a server. If you use MAC pools in service profiles, you do not have to manually configure the MAC addresses to be used by the server associated with the service profile.

To assign a MAC address to a server, you must include the MAC pool in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server. Complete the following procedure to create a MAC pool.

### Procedure

**Step 1** Click the **LAN** tab.

**Step 2** Right-click **Pools** .

**Step 3** Select **Create MAC Pool**.

# Configure UCS SAN

Each UCS 6120 fabric interconnect has an open slot to add expansion modules that add Fibre Channel ports for SAN connectivity. You can enable these ports and their attributes through the SAN scope of the UCS Manager.

Complete the following procedures to configure SAN properties such as VSANs, Fibre Channel uplink ports, World Wide Node Name (WWNN) pools, World Wide Port Name (WWPN) pools, and Virtual Host Bus Adapter (vHBA) templates, within the SAN view in the UCS Manager.


- Create VSANs, on page 285
- Associate VSAN with an FC Uplink Port, on page 285
- Create WWNN Pools, on page 286
- Create WWPN Pools, on page 286


## Create VSANs

A named VSAN creates a connection to a specific external SAN. The VSAN isolates traffic to that external SAN, including broadcast traffic. The traffic on one named VSAN knows that the traffic on another named VSAN exists, but cannot read or access that traffic.

Like a VLAN name, the name that you assign to a VSAN ID adds a layer of abstraction that allows you to globally update all servers associated with service profiles that use the named VSAN. You do not need to reconfigure the servers individually to maintain communication with the external SAN. You can create more than one named VSAN with the same VSAN ID.

In a cluster configuration, you can configure a named VSAN to be accessible only to the FC uplinks on one fabric interconnect or to the FC uplinks on both fabric interconnects. Complete the following procedure to create VSAN.

### Procedure

**Step 1** Click the **SAN** tab.

**Step 2** Right-click the VSANs and select create VSAN.

**Step 3** Configure the following to complete the VSAN configuration:

a) Enter a name for the VSAN.
b) Enter the VSAN interaction with Interconnect fabric(s).
c) Enter a VSAN ID.
d) Enter the FCoE VLAN.

## Associate VSAN with an FC Uplink Port

After you create a VSAN, you must associate it with a physical FC interface. Complete the following procedure to associate VSAN with an FC uplink port.

### Procedure

**Step 1** Click the **Equipment** tab.
**Step 2** Open the target FC port and select the desired VSAN from the drop-down list
**Step 3** Click **Ok** and save the changes.

## Create WWNN Pools

A World Wide Node Name (WWNN) pool is one of two pools used by the FC vHBAs in the UCS. You can create separate pools for WWNNs assigned to the server and World Wide Port Names (WWPNs) assigned to the vHBA. The pool assigns WWNNs to servers. If you include a WWNN pool in a service profile, the associated server is assigned a WWNN from that pool.

### Procedure

**Step 1** Click the **SAN** tab.
**Step 2** Choose **Pools**, select WWNN pools and expand it.
**Step 3** Choose WWNN Pool node-default
**Step 4** Right-click the **Create WWN Block**.
**Step 5** Enter the pool size and click **OK**.

## Create WWPN Pools

A WWPN is the second type of pool used by Fibre Channel vHBAs in the UCS. WWPN pool assigns WWPNs to the vHBAs. If a pool of WWPNs is included in a service profile, the associated server is assigned a WWPN from that pool.

### Procedure

**Step 1** Click the **SAN** tab.
**Step 2** Choose **Pools**, select WWPN pools and expand it.
**Step 3** Choose WWPN Pool node-default.
**Step 4** Right-click **Create WWPN Block**.
**Step 5** Enter the pool size and click **OK**.

# Configure UCS B Series Blade Server

Cisco UCS Manager uses service profiles to provision servers and their I/O properties. Server, network, and storage administrators creates the service profiles and stores in the Cisco UCS 6100 Series fabric interconnects. Service profiles are centrally managed and stored in a database on the fabric interconnect.

Service profile provides the following services:

- Service profiles are the central concept of Cisco UCS and thus each service profile ensures that the associated server hardware is configured to support the applications that it hosts.
- The service profile maintains the server hardware configurations, interfaces, fabric connectivity, and server, and network identity. This information is stored in a format that you can manage through Cisco UCS Manager.

Service profile provides the following advantages:

- Simplifies the creation of service profiles and ensures consistent policies within the system for a given service or application as service profile templates are used. This approach makes easy to configure one server or 320 servers with thousands of virtual machines, decoupling scale from complexity.
- Reduces the number of manual steps that need to be taken, helping reduce the chance for human error, improving consistency, and reducing server and network deployment times.
- Dissociates hardware specific attributes from the design. If a specific server in the deployment is replaced, the service profile associated with the old server is applied to the newly installed server allowing for near seamless replacement of hardware if needed.

# Configure MDS

Configure the following MDS to place the UCS server blade vHBAs and SAN Port World Wide Name (PWWN) under the same zone and activate the zoneset.

- Configure MDS-A, on page 287
- Configure MDS-B, on page 288

## Configure MDS-A

The CLI configuration for MDS-A is as follows:

```
fcalias name scale-esxi-c5b1-vHBA0 vsan 600
    member pwwn 20:00:00:25:b5:02:13:7e
fcalias name cx4-480-spb-b0 vsan 600
    member pwwn 50:06:01:68:46:e0:1b:e0
fcalias name cx4-480-spa-a1 vsan 600
    member pwwn 50:06:01:61:46:e0:1b:e0
zone name zone33 vsan 600
    member fcalias cx4-480-spb-b0
    member fcalias cx4-480-spa-a1
    member fcalias scale-esxi-c5b1-vHBA0
zoneset name scale_zoneset vsan 600
```

```
    member zone33
zoneset activate name scale_zoneset vsan 600
```

### Configure MDS-B

The CLI configuration for MDS-B is as follows:

```
fcalias name scale-esxi-c5b1-vHBA1 vsan 700
    member pwwn 20:00:00:25:b5:02:13:6e
fcalias name cx4-480-spa-a0 vsan 700
    member pwwn 50:06:01:60:46:e0:1b:e0
fcalias name cx4-480-spb-b1 vsan 700
    member pwwn 50:06:01:69:46:e0:1b:e0
zone name zone33 vsan 700
    member fcalias cx4-480-spa-a0
    member fcalias cx4-480-spb-b1
    member fcalias scale-esxi-c5b1-vHBA1
zoneset name scale_zoneset vsan 700
    member zone33
zoneset activate name scale_zoneset vsan 700
```

## Configure SAN

Complete the following procedure to configure SAN.

**Procedure**

**Step 1** Create Logical Unit Numbers (LUN) for boot (recommended to use the lowest LUN number, and make sure the LUN number for shared storage are higher than the ones used for boot), 8GB should be sufficient.

**Step 2** Register the hosts. Navigate to Storage System Connectivity Status and register each unknown vHBA.

**Step 3** Configure the following to create a storage group:

a) Create a storage group
b) Add LUN
c) Add Hosts

# ESX Boot from SAN

Complete the following procedures to configure for booting from SAN:


- Configure UCS B Series Blade Server, on page 289
- View Multilayer Director Switch, on page 289
- Configure SAN on Storage Device, on page 289
- Install ESX, on page 290

# Configure UCS B Series Blade Server

Complete the following procedure to configure the UCS.

### Procedure

**Step 1** Log in to the UCS Manager.

**Step 2** Click the **Servers** tab and choose the service profile that corresponds to the server for configuring the boot from SAN.

**Step 3** Click the **Servers** tab. Choose **Policies > Boot Policies** to create a boot policy with SAN storage parameters.

**Step 4** Assign this boot policy to the service profile of the server and click **OK**.

**Step 5** Click **Yes** in the dialog box **Modify Boot Policy**.
The server reboots after saving the boot policy.

# View Multilayer Director Switch

Complete the following procedure to view the Multilayer Director Switch (MDS).

### Procedure

**Step 1** Log in into your MDS (Telnet or SSH).

**Step 2** Enter the login ID and password.

**Step 3** Enter the following command and press **Enter**:
**show flogi database**

You should see a port name for each interface.

**Step 4** Match the port name in the database with the name listed in the UCS Manager under the HBA WWPN.

**Note** If you do not find the matching port in the database, you need to select a valid VSAN in the UCS Manager.

# Configure SAN on Storage Device

Complete the following procedure to configure the SAN on the storage device.

### Procedure

**Step 1** Verify that the WWPN number and WWNN number of the host are visible in SAN.
The WWPN and WWNN in SAN should match with the numbers in UCS Manager.

**Step 2** Configure a LUN on SAN for the server to boot (use 20 GB to 50 GB).

**Step 3** Create a storage group in SAN. Add the specific host to this storage group for access.
The host ID of the LUN associated to the host should be same as the LUN ID used on the boot policy in UCS Manager (usually 0).

# Install ESX

Complete the following procedure to install the ESX.

### Procedure

**Step 1** Choose **Virtual Media**, click **Add Image** and browse to the path and select ESXi iso image.

**Step 2** Click **Open**.

**Step 3** Check the check box **Mapped**. Server boots from the ISO image.

**Step 4** Access the KVM console of the server from UCS Manager and edit the boot order in the BIOS to the new SAN configuration.

**Step 5** Install ESXi on the LUN.
It should now reboot and come up booting from the SAN.

**Step 6** Reuse the boot policy on all servers that needs to boot from SAN.

**Step 7** If you install ESXi on the local disk, make sure to remove the disks or clear the ESXi data on them.

# Add ESX Host to vCenter

Complete the following procedure to add hosts to vCenter.

### Procedure

**Step 1** Add hosts using the vSphere client, using the Add Host Wizard. Enter the IP address of the host and the username/password of the ESXi server, which was configured when the ESXi software was loaded on the host.

**Step 2** Assign a license to the Host.

**Step 3** Review the options you have selected and click then **Finish** to add the Host

### What to Do Next

After you add a host, confirm by navigating to the **Home** > **Inventory** > **Hosts**.

# Deploy Nexus 1000v

VMware vSphere provisions Nexus 1000V platform using and the Nexus 1000V Installer App. The following sections describe how to prepare and install the Cisco Nexus 1000V software.



## Cisco Nexus 1000V Installer App Prerequisites

**Note** The Installation Application requires you to satisfy all the prerequisites.

If you migrate the host and adapters from the VMware vSwitch to the Cisco Nexus 1000V DVS:

- The host must have one or more physical NICs on each VMware vSwitch in use
- The VMware vSwitch must not have any active VMs
- To prevent a disruption in connectivity during migration, any VMs that share a VMware vSwitch with port groups used by the VSM must be powered off
- Make sure no VEMs were previously installed on the host where the VSM resides
- You must have administrative credentials for the vCenter Server
- The java.exe file must be located within the search path defined in your system

The ESX or ESXi hosts to be used for the Cisco Nexus 1000V have the following prerequisites:

- You have already installed and prepared the vCenter Server for host management using the instructions from VMware
- You have already installed the VMware Enterprise Plus license on the hosts
- The host must have one or more physical NICs on each VMware vSwitch that is being used
- All VEM hosts must be running ESX/ESXi 5.1 or later releases
- You have installed the appropriate vCenter Server and VMware Update Manager (VUM) versions
- When you perform any VUM operation on hosts that are a part of a cluster, ensure that VMware HA, VMware fault tolerance (FT), and VMware distributed power management (DPM) features are disabled for the entire cluster. Otherwise, VUM cannot install the hosts in the cluster
- If the hosts are in ESXi stateless mode, then enable the **Pxe Booted ESXi host settings** available under **Home** > **Solutions and Applications** > **Update Manager** > **Configuration** > **ESXi host/cluster**
- You have a copy of your VMware documentation available for installing software on a host

# Installing the VSM Software using Cisco Nexus 1000V Installer App

### Before You Begin

- You should have the following information:
  - Control VLAN ID
  - Packet VLAN ID
  - Management VLAN ID
  - Domain ID
  - Management IP address
  - Subnet mask
  - Gateway IP address
  - SVS datacenter name
  - Control, packet, and management port groups
  - Management VLAN ID of ESXi hosts
- You have the JDK version 1.6 or later installed on the host running the Cisco Nexus 1000V Installer App.

### Procedure

**Step 1** Download the Cisco Nexus 1000V file (Nexus1000v.4.2.1.SV2.2.1.zip) on to the local machine and unzip the file.

**Step 2** Double-click the application file ( **Nexus1000V-install_CNX.jar**) or at the command-line interface, navigate to **%Nexus%\VSM\Installer_App** folder and enter the following command to start the Cisco Nexus 1000V Installer App: **java -jar Nexus1000V-install_CNX.jar**

**Step 3** Click the **Cisco Nexus 1000V Complete Installation** radio button.

**Step 4** Click the **Custom** radio button.

**Step 5** After reading the prerequisites, click **Next**.

**Step 6** In the **vCenter Server Credentials** screen, do the following:

a) Enter the following vCenter credentials:

- IP Address
- Port (https only)

**Note** This field is prepopulated but can be modified.

- User ID
- Password

b) Click **Next**.

**Step 7** In the **Custom Configuration Data** screen, click the **Browse** button for the **Host 1 (Primary VSM's Host) IP Address / Name** field.

**Step 8** In the **Host 1 Selection vCenter Inventory** screen, do the following:

a) Choose the host for the primary VSM.

b) Click **Select Host**.

The **Host 1 IP Address / Name** and **Data Store** fields are populated. If needed Data Center can be changed by clicking the **Browse** button and select another Data Center.

**Step 9** In the **Host 1 vSwitch Custom Configuration Data** screen, click the **Browse** button for the **Host 1 vSwitch** field.

**Step 10** In the **1 vSwitch Selection** screen, do the following:

a) Choose a **vSwitch**.

b) Click **Select**.

The **Host 1 vSwitch** field is populate.

**Step 11** The **Host 2 IP Address Custom Configuration Data** screen, click the **Browse** button for the **Host 2 IP Address / Name** field.

**Step 12** In the **Host 2 Selection vCenter Inventory** screen, do the following:

a) Choose the host for the secondary VSM.

b) Click **Select Host**.

The **Host 2 IP Address / Name** and **Data Store** fields are populated. If needed Data Center can be changed by clicking the **Browse** button and select another Data Center.

**Step 13** In the **Host 2 vSwitch Custom Configuration Data** screen, click the **Browse** button for the **Host 2 vSwitch** field.

**Step 14** In the **Host 2 vSwitch Selection** screen, do the following:

a) Choose a vSwitch.

b) Click **Select**.

The **Host 2 Switch Custom Configuration Data** screen, click the **Browse** button for **Host 2 vSwitch** field.

**Step 15** In the **Switch Name** text box, enter the **Switch Name** (can be any meaningful name)

**Step 16** In the **Admin Password** text box, enter the **VSM Admin Password**.

**Step 17** In the **Confirm Admin Password** text box, enter the **Admin Password**

**Step 18** In the **Virtual Machine Name** text box, enter the **Virtual Machine Name** (can be any meaningful name).

**Step 19** In the **OVA Image Location** text box, click the **Browse** button and go to location in **Step 1** and select OVA file (nexus-1000v.4.2.1 SV2.2.1 ova) under **VSM\Install** folder.

**Step 20** In the **Layer 2 / Layer 3 Connectivity** radio buttons, select the **Layer L3** radio button (The layer three mode is selected by default).

**Step 21** In the **VSM IP Address** text box, enter the **VSM IP Address**.

**Step 22** In the **Subnet Mask** text box, enter the **Subnet Mask**.

**Step 23** In the **Gateway IP Address** text box, enter the **Gateway IP Address**.

**Step 24** In the **Domain ID** text box, enter the **Domain ID**.

**Step 25** Check the **Enable Telnet** check box, if you want to enable Telnet (By default, only SSH is enabled)

**Step 26** In the **Data Center Name** text box, click the **Browse** button for the **Data Center Name** and choose **Data Center** from the list.

**Step 27** Click the **Browse** button for the Control Port Group **Port Group Name**

**Step 28** In the **Make a Selection** screen, do the following:

a) Choose a VlanID.
b) Click **Select**.

**Step 29** For the **Control Port Group**

a) Choose the **Choose Existing** radio button.
b) For the **Port Group Name**, click the **Browse** button and select **VLANID**.

**Step 30** For the **Management Port Group**

a) Choose the **Choose Existing** radio button.
b) For the **Port Group Name**, click the **Browse** button and select **VLANID**.

**Step 31** In the **Management VLAN** text box, enter the **Management VLAN ID**.

**Step 32** In the **Migrate Host(s) to DVS** radio buttons, select **Yes**.

**Step 33** Click **Save Configuration** button if you want to save the settings to a configuration file.

**Step 34** Click **Next**.

**Step 35** In the **Custom Configuration Review** screen, do the following:

a) Validate the input.
b) Click **Next**.

The **Custom Configuration Review Installation Progress** screen opens. when the installation completes, the **Confirmation** screen opens.

**Step 36** In the **Custom Cofirmation** screen, do one of the following:

a) Click **Yes**, if you want to add more modules and continue the next step.
b) Click **No**, if you don't want to add more modules and proceed with the steps as prompted to complete the process.

**Step 37** In the **Confirmation** screen, complete the tasks as follows:

a) Do one of the following:

- Click **Install VIB** to install VIBs on this host.
- Click **Install VIB and add module to Nexus 1000V** to install VIBS on this host and move them to the Cisco Nexus 1000V.

b) In the **Management VLAN** text box, enter the **Mangement VLAN ID**
c) Click **Next** and the **Host Selection** screen opens.

**Step 38** In the **Host Selection** screen, do the following:
a) Choose the hosts you want to add.
b) Click **Next**.

**Step 39** In the **Host Review** screen, do the following:
a) Review the entries.
b) Click **Finish**.

**Step 40** In the **Custom Summary** screen, click **Close**.

# Installing the VEM Software Using the Cisco Nexus 1000V Installer App

- When the Cisco Nexus 1000V Installer App installs VEMs, it migrates all VEM kernels and their corresponding vmnics across vSwitches to the Cisco Nexus 1000V VEMs
- If a particular VEM is capable of hosting VSMs, the network administrator must manually allow a control VLAN in the uplink port profile of VEMs in Layer 3 deployment mode for VSM HA communication

### Before You Begin

You should have the following information:

- vCenter IP address
- vCenter user ID
- vCenter password
- VSM IP address
- VSM password

**Note** The hosts that will be installed as VEMs should not have any Cisco Nexus 1000V vSphere Installation Bundle (VIB) files. Uninstall any Cisco Nexus 1000V VIBs before starting the Cisco Nexus 1000V Installer App.

### Procedure

**Step 1** Double-click the application file (**Nexus1000V-install_CNX.jar**) or at the command-line interface, navigate to **%Nexus%\VSM\Installer_App** folder and enter the following command to start the Cisco Nexus 1000V Installer App: **java -jar Nexus1000V-install_CNX.jar**.

**Step 2** In the **Cisco Nexus 1000V Installer App** screen, click the **Virtual Ethernet Module Installation** radio button.

**Step 3** After reading the prerequisites, click **Next**.

**Step 4** In the **VEM Enter vCenter Credentials** screen, do the following:

a) Enter the following vCenter Credentials:

- IP address
- Port (https only)

**Note** This field is prepopulated but can be modified.

- **User ID** (for a vCenter user with administrator-level privileges)
- **Password** (for a vCenter user with administrator-level privileges)

b) Click **Next**.

**Step 5** In the **Enter VSM IP & Credentials** screen, do the following:

a) Enter the following Credentials:

- VSM IP address
- VSM Password

b) Click **Next**.

**Step 6** In the **Confirmation** screen, do one the following:

a) Do one of the following:

- Click **Install VIB** to install VIBs on this host
- Click **Install VIB and add module to Nexus 1000V** to install VIBS on this host and move them to the Cisco Nexus 1000V.

b) In the **Management VLAN** text box, enter the **Management VLAN ID**.

c) Click the **Next** button and the **Hosts Selection** screen opens.

**Step 7** In the **Host Selection** screen, do the following:

a) Choose the hosts you want to add.

b) Click **Next**.

**Step 8** In the **Host Review** screen, do the following:

a) Review the entries.

b) Click **Finish**.

**Step 9** In the **Custom Summary** screen, click **Close**.

# Configure Cisco Nexus

Complete the following procedure to configure the Cisco Nexus 1000V switch for Cisco HCS for Contact Center.

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

### Procedure

**Step 1** Configure the Nexus port profile uplink:

```
port-profile type ethernet n1kv-uplink0
vmware port-group
switchport mode trunk
switchport trunk allowed vlan <vlan ID's>
channel-group auto mode on mac-pinning
no shutdown
system vlan <vlan ID> # Customer specific native vlan ID identified in the switch
state enabled
```

**Step 2** Configure the public VM port profiles:

```
port-profile type vethernet Visible-VLAN
vmware port-group
switchport mode access
switchport access vlan <vlan ID> # Customer specific public vlan ID defined in the switch
no shutdown
state enabled
```

**Step 3** Configure the private VM port profiles:

```
port-profile type vethernet Private-VLAN
vmware port-group
switchport mode access
switchport access vlan <vlan ID> # Customer specific private vlan ID defined in the switch
no shutdown
state enabled
```

# Add Second Customer Instance in Single Blade for 500 Agent Deployment

Perform the following procedure to add a second customer instance for a single blade in a 500 agent deployment model.

### Procedure

**Step 1** Create new Data Stores (if needed) and associate the corresponding LUNs.

**Step 2** Create and configure a new VLAN on UCS Manager:

a) Log in to UCS Manager console and click **LAN**.
b) Navigate to **Create VLANs**.
c) Enter the following VLAN Details:

- Name
- ID
- Fabric and Sharing type

d) Click **Servers** tab and select **VNIC**.
e) Select **Ethernet** and click **Modify VLANs**.
f) Verify the VLANs that you want to associate with a particular server.

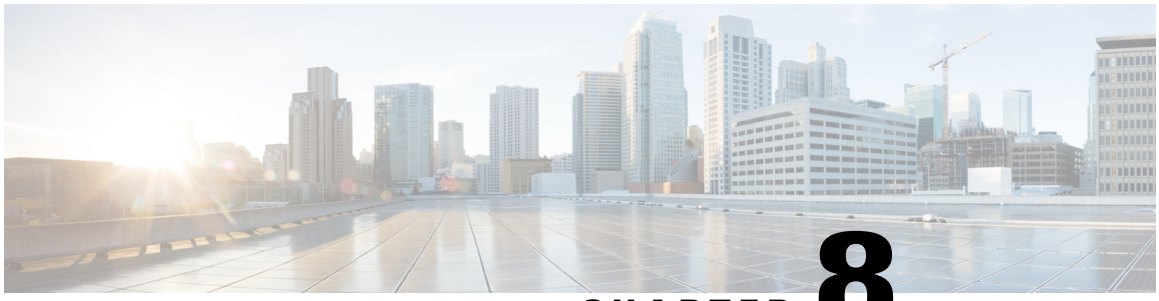
**Step 3** Enter the following commands in the Nexus prompt to configure Nexus to add one more VLAN:

- **config t**
- **vlan <VLAN ID>**
- **no shut**
- **end**

**Step 4** Refer to Configure Cisco Nexus section to add one more Public & Private VM port profiles. For more information, see Configure Cisco Nexus, on page 297.

**Step 5** Configure the following details to associate the second 500-agent virtual machines with the new VLAN:

a) Log in to the Vcenter Server using VMware Infrastructure Client.
b) Select a VM.
c) Select **Edit Settings**.
d) Select **Network Adapters**.
e) Select the newly created VM port profile from the list.
f) Click **OK**.

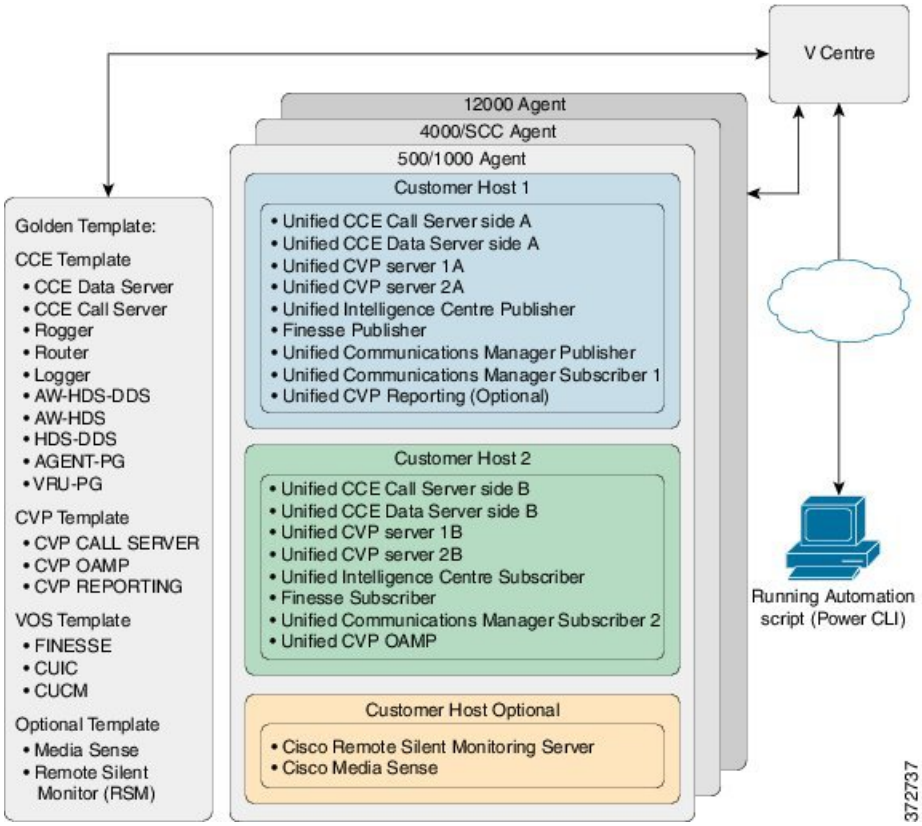


CHAPTER 8

# Clone and OS Customization



## Clone and OS Customization Process



# Automated Cloning and OS Customization

For automation software and download information see, Automation Software, on page 50

- Automated Cloning and OS Customization Using Golden Templates , on page 300
- Automated Cloning and OS Customization Using OVF , on page 306

# Automated Cloning and OS Customization Using Golden Templates

Ensure that required software is downloaded for Automated Cloning. For more information see, Automation Software, on page 50.

| Sequence | Task | Done |
|---|---|---|
| 1 | Download Golden Template Automation Tool, on page 300 | |
| 2 | Complete Automation Spreadsheet, on page 301 | |
| 3 | Run Automation Script, on page 303 | |
| 4 | OS Customization Process, on page 304 | |

## Download Golden Template Automation Tool

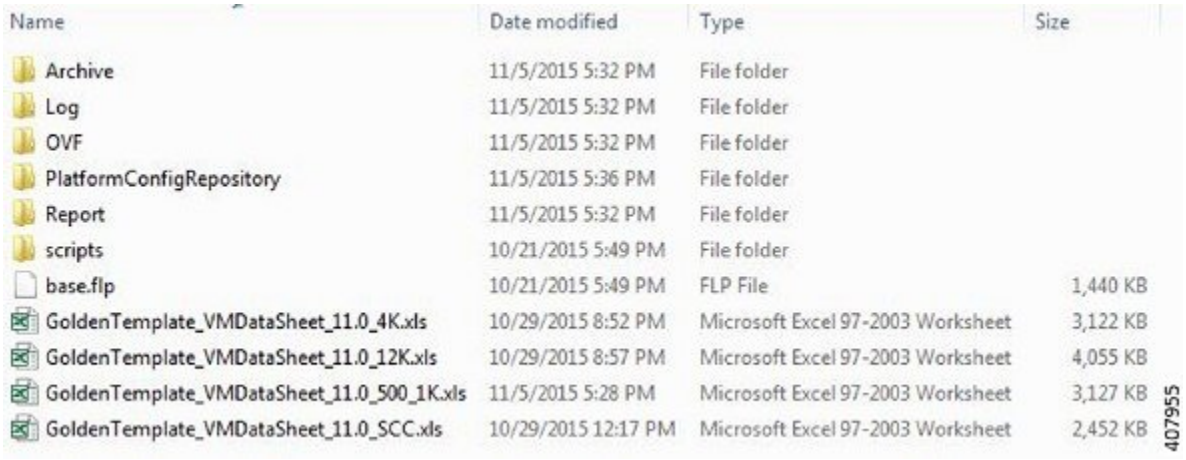
Golden Template Tool is required for automated cloning of Golden Templates and deploying the customized Virtual machines in a customer instance. Download and extract the Golden Template Tool to the root of the **C: drive** on your system. You can browse the automation scripts using VMware vSphere PowerCLI.

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.

***Figure 62: Download Automation Tool***




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.

## 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. See Automation Tool Spreadsheet, on page 790 for Automation Spreadsheet column description.

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* |

| Column | Domain-based VM | Workgroup-based VM | VOS-based VM |
|---|---|---|---|
| SOURCE_VMNAME | | | |
| 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* |
| 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* | | |

| Column | Domain-based VM | Workgroup-based VM | VOS-based VM |
|---|---|---|---|
| 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_NETWORK | | | |

## Run Automation Script

### Before You Begin

Download and install VMware vSphere PowerCLI 5.0 on the client computer. http://downloads.vmware.com/d/details/pcli50/dHRAYnQlKmpiZHAlJQ

**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

| | Command or Action | Purpose |
|---|---|---|
| **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 | Change the execution policy to run unsigned scripts on your local computer and signed sc |

| | Command or Action | Purpose |
|---|---|---|
| | Unrestricted, then enter Y. | |
| **Step 4** | Enter the CD < GoldenTemplate directory> command. | |
| **Step 5** | Run the automation script using the following syntax: | **Syntax:** **<Path to the script> <Path of the spreadsheet> <vCenter IP / Hostname> <vCenter User> <Password to connect to vCenter>**<br>***Example:*** `.\scripts\DeployVM.PS1 C:\GoldenTemplate\GoldenTemplate_VMDataS` **testvCenter testuser testpassword**<br><br>This starts the script that parses and validates the data, creates entries in the GoldenTemplate the completion percentage on the screen and generates the `Status Report` in the `Repor`<br><br>***Figure 63: Status Report of Golden Template Tool*** |

**Status Report of Golden Template Tool**

| VM NAME | OPERATION | HOST IP | DATASTORE NAME | STATUS | DESCR |
|---|---|---|---|---|---|
| CCE-Callserver | CREATE VM from an OVF | 10.86.129.60 | DS2-129-60 | Success | VM deployed successfu |
| CUIC | Export VM to OVF | ---- | ---- | Success | VM to OVF conversion |
| CCE-Dataserver | Template from an OVF | 10.86.129.61 | DS2-129-61 | Success | OVF to Golden Templa |
| CUCM-Publisher | CREATE VM from A Template | 10.86.129.61 | DS2-129-61 | Success | VM deployed successfu |

Log File

### What to Do Next

Click the **Log File** link to debug error conditions and to consult Cisco Support.

## OS Customization Process

| Sequence | Task | Done |
|---|---|---|
| **Windows Customization Process** | | |
| 1 | Validate Network Adapter Settings and Power On, on page 305 | |

| Sequence | Task | Done |
|---|---|---|
| 2 | Edit Registry Settings and Restart VM, on page 305 | |
| **VOS Customization Process** | | |
| 1 | Configure DNS Server, on page 437 | |
| 2 | Configure Host in DNS Server , on page 438 | |
| 3 | Validate Network Adapter Settings and Power On, on page 305 | |

## 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. For more information see, http://docwiki.cisco.com/wiki/Recover_from_Pressing_Ctrl-Alt-Del_During_Power-On .

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

## 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 300 | |
| 2 | Complete Automation Spreadsheet for Export, on page 307 | |
| 3 | Run Automation Script for Export , on page 307 | |
| 4 | Transport to Desired Location, on page 308 | |
| 5 | Ensure Readiness of the Location, on page 309 | |
| 6 | Complete the Spreadsheet for Import, on page 309 | |
| 7 | Run Automation Script for Import, on page 312 | |
| 8 | OS Customization Process, on page 304 | |

## 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 49: 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. | CallServerSideA |
| GOLDEN_TEMPLATE_NAME | New Name for the Exported VM cannot contain spaces or special characters. Maximum of 32 characters. | My CallServer |

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 then install VMware vSphere PowerCLI 5.0 on the client computer from which the automation scripts will be run. http://downloads.vmware.com/d/details/pcli50/dHRAYnQlKmpiZHAlJQ

**Procedure**

1. Launch **VMware vSphere PowerCLI (32-Bit)** as administrator.
2. Enter **get-executionPolicy** command to determine whether the Restricted Execution policy is in effect or is unrestricted.
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
4. Enter cd < GoldenTemplate directory> command.
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* |

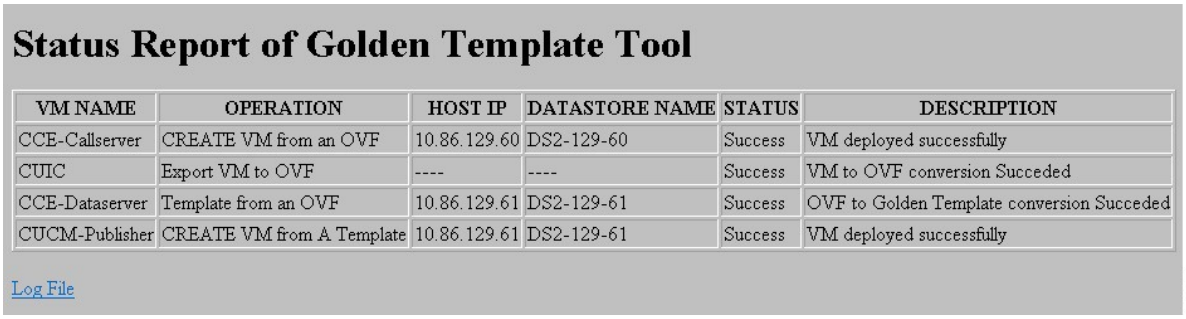
This starts a script that parses the data, validates the data, and creates entries in the *OVF* folder in the GoldenTemplate directory.

If the script runs successfully, it takes several hours to complete.

If there are errors, the script fails but keeps running. The errors display on the screen and are stored in the log file.

Completion of the script generates a status report in the *Report* folder. The status report has a link to the Log file. Refer this file to debug error conditions and to consult with Cisco Support.

***Figure 64: Status Report of Golden Template Tool***



**Status Report of Golden Template Tool**

| VM NAME | OPERATION | HOST IP | DATASTORE NAME | STATUS | DESCRIPTION |
|---|---|---|---|---|---|
| CCE-Callserver | CREATE VM from an OVF | 10.86.129.60 | DS2-129-60 | Success | VM deployed successfully |
| CUIC | Export VM to OVF | ---- | ---- | Success | VM to OVF conversion Succeded |
| CCE-Dataserver | Template from an OVF | 10.86.129.61 | DS2-129-61 | Success | OVF to Golden Template conversion Succeded |
| CUCM-Publisher | CREATE VM from A Template | 10.86.129.61 | DS2-129-61 | Success | VM deployed successfully |

Log File

390140

## 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

## Complete the Spreadsheet for Import

To complete the automation spreadsheet for import, use the information provided in the table below. The import automation script requires this information to import the virtual machines to the desired ESXi host.

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

***Table 50: Complete Automation Spreadsheet Columns for Import***

| Column | Description | Example |
|---|---|---|
| CREATEVM | Select **YES** to create a VM.<br>Select **NO** to create a template. | YES |
| OPERATION | Select **ImportServer**. | ImportServer |
| CUSTOMIZATION | Select **YES** to apply values in the spreadsheet to the imported server.<br>Select **NO** if you do not have the values at the time you complete the spreadsheet.<br>If you do have the values but set to **NO**, the values will not be applied. | YES |
| SOURCE_HOST_IP | Leave Blank | Leave Blank |
| SOURCE_DATASTORE_NAME | Leave Blank | Leave Blank |
| SOURCE_VMNAME | Leave blank. | Leave blank. |
| GOLDEN_TEMPLATE_NAME | Enter the name of the exported golden template that is in *OVF* Subfolder. | GTCS-1A |

| Column | Description | Example |
|---|---|---|
| NEW_VM_NAME | The name for the new VM. Should not contain spaces or special characters. Maximum of 32 characters. | CallServerSideA |
| DEST_HOST_IP | The IP address or the DNS name of the ESXi Host for the new VM. | xx.xx.xxx.xxx |
| DEST_DATASTORE_NAME | The name of the Datastore for the new VM. | datastore2(1) |
| PRODUCT_VERSION | Currently this field is applicable only for VOS Product | ?? 10.0(x)? |
| COMPUTER_NAME | The NET BIOS name for the new computer. Maximum 15-characters. Do not use special characters. | Demo-CallSrvA |
| WORK_GROUP | Dropdown:<br>**YES** adds the VM to a WorkGroup and enables WORK_GROUP_NAME.<br>**NO** adds the VM to a domain and enables DOMAIN_NAME,<br>DOMAIN_USER, and DOMAIN_PASSWORD. | NO |
| WORK_GROUP_NAME | Enter the Workgroup name. Used only if WORK_GROUP is set to **YES**. | NA |
| DOMAIN_NAME | Enter the Domain name. Used only if WORK_GROUP is set to **NO** | xx.xx.xxx.xxx |
| TIME_ZONE_LINUX_AREA | Drop-down selection of the timezone area to be set Unified CM. For the United States of America, select *America*. | America |
| TIME_ZONE_LINUX_LOCATION | Drop-down selection of the timezone location to be set for Unified CM, CUIC, or Finesse. | Eastern |
| TIME_ZONE_WINDOWS | Drop-down selection of the timezone to be set for the Unified CVP and Unified CCE VMs. | (GMT-05:00) Eastern Time (US & Canada) |

| Column | Description | Example |
|---|---|---|
| DOMAIN_USER | The user name for a domain user with privileges to add the new computer to the domain. Enabled only if WORK_GROUP is set to **NO**. | DOMAIN\Username<br>(Optional) |
| DOMAIN_PASSWORD | The password for the package123 domain user. Enabled only if WORK_GROUP is set to **NO**. | package123 |
| PRODUCT_KEY | The valid Windows OS product key in the format xxxxx-xxxxx-xxxxx-xxxxx-xxxxx. | ZZZM2-Y330L-HH123-99Y1B-GJ20B |
| OWNER_NAME | The full name of the owner.<br>*Administrator* and *Guest* are not allowable names.<br>This is a mandatory field for OS_TYPE Windows 2012. | LabAdmin |
| ORGANIZATION_NAME | The Organization name to be set for Unified CM, CUIC, MediaSense or Finesse. | MyName |
| ORGANIZATION_UNIT | The Organization unit to be set for Unified CM, CUIC, MediaSense or Finesse. | MyUnit |
| ORGANIZATION_LOCATION | The Organization location to be set for Unified CM, CUIC, MediaSense or Finesse. | MyCity |
| ORGANIZATION_STATE | The Organization state to be set for Unified CM, CUIC, MediaSense or Finesse. | MyState |
| ORGANIZATION_COUNTRY | Drop-down selection of the Organization Country to be set for Unified CM, CUIC, or Finesse.<br>Drop-down selection of the Organization Country to be set for Unified CM, CUIC, MediaSense or Finesse. | United States of America |
| NTP_SERVER | The IP Address of the NTP server. | xx.xx.xxx.xxx |

| Column | Description | Example |
|---|---|---|
| NIC_NUM | Values in the field are pre-populated based on VM_TYPE field and are protected. Values are “1” or “2”. | 2 |
| IP_ADDRESS_NIC1 | A valid IPv4 address for NIC 1.<br>Valid only if the value in the NIC_NUM fields is 1. | xx.xx.xxx.xxx |
| SUB_NET_MASK_NIC1 | A valid subnet mask (IPv4 address) for NIC 1. | xx.xx.xxx.xxx |
| DEFAULT_GATEWAY_NIC1 | A valid Default gateway (IPv4 address) for NIC1. | xx.xx.xxx.xxx |
| DNS_IP_NIC1 | A valid IPv4 address for the primary DNS for NIC1. | xx.xx.xxx.xxx |
| IP_ADDRESS_NIC2 | A valid IPv4 address for NIC 2.<br>Valid only if the value in the NIC_NUM fields is 2. | xx.xx.xxx.xxx |
| SUB_NET_MASK_NIC2 | A valid subnet mask (IPv4 address) for NIC 2. For Unified CCE VMs only. | 255.255.255.255 |
| DNS_IP_NIC2 | A valid IPv4 address for the primary DNS for NIC2. For Unified CCE VMs only. | xx.xx.xxx.xxx |
| DNS_ALTERNATE_NIC2 | A valid IPv4 address for the alternate DNS for NIC2. For Unified CCE VMs only. Must differ from the address of the primary DNS for NIC2. (Optional) | xx.xx.xxx.xxx |
| VM_NETWORK | A valid Network adapter settings | VLAN2 |

## Run Automation Script for Import

The script imports the OVF files and converts them to templates, so that the spreadsheet values can be applied to the virtual machines.

**Note** If you import any of the VOS VMs and have an un-licensed copy of WinImage, you will see one pop-up dialog for each VOS platform. Click **OK** to continue the import process.

**Procedure**

1. Launch **VMware vSphere PowerCLI (32-Bit)** as administrator
2. Enter get-executionPolicy command to determine whether the Restricted Execution policy is in effect or is unrestricted.
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
4. Enter cd < GoldenTemplate directory> command.
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* |

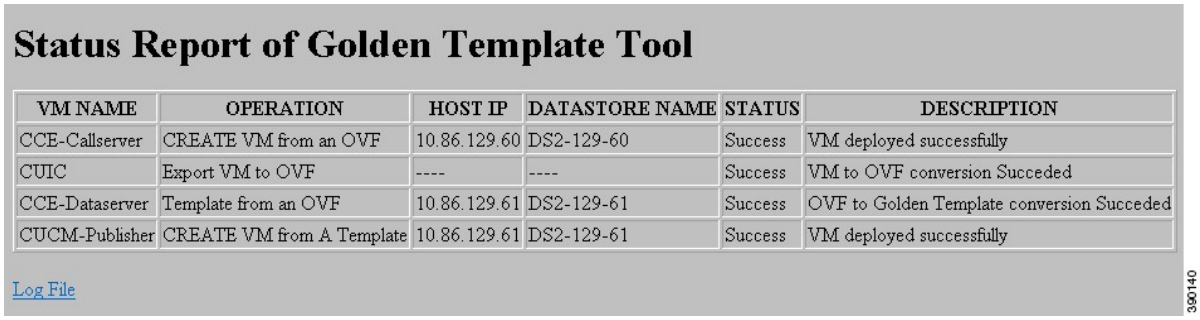
This starts a script that parses the data, validates data, and deploys virtual machine with OS level customization from the *OVF* folder in the GoldenTemplate directory. Updates on the screen show the percentage completed.

If the script runs successfully, it typically completes in several hours.

If there are errors, the script fails but, keeps running. The errors display on the screen and are stored in the log file.

Completion of the script generates a status report in the Report folder. The status report has a link to the Log file. Refer this file to debug the error conditions and to consult with Cisco Support.

***Figure 65: Status Report of Golden Template Tool***



**Status Report of Golden Template Tool**

| VM NAME | OPERATION | HOST IP | DATASTORE NAME | STATUS | DESCRIPTION |
|---|---|---|---|---|---|
| CCE-Callserver | CREATE VM from an OVF | 10.86.129.60 | DS2-129-60 | Success | VM deployed successfully |
| CUIC | Export VM to OVF | ---- | ---- | Success | VM to OVF conversion Succeded |
| CCE-Dataserver | Template from an OVF | 10.86.129.61 | DS2-129-61 | Success | OVF to Golden Template conversion Succeded |
| CUCM-Publisher | CREATE VM from A Template | 10.86.129.61 | DS2-129-61 | Success | VM deployed successfully |

Log File

390140

# 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 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. Cisco suggests that you 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. See Copy Answer Files to Virtual Machines, on page 316

# 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_IO\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>.

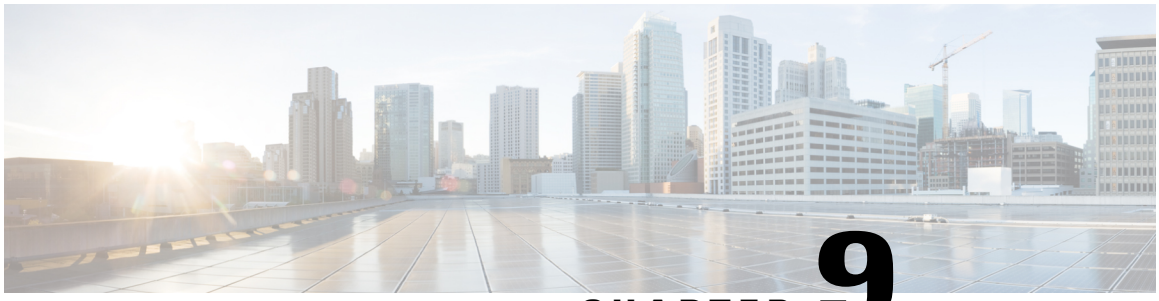
**Example:**
*CUCM_PUB* .

**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 9

# Configure Customer Instance



# Create a Customer Instance for the 500 Agents Deployment Model

Follow this sequence of tasks to create a customer instance to deploy 500-agents for Cisco Hosted Collaboration Solution for Contact Center.

***Table 51: Create customer instance for 500 agent deployment of Cisco HCS for Contact Center***

| Sequence | Task | Done? |
|---|---|---|
| 1 | Upgrade VMware Tools, on page 320 | |
| 2 | Set Up Virtual Machine Startup and Shutdown, on page 320 | |
| 3 | Create a Domain Controller Server, on page 321 | |
| 4 | Configure Cisco Unified CCE Call Server, on page 323 | |
| 5 | Configure Unified CCE Data Server, on page 338 | |
| 6 | Configure Unified CVP, on page 347 | |
| 7 | Configure Cisco IOS Enterprise Voice Gateway, on page 369 | |

| Sequence | Task | Done? |
|---|---|---|
| 8 | Configure Unified Communications Manager, on page 375 | |
| 9 | Configure Unified Intelligence Center with Live Data, on page 380 | |
| 10 | Configure Cisco Finesse, on page 392 | |

# 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 should be installed in all VMs

# Set Up Virtual Machine Startup and Shutdown

### Procedure

**Step 1** Select a virtual machine from the VMware vSphere Client.

**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 **Allow virtual machines to start and stop automatically with the system**.

**Step 6** Use the **Move Up** and **Move Down** buttons to rearrange the virtual machines under **Automatic Startup** in the following order:
**500 and 1000 Agent Deployment**:

- Cisco Unified CCE Database Servers
- Cisco Unified CCE Call 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

**Other HCS Deployments:**

- 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 322
- Install Microsoft Windows Server, on page 322
- Install the Antivirus Software, on page 322
- Configure a DNS Server, on page 322
- Set Up the Domain Controller, on page 322
- Create Two-Way Forest Trust, on page 323

## Create a Virtual Machine for the Domain Controller

### Procedure

**Step 1** See, Set Up Virtual Machine Startup and Shutdown, on page 320 and 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 as specified in Table 37: Domain Controller Minimum Requirements, on page 167.

## Install Microsoft Windows Server

To install Microsoft Windows Server 2012 R2 Standard Edition, see Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252.

## Install the Antivirus Software

For third-party applications installation, see Install Antivirus Software, on page 253.

## Configure a DNS Server

To configuring a DNS server, see Configure DNS Server, on page 437.

## Set Up the Domain Controller

Complete the following procedure to set up the domain controller.

### Procedure

**Step 1** Select **Start** > **Run** and enter dcpromo.exe.

**Step 2** Click **Next** to launch the Active Directory Domain Services Wizard.

**Step 3** In the **Operating System Compatibility** page, click **Next**.

**Step 4** In the **Choose Deployment Configuration** page, click **Create a new domain in a new forest** radio button and click **Next**.

**Step 5** In the **Name the Forest Root Domain** page, enter the fully qualified domain name (FQDN) and click **Next**.

**Step 6** In the **Set Forest Functional Level** page, choose **Windows Server 2008 R2** from the drop-down list and click **Next**.

**Step 7** In the **Additional Domain Controller Options** page, choose **DNS Server** and click **Next**.

**Step 8** In the **Location for Database**, **Log Files**, and **SYSVOL** page, select the default folders and click **Next**.

**Step 9** Enter the password that meets the criteria detailed on the **Directory Services Restore Mode Administrator Password** page and click **Next**.

**Step 10** Click **Next**.

**Step 11** Click **Finish** and restart Windows.

## Create Two-Way Forest Trust

To create two-way forest trust between Unified CCE and CCDM, see Establish Two-Way Forest Trust, on page 456.

# Configure Cisco Unified CCE Call Server

This table lists the configuration procedures that you must perform for sides A and B of Unified CCE Call Server.

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Network Cards, on page 338 | |
| 2 | Verify the Machine in Domain, on page 334 | |
| 3 | Configure the Domain Manager, on page 324 | |
| 4 | Configure Unified CCE Encryption Utility, on page 340 | |
| 5 | Configure the Unified CCE Router, on page 405 | |
| 6 | Configure a Generic Peripheral Gateway, on page 325 | |
| 7 | Configure CTI Server, on page 329 | |
| 8 | Configure Media Routing Peripheral Gateway, on page 330 | |

| Sequence | Task | Done? |
|---|---|---|
| 9 | Configure CTI OS Server, on page 332 | |
| 10 | Install JTAPI, on page 333 | |
| 11 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 12 | Cisco SNMP Setup, on page 334 | |

## Configure the Domain Manager

This procedure creates a organizational unit (Cisco_ICM, facility,instance) from any of the Unified CCE Call Servers.

**Note**

- The domain manager is a one-time configuration. You do not need to configure the domain manager for side B
- 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 service provider (UCCE) domain
- Skip the below procedure if you want to install Agent PG in the service provider (UCCE) domain

### Procedure

**Step 1** Go to **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Domain Manager**.

**Step 2** Log in as a user who has permissions to create organizational units (OUs) in the domain.

**Step 3** In the section on the left, expand the domain.

**Step 4** Add the Cisco root as Cisco_ICM :

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

b) Select the **OUs** under which you want to create the Cisco root OU and click **OK**.
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 5** 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 6** 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 Instance, click **Add**.

c) Enter the instance name and click **OK**.

**Step 7** Click **Close**.

## Configure a Generic Peripheral Gateway

In CCE, the Generic Peripheral Gateway is called the Agent Peripheral Gateway.

### Add a Generic PG

#### Procedure

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

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

**Step 3** In the **Component Selection** dialog box, choose **Peripheral Gateway**.

**Step 4** In the **Peripheral Gateway Properties** dialog box, do the following:

a) Check **Production mode**.
b) Check **Auto start system startup**.
c) Check **Duplexed Peripheral Gateway**.
d) In the PG node Properties ID field, choose **PG1**.
e) Select the appropriate side (**Side A** or **Side B**).
f) Under the Client Type section, add **CUCM** and **VRU** to the selected types.
g) Click **Next**.

### Add PIM1(Unified Communications Manager PIM)

To add Peripheral Interface Manager (PIM1) as the Unified Communication Manager PIM, do the following:

#### Procedure

**Step 1** In the **Peripheral Interface Manager** section of the **Peripheral Gateway Component Properties** dialog box, click **Add**.

**Step 2** Select **CUCM** and **PIM1** and click **OK**.

**Step 3** Check **Enabled.**

**Step 4** In the **Peripheral Name** field, enter CM.

**Step 5** In the **Peripheral ID** field, enter 5000.

**Step 6** In the **Agent Extension Length** field, enter the extension length for this deployment.

**Step 7** In the **Unified Communications Manager Parameters** section, do the following:

a) In the **Service** field, enter the hostname of the Unified Communications Manager Subscriber.
b) In the **User ID** field, enter pguser.

c) In the **User Password** field, enter the password of the user that will be created on Unified Communications Manager.
d) In the **Mobile Agent Code**c field, choose either **G711 ULAW/ALAW** or **G.729**.

**Step 8** Click **OK**.

**Note** Unified Communication Domain Manager sets the default password as "pguser", during Unified Communication Manager integration.

### Add PIM2 (First VRU PIM)

To add the PIM2 as the first Voice Response Unit (VRU) PIM, do the following:

#### Procedure

**Step 1** In the **Peripheral Interface Manager** section of the **Peripheral Gateway Component Properties** dialog box, click **Add**.
**Step 2** Select the **Client Type of VRU** and **PIM2**, then click **OK**.
**Step 3** Check **Enabled**.
**Step 4** In the **Peripheral Name** field, enter CVP1.
**Step 5** In the **Peripheral ID** field, enter 5001.
**Step 6** In the **VRU Hostname** field, enter the hostname of CVP1 (Side A).
**Step 7** In the **VRU Connect Port** field, enter 5000.
**Step 8** In the **Reconnect interval (sec)** field, enter 10.
**Step 9** In the **Heartbeat interval (sec)** field, enter 5.
**Step 10** In the **DSCP** field and choose **CS3(24)**.
**Step 11** Click **OK.**

### Add PIM3 (Second VRU PIM)

#### Procedure

**Step 1** In the **Peripheral Interface Manager** pane of the **Peripheral Gateway Component Properties** dialog box, click **Add**.

**Step 2** Select **Client Type of VRU** and **PIM3**. Then click **OK**.

**Step 3** Check **Enabled**.

**Step 4** In the Peripheral name field, enter CVP2.

**Step 5** In the Peripheral ID field, enter 5002.

**Step 6** In the VRU hostname field, enter the hostname of CVP1 (Side B).

**Step 7** In the VRU Connect port field, enter 5000.

**Step 8** In the Reconnect interval (sec) field, enter 10.

**Step 9** In the Heartbeat interval (sec) field, enter 5.

**Step 10** In the DSCP field, choose **CS3(24)**.

**Step 11** Click **OK** .

### Add PIM4 (Third VRU PIM)

#### Procedure

**Step 1** In the **Peripheral Interface Manager** pane of the **Peripheral Gateway Component Properties** dialog box, click **Add**.

**Step 2** Select **Client Type of VRU** and **PIM4** then click **OK**.

**Step 3** Check **Enabled**.

**Step 4** In the Peripheral name field, enter CVP3.

**Step 5** In the Peripheral ID field, enter 5003.

**Step 6** In the VRU hostname field, enter the hostname of CVP2 (Side A).

**Step 7** In the VRU Connect port field, enter 5000.

**Step 8** In the Reconnect interval (sec) field, enter 10.

**Step 9** In the Heartbeat interval (sec) field, enter 5.

**Step 10** In the DSCP field, choose **CS3(24)**.

**Step 11** Click **OK** .

### Add PIM5 (Fourth VRU PIM)

#### Procedure

**Step 1** In the **Peripheral Interface Manager** pane of the **Peripheral Gateway Component Properties** dialog box, click **Add**.

**Step 2** Select **Client Type of VRU** and **PIM4** then click **OK**.

**Step 3** Check **Enabled**.

**Step 4** In the Peripheral name field, enter CVP4.

**Step 5** In the Peripheral ID field, enter 5004.

**Step 6** In the VRU hostname field, enter the hostname of CVP2 (Side B).

**Step 7** In the VRU Connect port field, enter 5000.

**Step 8** In the Reconnect interval (sec) field, enter 10.

**Step 9** In the Heartbeat interval (sec) field, enter 5.

**Step 10** In the DSCP field, choose **CS3(24)**.

**Step 11** Click **OK** .

### After Creating PIMs

Perform this task at the Peripheral Gateway Component Properties page.

#### Procedure

**Step 1** Enter 5000 in the Logical Controller ID field.

**Step 2** Enter 0 in the CTI Call Wrapup Data delay field.

**Step 3** In the VRU Reporting pane, click **Service Control** and check **Queue Reporting**. Click **Next** to open the Device Management Protocol Properties dialog box.

**Step 4** In the Device Management Protocols Properties dialog box, complete all interface fields:

a) For Side A PG:

- Select **Side A Preferred**.
- For Side A Properties, check **Call Router is local**.
- For B Properties, check **Call Router is remote (WAN)**.

b) For Side B PG:

- Select **Side B Preferred**.
- For Side A Properties, check **Call Router is remote (WAN)**.
- For Side B Properties, check **Call Router is local**.

c) For both Sides:

- Accept the default in the Usable Bandwidth (kbps) field.
- Accept the default in the Heartbeat Interval (100ms) field.

d) Click **Next.**

**Step 5** In the Peripheral Gateway Network Interfaces dialog box, complete all interface fields:

a) Enter the Private and Visible network interface hostnames. For the PG and Router entries, use the same hostnames for Private and Private High, and the same hostnames for Visible and Visible High.
b) 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**.
c) Click the **QoS** button in the Visible Interfaces section for both the Side A and Side B PGs. In the PG Visible Link QoS Settings, check **Enable QoS**, click **OK**.
d) Click **Next**.

**Step 6** In the Check Setup Information dialog box, click **Next**.

**Step 7** In the Setup Complete dialog box, click **Finish**.

**Step 8** Click **Exit Wizard**.

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

## Configure CTI Server

### Procedure

**Step 1** In the Instance Components pane of the Components Setup dialog box, click **Add**.

**Step 2** 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** in the CG node properties pane ID field.
e) Enter 1 in the CG node properties ICM system ID field.
f) Click the appropriate side.
g) Click **Next**.

**Step 3** In the Server Component Properties dialog box, configure as follows:

a) For Side A, enter 42027 in the Client Connection Port Number field.
b) For Side B, enter 43027 in the Client Connection Port Number field.

**Step 4** Click **Next**.

**Step 5** In the Network Interface Properties dialog box, fill in all interface fields Then click **Next** .

**Step 6** Enter the PG public interfaces, CG private interface, and CG visible interfaces details and click **Next**.

**Step 7** Under the Check Setup Information page, click **Next**.

**Step 8** In the Setup Completed dialog box, click **Finish**.

**Step 9** Click **Exit Setup**.

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

## Configure Media Routing Peripheral Gateway

Complete the following procedure to set up the Unified CCE Media Routing Peripheral Gateway. The MR PG is required; you must configure it.

The Media Routing Peripheral Gateway can optionally have two PIMs—the MultiChannel PIM (PIM1) and the Outbound PIM (PIM2). The Multichannel PIM can be configured for Unified WIM and Unified EIM. You can configure these PIMs if you use those features.

### Add Media Routing PG

Complete the following procedure to add the MR PG and the Multichannel PIM (PIM1) and the Outbound PIM (PIM2). You can have one of each PIM. The Multichannel PIM can be used for either Unified WIM and Unified EIM

#### Procedure

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

**Step 2** Click **Add** in the **Instance Components** pane, and from the **Component Selection** dialog box choose **Peripheral Gateway**.

**Step 3** In the **Peripheral Gateway Properties** dialog box:

a) Check **Production Mode**.
b) Check **Auto start system startup**.
c) Check **Duplexed Peripheral Gateway**.
d) Choose **PG2** in the **PG node Properties ID** field.
e) Click the appropriate side.
f) Under Client Type pane, add **Media Routing** to the selected types.
g) Click **Next**.

**Step 4** In the Peripheral Interface Manager pane of the Peripheral Gateway Component Properties dialog box, click **Add** and configure PIM1 (the Multichannel PIM) with the Client Type of Media Routing.

a) Check **Enabled**.
b) In the Peripheral name field, enter **MR**.
c) In the Peripheral ID field, enter **5005**.
d) In the Application Hostname (1), field, enter the hostname or the IP address of the Unified WIM and EIM services server machine or of SocialMiner.
e) In the Application Connection Port (1), field, enter the port number on the Unified WIM and EIM services server/SocialMiner machine that the PIM will use to communicate with the application. The default port is 38001.
f) In the Application Hostname (2), field, leave the field blank.
g) In the Application connection port (2), field, leave the field blank.
h) In the Heartbeat interval (sec) field, enter **5**.
i) In the Reconnect interval (sec) field, enter **10**.

j) Click **OK**.

**Step 5** Click **Add** and configure PIM2 (the Outbound PIM) with the client type of Media Routing as follows:

a) Check **Enabled**.
b) In the Peripheral name field, enter **MR2** or a name of your choice.
c) In the Peripheral ID field, enter **5006**.
d) In the Application Hostname(1) field, enter **UCCE call server side A IP**.
e) The Application Connection port (1), retain the default value.
f) In the Application Hostname (2), field, enter **UCCE Call server side B IP**.
g) The Application Connection port (2), retain the default value.
h) In the Heartbeat interval (sec) field, enter **5**.
i) In the Reconnect interval (sec) field, enter **10**.
j) Click **OK**.

**Step 6** Enter **5001** in the Logical Controller ID field.

**Step 7** Enter **0** in the CTI Call Wrapup Data delay field. Click **Next**.

**Step 8** In the Device Management Protocol Properties dialog box, configure as follows:

a) For Side A PG:

- Select **Side A Preferred**.
- For Side A Properties, check **Call Router is local**.
- For B Properties, check **Call Router is remote (WAN)**.

b) For Side B PG:

- Select **Side B Preferred**.
- For Side A Properties, check **Call Router is remote (WAN)**.
- For Side B Properties, check **Call Router is local**.

c) For both Sides:

- Accept the default in the Usable Bandwidth (kbps) field.
- Enter **4** in the Heartbeat Interval (100ms) field.

d) Click **Next.**

**Step 9** In the Peripheral Gateway Network Interfaces dialog box, enter the Private Interfaces and the Visible Interfaces. This step applies only to Side A.

a) Enter the Private and Visible network interface hostnames. For the PG and Router entries, use the same hostnames for Private and Private High, and the same hostnames for Visible and Visible High.
b) 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**.
c) Click the **QoS** button in the Visible Interfaces section for both the Side A and Side B PGs. In the PG Visible Link QoS Settings, check **Enable QoS**, click **OK**.

d) Click **Next**.

**Step 10** In the Check Setup Information dialog box, click **Next**.

**Step 11** In the Setup Complete dialog box, click **Finish**.

**Step 12** Click **Exit Setup**.

**Note** Do not start Unified ICM/CC Node Manager 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**). Click **Next**.

**Step 10** 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 11** In the Connect Information dialog box, enter Listen Port 42028 and accept all defaults and then click **Next**.

**Step 12** In the Statistics Information dialog box, check **Polling for Agent Statistics at End Call** and then click **Next**.

**Step 13** In the IPCC Silent Monitor Type dialog box, set Silent Monitor Type to **CCM Based** and click **Next**.

**Step 14** 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 15** Click **Finish**.

**Step 16** In the Cisco CTI OS Server Security dialog box, uncheck **Enable Security**. Click **OK**.

**Step 17** In the CTI OS Security dialog box, click **Finish**.

**Step 18** When prompted to restart the computer, click **Yes**. If there is a Maintenance Release, its installation begins automatically.

**Step 19** Follow all prompts to install the Maintenance Release, if there is one.

**Step 20** When the Maintenance Release install completes, click **Finish** and follow the prompts to restart.

**Step 21** Access Registry Editor (**Run > regedit**).

**Step 22** Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,Inc.\Ctios\CTIOS_<instance name>\CTIOS1\Server\Agent**.

**Step 23** Set **forceLogoutOnSessionClose** to **1**.

## Install JTAPI

**Note** This procedure is required for the Unified Contact Center Enterprise Machine having a PG with Unified Communications Manager PIM. However, you must postpone this task until after you Configure Unified Communications Manager, on page 375.

Complete the following procedure to install JTAPI on the Unified Contact Center Enterprise Machine having a PG with Unified Communications Manager PIM for Side A and Side B.

### Procedure

**Step 1** Launch the Unified Communications Manager in a browser (https://{callmanager-hostname}) and log in.

**Step 2** Navigate to **Application** > **Plugins**. Click **Find**.

**Step 3** Download the Cisco JTAPI 32-bit Client for Windows.

**Step 4** Install the downloaded file, accepting all of the default settings.

**Step 5** At the prompt, enter the IP address for the Unified Communications Manager TFTP Server, and click **Next**.

**Step 6** Click **Finish**.

## 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.

### Before You Begin

Set Local Administrator Password, on page 334

### 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.

## Cisco SNMP Setup

Complete the following procedures to configure Cisco SNMP:

## 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 335 and Save Cisco SNMP Agent Management Snap-In View, on page 335.

### 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 335 and Save Cisco SNMP Agent Management Snap-In View, on page 335.

### 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 335 and Save Cisco SNMP Agent Management Snap-In View, on page 335.

### 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.

# Configure Unified CCE Data Server

This section explains the configuration procedures you must perform for the Unified CCE Data Servers.

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Network Cards, on page 338 | |
| 2 | Verify the Machine in Domain, on page 334 | |
| 3 | Configure Unified CCE Encryption Utility, on page 340 | |
| 4 | Configure SQL Server, on page 341 | |
| 5 | Configure Secondary Drive, on page 341 | |
| 6 | Configure the Unified CCE Logger, on page 342 | |
| 7 | Configure Administration Server and Real-Time Data Server Components , on page 344 | |
| 8 | Load Base Configuration, on page 345 | |
| 9 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 10 | Cisco SNMP Setup, on page 334 | |
| 11 | Final Tasks, on page 346 | |

## Configure Network Cards

**Note** Do this for all the Unified Contact Center Enterprise 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. Append a suffix such as **p** to the hostname for this IP, to identify it as private.
**Step 8** Optional: Add another entry for the public high IP address. Append a suffix such as **ph** to the hostname for this IP, to identify it as public high.
**Step 9** Click **OK** twice. Then, click **Close**.

### Configure Visible 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 high public 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 high IP address. Assign an unique suffix, for example, **ph** to the hostname for this IP, to identify it as public high.
**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**.

## 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 340

### 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

### Procedure

**Step 1** Go to **Start** > **All Programs** > **Microsoft SQL Server 2008 R2** > **SQL Server Management Studio**.

**Step 2** Log in.

**Step 3** Expand **Security** and then **Logins**.

**Step 4** 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) Make sure that **public** and **sysadmin** are both checked.

## Configure Secondary Drive

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

### Procedure

**Step 1** Open **Computer Management**.

**Step 2** Expand **Storage** in the left pane, click **Disk Management**.

**Step 3** Right-click **Disk 1** and choose **Online**.

**Step 4** Right-click **Disk 1** and choose **Initialize Disk**.

**Step 5** In Initialize Disk pop up window, under Select disks. Check **Disk 1** and choose **MBR (Master Boot Record)** under **Use the following partition style for the selected disks** pane. Click **OK**.

**Step 6** Create a new disk partition as follows: right-click the disk you just initialized, choose **New Simple Volume**, and run the wizard.

## Configure the Unified CCE Logger

Complete the following procedure to configure the Unified CCE Logger.

**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 rights.

**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** Configure the logger database as follows:

a) Select **Start** > **All Programs** > **Cisco Unified CCE Tools** > **ICMdba**. Click **Yes** at the warnings.
b) Navigate to **Server > Instance** (logger being installed).
c) Right-click the instance name and choose **Create** to create the logger database.
d) In the **Select Component** dialog box, choose the logger you are working on ( Logger A or Logger B). Click **OK**.
e) At the prompt “”SQL Server is not configured properly. Do you want to configure it now?“”, click **Yes**.
f) On the Configure page, in the SQL Server Configurations pane, check **Memory (MB) = Dynamic** and **Recovery Interval = 1**. Click **OK**.
g) On the Stop Server page, click **Yes** to stop the services.
h) In the **Select Logger Type** window, select **Enterprise** from the drop-down list. Click **OK**.

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

a) In the **DB Type** field, choose the side (A or B).
b) In the **Storage** pane, click **Add**.

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

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

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

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

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

**Step 11** In the Create Database dialog box, 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**. Click **Add**. Choose the Instance.
c) On the Deployment page, select the Logger (A or B). Select **Duplexed**. Click **Next**.
d) On the Central Controller Connectivity page, enter the host names for Sides A and B for the Router Private Interface and Logger Private Interface.

**Step 13** On the Additional Options page, configure the following and click **Next**:
a) If an external AW-HDS-DDS exists in the deployment, then check **Enable Historical/Detail Data Replication**.
b) If no external AW-HDS-DDS exists in the deployment, leave **Enable Historical/Detail Data Replication** unchecked.
c) Check **Display Database Purge Configuration Steps**.

**Step 14** On the Data Retention page, modify the Database Retention Configuration table:
a) For the seven following tables, set the retention period to 40 days: Application_Event, Event, Network_Event, Route_Call_Detail, Route_Call_Variable, Termination_Call_Detail, and Termination_Call_Variable.
b) Set the retention period for all other tables to 400 days.
Applies only for HCS 500 and 1000 agent deployment without external HDS.
c) Click **Next**.

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

**Step 16** Review the Summary page, and then click **Finish**.

**Note** Do not start service until all ICM components are installed.

## Database and Log File Size

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

### Before You Begin

Use DB Estimator Tool to calculate database and log file size.

Alternative option is to size the database and log using the values from Table 52: Data and Log File Size, on page 344. The values in the table for HCS 500 and 1000 agent deployments are sized without considering optional HDS.

### Procedure

**Step 1** Open **SQL Server 2014 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 log files.

**Step 5** Set the initial size of the data and log files according to DB Estimator Tool or from the following table:

*Table 52: Data and Log File Size*

| Database | Data size(MB) | Log Size(MB) | Deployment Type |
|---|---|---|---|
| Side A, Side B | 409600 | 1024 | 500 and 12000 Agent Deployments |
| Side A, Side B | 665600 | 3072 | 1000 Agent Deployment |
| Side A, Side B | 122900 | 1024 | Other HCS Deployments |

## Configure Administration Server and Real-Time Data Server Components

### Procedure

**Step 1** Go to the **Unified CCE Web Setup**.

**Step 2** Choose **Component Management** > **Administration & Data Servers**. Click **Add.**

**Step 3** On the Add Administration & Data Servers page, configure as follows:

a) Choose the current instance
b) Click **Enterprise.** Then click **Small to Medium** Deployment Size.
c) Click **Next**.

**Step 4** On the Role page, choose the option **Administration Server and Real-time Data Server (AW)**. Click **Next**.

**Step 5** Configure primary/secondary Administration and Data Servers connectivity, as follows:
Follow the below steps for primary:

a) Select **Primary Administration & Data Server** option.
b) In **Secondary Administration & Data Server** field, enter secondary AW hostname.
c) In **Primary/Secondary Pair (Site) Name** field, enter primary sitename.

Follow the below steps for secondary:

a) Select **Secondary Administration & Data Server** option.
b) In **Primary Administration & Data Server** field, enter primary AW hostname.
c) In **Primary/Secondary Pair (Site) Name** field, enter secondary sitename.

**Step 6** On the Database and Options page, configure as follows:

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

**Step 7** On the Central Controller Connectivity page, configure as follows:

a) For Router Side A, enter the Call Server Side A Public hostname.
b) For Router Side B, enter the Call Server Side B Public hostname.
c) For Logger Side A, enter the Data Server Side A Public hostname.

d) For Logger Side B, enter the Data Server Side B Public hostname.
e) Enter the **Central Controller Domain Name**.
f) Select **Central Controller Side A Preferred** or **Central Controller Side B Preferred**, based on what side you are on.
g) Click **Next**.

**Step 8** Review the Summary page, and then click **Finish**.

**Note** Do not start service until all ICM components are installed.

## Load Base Configuration

Complete this procedure to upload the following base configuration parameters. For more information about base configuration parameter, see Base Configuration Parameters for 500 and 1000 Agent Deployment, on page 768.

1. PG Explorer
2. Network VRU Explorer
3. System Information
4. Expanded Call Variable List
5. Network VRU Script
6. Default Agent Desk Settings
7. Application Instance List
8. Media Class for Multi Channel
9. Media Routing Domain
10. Network VRU Mapping

### Procedure

**Step 1** Download the HCS-11.0.1-500-and-1000-Agent-Day1-Configuration.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 CCE Data Server on Side A.

**Step 4** Open the ICMDBA Tool on the CCE Data Server on Side A.

**Step 5** Select the CCE Data Server 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 CCE Data Server 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. Open Data on the menu bar and click **Synchronize**.

a) Enter the hostname for the CCE Data Server on Side A.
b) Enter the database name as <instance name>_sideA for the source side.
c) Enter the hostname for the CCE Data Server on Side B.
d) Enter the database name as <instance name>_sideB for the target side.
e) Click **Synchronize**.

**Step 12** Click **Start** and then click **OK** on all messages.

## 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.

## Final Tasks


- Set the HCS Deployment Type, on page 346
- Start Unified CCE Services, on page 347


### Set the HCS Deployment Type

### Procedure

**Step 1** Go to **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Administration Tools** > **CCE Web Administration**.

**Step 2** Login with user credentials.

**Step 3** Set the HCS 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-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**

### 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 each Unified CCE Server machine, open **Unified CCE Service Control**.

**Step 2** Select each **CCE Component**in the following sequence and click **Start**.

1. Logger A
2. Router A
3. PG's Side A
4. Logger B
5. Router B
6. PG's Side B
7. Administration & Data Servers

# Configure Unified CVP

This section explains the procedures to configure Unified CVP.

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Unified CVP Server, on page 348 | |
| 2 | Configure Unified CVP Reporting Server, on page 351 | |
| 3 | Configure Cisco Unified CVP Operations Console, on page 359 | |

## Configure Unified CVP Server

This section explains the procedures to configure Unified CVP Server.

| Sequence | Task | Done? |
|---|---|---|
| 1 | Validate Network Card, on page 348 | |
| 2 | Setup Unified CVP Media Server IIS, on page 349 | |
| 3 | Setup FTP Server, on page 350 | |

### 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 4.5
    - ASP.NET 4.5
    - 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, on page 350
- Enable FTP Server, on page 350
- Configure Basic Settings for FTP Server, on page 351


### *Install FTP Server*

**Procedure**

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

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

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

**Step 4** Goto **Installation Type** tab, choose **Role-based or feature-based Installation** and click **Next**.

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

**Step 6** No additional features are necessary to install the web Adaptor and click **Next**.

**Step 7** In **Web Server Role(IIS)** window click **Next**.

**Step 8** Check **FTP Server** check box and click **Next**.

**Step 9** 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 500 & 1000 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 348 | |
| 2 | Configure Secondary Drive, on page 341 | |
| 3 | Install Unified CVP Reporting Server, on page 263 | |
| 4 | Unified CVP Reporting Users, on page 352 | |
| 5 | Create Data Source and Import Report Templates, on page 356 | |

## Unified CVP Reporting Users

### *Create Reporting Users*

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.

Although you can create a user on the Unified Intelligence Center User List page, an entry on the User List is not sufficient for that user to sign in to the Unified Intelligence Center. One reason to create users on the User List page is to expedite the permissions for users before their Active Directory domain is configured.

Create Superusers

**Procedure**

**Step 1** Log in to the Cisco Unified Intelligence Center Administration Console `(http://{hostname}/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 at http://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html or the Administration console online help.

**Step 4** Click **Save**.

Configure Active Directory Server

Fields on the Active Directory tab configure the Active Directory server to authenticate reporting users as they log in to the Unified Intelligence Center Web application.

You must configure Active Directory for the Unified ICM/CC supervisors so that they can sign in as Unified Intelligence Center Reporting users.

**Note** Cisco Unified Intelligence Center uses LDAP V2 which does not support all Unicode characters that are used in the first name or surname of LDAP users.

Active Directory is not used to authenticate Administration Super Users. These Super Users can only be authenticated through the local database. The first Super User is added during installation. All other Super Users are added through the **Admin User Management** interface, and their credentials are encrypted into the local database.

To navigate to this page, choose **Cluster Configuration** > **Reporting Configuration** and select the Active Directory tab.

***Table 53: Fields on This Tab***

| Field | Description |
|---|---|
| Host Address and Port for Primary Active Directory Server | Provide the Host name or IP address and the port of the Primary Active Directory server.<br>The port defaults to 389. |
| Host Name and Port for Redundant Active Directory Server | Provide the Host name or IP address and the port of the Redundant Active Directory server.<br>The port defaults to 389. |
| Use SSL | Check these boxes if you want the connection from the Unified device to the Active Directory connection to be encrypted with SSL while doing authentication. |
| Manager Distinguished Name | Enter the Manager Distinguished Name used to login to the Active Directory server, for example, on a default installation of Microsoft AD: `CN=Administrator, CN=users, DC=MYSERVER, DC=COM`. Replace *MYSERVER* and *COM* with your respective hostname.<br>**Note** If users other than the LDAP administrator, is configured as Manager Distinguished Name in the OAMP LDAP configurations, they should have the following rights:<br>**1** User search permissions on the domain.<br>**2** Read access to the user objects and their attributes.<br>**3** Read access to the base DN<br>**4** Permission to bind to LDAP. |
| Manager Password | Enter the Active Directory manager password. |
| Confirm Manager Password | Confirm the Active Directory manager password. |
| User Search Base | Specify the user search base. For example, on a default installation of Microsoft AD, `CN=users, DC=MYSERVER, DC=COM`, replace *MYSERVER* and *COM* with your respective hostname.<br>**Note** This example assumes you placed the users in the USERS subtree of AD. If you created a new organizational unit within your subtree, then the syntax would be: `OU=MYUSERS, DC=MYSERVER, DC=COM`. Note that it is "OU=MYUSERS" instead of "CN=MYUSERS". |

| Field | Description |
|---|---|
| Attribute for User ID | Whenever a user logs in, Unified Intelligence Center searches for that user in the LDAP (Lightweight Directory Access Protocol) using the login attribute specified in the LDAP configuration. After the user is found, the full DNS of the user is extracted and used for authenticating the user.<br><br>The login attribute specified in the LDAP configuration will be the property against which LDAP search is issued to find the matching username. If you do not know which attribute to use, use *sAMAccountName*, which is the default Microsoft username attribute.<br><br>Different organizations settle on different LDAP attributes to identify the user name across the organization, depending on the tools used to administer LDAP within their organizations. This attribute allows you to customize the login depending on the attribute used. Even a custom attribute can be specified using this dialog.<br><br>*sAMAccountName* indicates the user attribute to search the user for is the *userPrincipalName*. *sAMAccountName* contains just the short user name. For example, jDoe for the user John Doe.<br><br>*userPrincipalName* indicates the user attribute to search the user for is the *userPrincipalName*. This attribute contains user name in the email format, in the form user@compay.com. Therefore this entire string becomes the user name and not just user. Therefore when this attribute is selected this entire form of username has to be typed in as the username in the login box.<br><br>**Custom User Attribute** allows you to specify the attribute used for searching the user in LDAP.<br>**Note** Custom User attributes are not validated and are used as is. Ensure that the correct case and attribute name are used.<br><br>Contact your Active Directory Administrator for the correct attribute to use. |

| Field | Description |
|---|---|
| UserName Identifiers | Users are stored in Unified Intelligence Center in the format <UserName Identifier>\<username><br><br>The UserName Identifiers are used to identify the different kinds of users within Unified Intelligence Center. For example, local, LDAP, user-synced user, users from different LDAP domains and so on.<br><br>The username identifier has to be first declared for use in this page before it can be used. When LDAP is configured at least one identifier must be configured and set as default so that LDAP users can be identified in the system.<br><br>When *userPrincipalName* are used as the LDAP attribute for searching users in the domain, valid formats for username has to be supplied in the form of *@company.com*. Unlike *sAMAccountName* any identifier cannot be configured. Only existing identifiers as configured in the LDAP Active Directory *userPrincipalName* attribute should be configured here. Users are created as company\user.<br><br>UserSychronization brings in users in format <syncdomain>\username and collections will have users in the same format. It is therefore required that these users login to Unified Intelligence Center using the syncdomain\user syntax. To enable please add syncdomain or @syncdomain.com (if you are using *userPrincipalName*) to the list of valid identifiers.<br><br>The maximum allowed length of a UserName identifier is 128 characters. |
| set Default. (UserName Identifier) | Default identifiers allows users to login without typing the full domain identifier (<domain>\user) or the *userPrincipalName* suffixes to usernames (user <@company.com>) on the Login page.<br><br>It can be set by choosing one of the Identifiers from the list box and by clicking the **Set Default** button.<br><br>Users who need to use any other identifier can still login by typing their full identifier in the login box. For example, domain2\user or netbiosname\user, provided those identifiers have already been configured. |
| Test Connection button | Click to test the connection to the primary and secondary LDAP servers and display the connection status. |

- **Save** saves the configuration information you entered for the active directory. Clicking **Save** *does not validate the configuration*.
- **Refresh** rolls back all changes since the last save and reloads the values set during the last save.

The UserName Identifier list box is pre-populated with the UserName Identifiers after upgrade to 9.0 release from 8.x releases based on the list of user names stored in the Unified Intelligence Center database. The most frequently occurring identifier in the list of user name is auto-selected as the default.

**Note** You cannot save LDAP configuration unless you choose a default Identifier from the UserName Identifiers list box and clicking the Set Default button.

### *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 (`http://{hostname}/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.

#### What to Do Next

## Create Data Source and Import Report Templates

| Sequence | Task | Done? |
|---|---|---|
| 1 | Create Data Source for Cisco Unified CVP Report Data, on page 356 | |
| 2 | Obtain Cisco Unified CVP Report Templates , on page 358 | |
| 3 | Import Unified CVP Report Templates and Set Data Source, on page 358 | |

### *Create Data Source for Cisco Unified CVP Report Data*

Similar to creating an Open Database Connectivity (ODBC) connection, this task is necessary to access the Unified CVP reporting data.

In Unified Intelligence Center, the user must perform this task with the System Configuration Administrator User Role.

Perform the following procedure to create a data source.

### Procedure

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

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

**Step 3** Click **Create** to open an Add Data Source window.

**Step 4** Complete fields on this page as follows:

| Field | Value |
|---|---|
| **Name** | Enter the name of this data source.<br>Report Designers and Report Definition Designers do not have access to the Data Sources page but can see the list of Data Sources when they create custom reports. To benefit those users, give a new Data Source a meaningful name. |
| **Description** | Enter a description for this data source. |
| **Type** | Choose **Informix**.<br>**Note** Type is disabled in Edit mode. |
| **Database Host** | Enter the IP address or Domain Name System (DNS) name for the Unified CVP Reporting server. |
| **Port** | Enter the port number. Typically, the port is 1526. |
| **Database Name** | Enter the name of the reporting database on the Unified CVP reporting server. |
| **Instance** | Specify the instance name of the desired database. By default, this is `cvp`. |
| **Timezone** | Choose the correct time zone for the data stored in the database. In locations that change from Standard Time to Daylight Savings Time, this time zone is updated automatically. |
| **Database User ID** | Enter the user ID of the Reporting User who is configured in the Operations Console to access the Unified CVP reporting database.<br>(The cvp_dbuser account is created automatically during Unified CVP Reporting server installation.) |
| **Password and Confirm Password** | Enter and confirm the password for the database user. |

| Field | Value |
|---|---|
| **Charset** | Choose UTF-8.<br>**Note** If this field is not set correctly, the Unified Intelligence Center cannot connect. |
| **Default Permissions** | View or edit the permissions for this datasource for My Group and for the All Users group. |

**Step 5** Click **Test Connection**.
If the status is not Online, review the error message to determine the cause and edit the data source accordingly.

**Step 6** Click **Save** to close the Add Data Source window.
**Note** If CVP Call Back Reports have to be imported on the standard data source (cvp_data), the import fails with a message "*Import could not be completed: Query validation failed against the selected data source.*"
To correct this issue, create a separate data source pointing to the callback database instead of the cvp_data database.
The new data source appears on the Data Sources list.

### *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 Unified CVP Report Templates and Set Data Source*

Who can do this:

- Initially, the System Application User who has full permissions in Unified Intelligence Center Reporting.
- Eventually, any Report Designer who has full permissions.

Before reporting users can run the Unified CVP report templates in the Unified Intelligence Center reporting application, a Unified IC reporting user with permission to do so must import them into Unified IC and associate them with the Unified CVP Data Source.

### Procedure

**Step 1** Launch the Unified Intelligence Center web application using the `URL http://<HOST ADDRESS>:8444/cuic`

**Step 2** Enter your User Name and Password.
This opens the Overview page.

**Step 3** Click**Reports**.

**Step 4** Right-click the top Reports folder and select **Create Sub-Category**.

**Step 5** Name the new sub-category as a container for Unified CVP reports. Click **OK**.

**Step 6** Click **Import Reports**.

**Step 7** Browse to the location where you copied the Unified CVP Reporting templates files.

**Step 8** Select a report.
This populates the File Name with the full path for the report.

**Step 9** Click **Import**.

**Step 10** From the **Data source for Report Definition** and **Data source for value List** drop down lists, Choose the Data source you created to access the Unified CVP Reporting database.

**Step 11** **Save to** the Unified CVP sub-category folder you created in Step 5.

**Step 12** Click **Import**.

**Step 13** Repeat for the callback templates.

## Configure Cisco Unified CVP Operations Console

| Sequence | Task | Done? |
|---|---|---|
| 1 | Validate Network Card, on page 348 | |
| 2 | Enable Unified CVP Operations Console, on page 360 | |
| 3 | Configure Unified CVP Call Server Component, on page 360 | |
| 4 | Configure Unified CVP VXML Server Component, on page 361 | |
| 5 | Configure Unified CVP Reporting Server, on page 361 | |
| 6 | Configure Unified CVP Media Server, on page 362 | |
| 7 | Install Unified CVP licenses, on page 363 | |
| 8 | Configure Gateways, on page 363 | |
| 9 | Add Unified CCE Devices, on page 365 | |
| 10 | Add Unified Communications Manager Devices, on page 365 | |
| 11 | Add Unified Intelligence Center Devices , on page 366 | |
| 12 | Transfer Scripts and Media Files, on page 364 | |
| 13 | Configure SNMP, on page 364 | |

| Sequence | Task | Done? |
|---|---|---|
| 14 | Configure SIP Server Group, on page 366 | |
| 15 | Configure Dialed Number Patterns, on page 367 | |

## 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

### 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 Call Servers.

### Configure Unified CVP VXML Server Component

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

**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 servers on Side B for the 1000 agent deployment
- There are eight Unified CVP servers on Side A and eight Unified CVP servers on Side B for 4000 agent deployment and small contact center agent deployment
- There are twenty four Unified CVP servers on Side A and twenty four Unified CVP servers on Side B for the 12000 agent deployment

#### 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, he 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, he 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) Name the community string.
b) Select the **Devices** tab and assign the SNMP community string to a device.
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) Complete the fields.
c) Select the **Devices** tab and assign the SNMP notification destination to a device.
d) 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.

**Note** For Small Contact Center deployment add the NAT IP address of the agent PG.

**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
- In 12000 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**.<br>Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example, vxmlgw.cisco.com).<br>Check **Enable Send Calls to Originator**. |
| 92* | Error | Check **Enable Local Static Route**.<br>Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example, vxmlgw.cisco.com).<br>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. Not applicable to SCC Deployment model. | Check **Enable Local Static Route**.<br>Route to SIP Server Group and IP Address/Hostname/Server Group Name are both the Unified Communications Manager gateway.<br>Check **Enable RNA Timeout for Outbound Calls**. The timeout is 60 seconds. |
| 777* | Network VRU Label | Check **Enable Local Static Route**.<br>Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example vxmlgw.cisco.com).<br>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.<br>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><br>For each sub customer a unique port must be configured.<br>Check Enable RNA Timeout for Outbound Calls. The timeout is 15 seconds. |

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

**Step 5** Restart the Unified CVP Call Server components.

# 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
 # If this gateway is being licensed as a Cisco UBE the following lines are also required
 mode border-element
sip
     rel1xx disable
     header-passing
     options-ping 60
     midcall-signaling passthru
```

**Step 2** Configure voice codec preference:

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

**Step 3** Configure default services:

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

**Step 4** 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 5** 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 6** Configure the hardware resources (transcoder, conference bridge, and MTP):

```
#This section is only for reference.
#You must 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 7** 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 8** 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
```

**Step 9** Configure SNMP:

```
snmp-server community <string name> ro
```

**Step 10** Configure back-office:

```
# Example here is for Internal number that is dialed is 82009999 and converting the Internal
 number
# to the PSTN number : 2142009999
# Note
# Example:
voice translation-rule 2
     rule 1 /^8200/ /214200
voice translation-profile Xform
     translate called 2

# Note Ensure that you configure dial-peers for each CVP server
dial-peer voice 2 voip
    description out dial-peer CC pilot dial-peer
     translation-profile outgoing Xform
     destination-pattern 8200T
     session protocol sipv2
     session target ipv4:<IP address of CVP Server>
     session transport tcp
     voice-class codec 1
     dtmf-relay rtp-nte
```

## Configure VXML Gateway

### 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
```

# 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 375 | |
| 2 | Configure Unified Communications Manager Subscriber, on page 376 | |
| 3 | Install VMware Tools, on page 252 | |
| 4 | Unified Communications Manager License, on page 377 | |
| 5 | Activate Services , on page 379 | |
| 6 | Validate Clusterwide Domain Configuration, on page 380 | |
| 7 | Install JTAPI on Unified CCE Servers, on page 380 | |
| 8 | Configure SNMP, on page 401 | |

## 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

#### Before You Begin

Generate the license using this procedure: Generate and Register License, on page 378

### 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** Go to **License Management > Licenses**. Under Other Fulfillment options, click **Generate License Request**.

**Step 2** When the License Request and Next Steps window opens, copy the text as directed (PAK ID) and save it to a text editor.

**Step 3** Click the **Cisco License Registration** site and proceed with steps in the site. Keep the PAK handy; you will need it.

**Step 4** Enter the PAK when prompted.
You will 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 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 366.

## Install JTAPI on Unified CCE Servers

Now that you configured the Unified Communications Manager, you can Install JTAPI, on page 333 .

# Configure Unified Intelligence Center with Live Data

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Unified Intelligence Center Publisher, on page 381 | |
| 2 | Configure Unified Intelligence Center Subscriber, on page 381 | |
| 3 | Install VMware Tools, on page 252 | |
| 4 | Configure Unified Intelligence Center Reporting, on page 382 | |
| 5 | Configure Unified Intelligence Center Administration, on page 385 | |

| Sequence | Task | Done? |
|---|---|---|
| 6 | Configure SNMP, on page 401 | |
| 7 | Configure Live Data AW-Access, on page 387 | |
| 8 | Configure Live Data Machine Services, on page 388 | |
| 9 | Configure Live Data Unified Intelligence Data Sources, on page 389 | |
| 10 | Configure Live Data Reporting Interval, on page 390 | |
| 11 | Import Live Data Reports, on page 391 | |
| 12 | Add Certificate for HTTPS Gadget, on page 391 | |

## 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.

## 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.

## 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 2014 Management Studio**.

**Step 3** Login using default 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 following check boxes:

- **public**
- **securityadmin**
- **serveradmin**
- **setupadmin**
- **sysadmin**

**Step 7** In **User Mapping** page, enter the following values:

a) Check the **Real-time database** and **Historical database** check boxes .

b) In **Database role memberships** pane, check the following check boxes:

- **db_datareader**
- **db_datawriter**
- **db_ddladmin**
- **db_owner**
- **db_securityadmin**
- **public**

**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** Click **Data Sources** drawer in the left panel to open the **Data Sources** page.

**Step 3** Choose the **UCCE Historical** 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 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 **UCCE 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 ICM/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 **sAMAccountName**.

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**.

**Step 3** Configure syslog for all devices.

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

- Select the associated servers.
- 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.

#### What to Do Next

### Upload License

Who can upload the license: The System Application User who is the default Superuser.

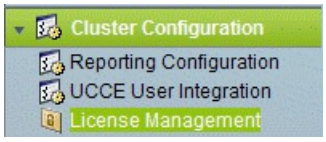
As soon as the System Application User signs in, the user must upload the license file. The file is uploaded to the Controller publisher node and, within a minute, is automatically replicated to all nodes in the cluster.

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 66: 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 352

## Configure Live Data AW-Access

Live Data AW DB access commands allow you to configure and view CCE AW DB (real-time distributor) access for Contact Center Enterprise Live Data Product Deployment Selection. You can also test the connection.

### Procedure

**Step 1** Log in to **CUIC Live Data Console** and execute 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 54: Command Description*

| Command | Description | Example |
|---|---|---|
| **addr** | Specifies the hostname or IP address of the primary or secondary 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)<br>For more information about creating user, see Configure the SQL User Account , on page 383 | user |
| **pwd** | Specifies the login password (maximum 128 characters). | password |
| **test** | This parameter is optional.<br>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 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 55: 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.

## 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 56: 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<br>**Important** Given node should be in service. |

| Command | Description | Example |
|---|---|---|
| **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 57: Command Description***

| Command | Description | Example |
|---|---|---|
| **reporting-interval-in-minutes** | Specifies the reporting interval in minutes format.<br>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**

## Import Live Data Reports

Ensure that the data source is used to import 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.

Follow the below steps to import an existing Unified Intelligence Center stock reports and report definition.

### Procedure

**Step 1** Click **Reports** in the left pane.

**Step 2** Click **Import Report**.

**Step 3** In **File Name (XML File)** field, click **Browse** to select the XML file.

**Step 4** Browse the report XML zip file and click **Open**.

**Step 5** In **Save to** filed, browse the folder where you want to place the imported report definition.
Use arrow keys to expand the folders.

**Step 6** Click **Import**.

**Step 7** Choose **Data Source for ReportDefinition** from the drop-down list.

**Step 8** Choose **Data Source for ValueList** defined in report definition from the drop-down list.

**Step 9** Optional, in **Save to** filed, browse the folder where you want to place the imported report definition.

**Step 10** Click **Import**.

## 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 393 | |

| Sequence | Task | Done? |
|---|---|---|
| 2 | Configure Settings for the CTI Server and Administration and Data Server, on page 394 | |
| 3 | Configure Cisco Finesse Secondary Node, on page 396 | |
| 4 | Install VMware Tools, on page 252 | |
| 5 | Configure Cisco Finesse Administration, on page 398 | |
| 6 | Configure SNMP, on page 401 | |

## 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 CTI Server Settings in the Cisco Finesse Primary Node, on page 394
- Configure Unified Contact Center Enterprise Administration and Data Server, on page 396
- Restart the Cisco Tomcat Service, on page 396


### Configure CTI Server Settings in the Cisco Finesse Primary Node

#### Procedure

**Step 1** Launch the URL `http://<HOST ADDRESS>/cfadmin`, where *Host Address* is the hostname or IP address of your primary Cisco Finesse server.

**Step 2** Go to **Home > Contact Center Enterprise CTI Server Settings**.

**Step 3** Under **Contact Center Enterprise CTI Server Settings**, update the following:

a) See Table 58: Cisco Finesse Configurations, on page 395 and enter the side A host/IP Address.
b) Side A Port (CTI server port on side A), enter 42027.
c) See Table 58: Cisco Finesse Configurations, on page 395 and enter the peripheral ID (of the call manager PIM).
d) See Table 58: Cisco Finesse Configurations, on page 395 and enter the side B host/IP Address.
e) Side B Port (CTI server port on side B), enter 43027.

**Step 4** Click **Save**.

*Table 58: Cisco Finesse Configurations*

| | 500/1000 Agents | 4000 Agents | Small Contact Center | 12,000 Agents |
|---|---|---|---|---|
| Side A host/IP address | CCE Call Server A | FINESSE1: CCE Agent PG 1A<br>FINESSE2: CCE Agent PG 2A | FINESSE X: CCE Agent PG XA. *Where X is the sub customer number* | FINESSE1: CCE Agent PG 1A<br>FINESSE2: CCE Agent PG 2A<br>FINESSE3: CCE Agent PG 3A<br>FINESSE4: CCE Agent PG 4A<br>FINESSE5: CCE Agent PG 5A<br>FINESSE6: CCE Agent PG 6A |
| Side A Port | 42027 | 42027 | 42027 | 42027 |
| Peripheral ID | 5000 | FINESSE1: 5000<br>FINESSE2: 5001 | See**PG Explorer** and enter the peripheral ID of the sub customer. | FINESSE1: 5000<br>FINESSE2: 5001<br>FINESSE3: 5002<br>FINESSE4: 5003<br>FINESSE5: 5004<br>FINESSE6: 5005 |
| Side B host/IP address | CCE Call Server B | FINESSE1: Agent PG 1B<br>FINESSE2: Agent PG 2B | FINESSE X: CCE Agent PG XB. *Where X is the sub customer number* | FINESSE1: CCE Agent PG 1B<br>FINESSE2: CCE Agent PG 2B<br>FINESSE3: CCE Agent PG 3B<br>FINESSE4: CCE Agent PG 4B<br>FINESSE5: CCE Agent PG 5B<br>FINESSE6: CCE Agent PG 6B |
| Side B Port | 43027 | 43027 | 43027 | 43027 |

### Configure Unified Contact Center Enterprise Administration and Data Server

#### Procedure

**Step 1** Select **Home** > **Contact Center Enterprise Administration & Data Server Settings**. (This menu structure assumes the default configuration.)

**Step 2** Under **Contact Center Enterprise Administration & Data Server Settings**, update the following:

a) Primary Host/IP Address (of Side A AW Server)
b) Database Port: 1433
c) Backup Host/Ip Address (of Side B AW Server)
d) Domain (required field): The name of the Unified CCE to which Finesse connects.
e) AW Database Name: <ucceinstance_awdb>
f) UserName: The domain username that is required to sign in to the database. This should not be SQL user.
g) Password: The password required to sign in to the database.

**Step 3** Click **Save**.

### Restart the Cisco Tomcat Service

After you change and save any value on Contact Center Enterprise 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.

#### What to Do Next

For golden templates, configure the secondary node.

For direct installation, check the replication status.

## 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 a CA Certificate

**Note** This procedure applies only if you are using HTTPS.

This procedure is optional. If you are using HTTPS, you can choose to obtain and upload a CA certificate or you can choose to use the self-signed certificate provided with Cisco Finesse.

To eliminate browser security warnings each time that you sign in, obtain an application and root certificate signed by a Certificate Authority (CA). Use the Certificate Management utility from Cisco Unified Operating System Administration.

To open Cisco Unified Operating System Administration, enter the following URL in your browser: `https://FQDN of primary Finesse server:8443/cmplatform`.

Sign in using the username and password for the application user account created during Cisco Finesse installation.

### Procedure

**Step 1** Generate a CSR as follows.
a) Select **Security > Certificate Management > Generate CSR**.
b) From the certificate name drop-down list, select **tomcat**.
c) Click **Generate CSR**.

**Step 2** Download the CSR.
a) Select **Security > Certificate Management > Download CSR**.
b) From the certificate name drop-down list, select **tomcat**.
c) Click **Download CSR**.

**Step 3** Use the CSR to obtain the signed application certificate and the CA root certificate from the Certificate Authority.

**Step 4** When you receive the certificates, select **Security > Certificate Management > Upload Certificate**.

**Step 5** Upload the root certificate.
a) Choose **tomcat-trust** from **Certificate Name** drop-down list.
b) Click **Browse** and open the root certificate file, in **Upload File** field.
c) Click **Upload File**.

**Step 6** Upload the application certificate.
a) Choose **tomcat** from **Certificate Name** drop-down list.
b) Enter the name of the CA root certificate in the **Root Certificate** field.

c) Click **Browse** and open the root certificate file, in **Upload File** field.
d) Click **Upload File**.

**Step 7** After the upload is complete, sign out from Cisco Finesse.

**Step 8** Access the CLI on the primary Cisco Finesse server.

**Step 9** Enter **utils service restart Cisco Finesse Notification Service** command to restart the Cisco Finesse Notification service.

**Step 10** Enter **utils service restart Cisco Tomcat** command to restart the Cisco Tomcat service.

**Step 11** Upload the root certificate and application certificate to the secondary Cisco Finesse server.

**Note** Enter the following URL in browser: `https://FQDN of secondary Finesse server:8433/cmplatform`, to open **Cisco Unified Operating System Administration** for the secondary server.

**Step 12** Access the CLI on the secondary Cisco Finesse server and restart the Cisco Finesse Notification Service and the Cisco Tomcat Service.

## Trust Self-Signed Certificate for Cisco Finesse

After you define configuration settings, disable CSA, and restart services. Authorized agents can sign in to the Cisco Finesse Agent Desktop.

After you restart Cisco Finesse, it takes approximately 6 minutes for all server-related services to restart. Therefore, you should wait 6 minutes before you attempt to sign in to the Agent Desktop.

### Procedure

**Step 1** Enter the following URL in browser: `https://FQDN of Finesse server:8443/cmplatform`.

**Step 2** When you access Agent Desktop for the first time using HTTPS, it prompts you to trust the self-signed certificate provided with Cisco Finesse. Following table describes the procedure for each supported browser.

**Note** If you are using HTTP or if you have installed a CA Certificate, you are not prompted to trust the self-signed certificate. Enter your agent ID, password, and extension, and click **Sign In**.

| Browser | Description |
|---|---|
| Internet Explorer | **1** A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)**. This action opens the sign in page for the Agent Desktop.<br>A certificate error appears in the address bar of your browser.<br>**2** Click **Certificate Error**, and then click **View Certificates** to open the Certificate dialog box.<br>**3** In Certificate dialog box, click **Install Certificate**, to open Certificate Import Wizard.<br>**4** Click **Next**.<br>**5** Select **Place all certificates in the following store**, and then click **Browse**.<br>**6** Select **Trusted Root Certification Authorities**, and then click **OK**.<br>**7** Click **Next**.<br>**8** Click **Finish**.<br>**9** If a Security Warning dialog box asks if you want to install the certificate, click **Yes**.<br>After installation, displays success message.<br>**10** Click **OK**.<br>**11** Enter your agent ID, password, and extension, and then click **Sign In**. |
| Mozilla Firefox | **1** A page appears that states this connection is untrusted.<br>**2** Click **I Understand the Risks**, and then click **Add Exception**.<br>**3** In **Add Security Exception** dialog box, ensure the **Permanently store this exception** check box is checked.<br>**4** Click **Confirm Security Exception**.<br>The page that states this connection is untrusted automatically closes and the Agent Desktop loads.<br>**5** Enter your agent ID, password, and extension, and then click **Sign In**. |

## Browser Settings for Internet Explorer

Configure the following privacy and advanced settings:

### Before You Begin

If you are using Internet Explorer to access the Cisco Finesse desktop, you must configure the following to the browser to ensure that all the features of Cisco Finesse work properly.

- Disable pop-up blockers.

- Ensure that the desktop is not running in Compatibility View; Cisco Finesse does not support Compatibility View.

### Procedure

**Step 1** From the browser menu bar, choose **Tools** > **Internet Options**.
**Step 2** Click **Privacy** tab and click **Sites**.
**Step 3** In **Address** field, enter the domain name for side A of Cisco Finesse server.
**Step 4** Click **Allow**.
**Step 5** In **Address** field, enter the domain name for side B of Cisco Finesse server.
**Step 6** Click **Allow** and click **OK**.
**Step 7** Click **Advanced** tab on the Internet Options dialog box.
**Step 8** Uncheck **Warn about certificate address mismatch** check box, in **Security** pane.
**Step 9** Click **Ok**.

### What to Do Next

You must enable the following security settings to allow users to sign in:

- Run ActiveX controls and plug-ins
- Script ActiveX controls marked as safe for scripting
- Active scripting

To enable these setting , do the following:

1 From the browser menu bar, choose **Tools** > **Internet Options**.
2 Choose **Security** tab and click **Custom Level**.
3 Enable the **Run ActiveX controls and plug-ins** and **Script ActiveX controls marked safe for scripting**, in **ActiveX controls and plug-ins**.
4 Enable the **Active Scripting**, in **Scripting**.

## Configure SNMP

### Procedure

**Step 1** Log in to the Cisco Unified Serviceability *(https://hostname of primary server/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 master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master 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 master agent. To continue the configuration without restarting the SNMP master agent, click **Cancel**. To restart the SNMP master agent service, click **OK**.
j) Click **OK**.

# Create a Customer Instance for the1000 Agent Deployment Model

Follow this sequence of tasks to create the customer instance to deploy 1000 agent for Cisco HCS for Contact Center.

*Table 59: Create customer instance for 1000 agent deployment of Cisco HCS for Contact Center*

| Sequence | Task | Done? |
|---|---|---|
| 1 | Upgrade VMware Tools, on page 320 | |
| 2 | Set Up Virtual Machine Startup and Shutdown, on page 320 | |
| 3 | Create a Domain Controller Server, on page 321 | |
| 4 | Configure Cisco Unified CCE Call Server, on page 323 | |
| 5 | Configure Unified CCE Data Server, on page 338 | |
| 6 | Configure Unified CVP, on page 347 | |
| 7 | Configure Cisco IOS Enterprise Voice Gateway, on page 369 | |
| 8 | Configure Unified Communications Manager, on page 375 | |
| 9 | Configure Unified Intelligence Center with Live Data, on page 380 | |
| 10 | Configure Cisco Finesse, on page 392 | |

# 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 Contact Center. After each task, return to this page to mark the task “done” and continue the sequence.

*Table 60: Create customer instance for 4000 agent deployment of Cisco HCS for Contact Center*

| Sequence | Task | Done? |
|---|---|---|
| 1 | Upgrade VMware Tools, on page 320 | |
| 2 | Set Up Virtual Machine Startup and Shutdown, on page 320 | |
| 3 | Create a Domain Controller Server, on page 321 | |
| 4 | Configure Cisco Unified CCE Rogger, on page 404 | |
| 5 | Configure Unified CCE AW-HDS-DDS, on page 409 | |
| 6 | Configure Unified CCE Agent PG 1, on page 412 | |
| 7 | Configure Unified CCE Agent PG 2, on page 418 | |
| 8 | Configure Unified CCE VRU PG, on page 420 | |
| 9 | Configure Unified CVP, on page 347 | |

| Sequence | Task | Done? |
|---|---|---|
| 10 | Configure Cisco IOS Enterprise Voice Gateway, on page 369 | |
| 11 | Configure Unified Communications Manager, on page 375 | |
| 12 | Configure Unified Intelligence Center , on page 423 | |
| 13 | Configure Live Data Reporting System, on page 423 | |
| 14 | Configure Cisco Finesse, on page 392 | |

# 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 338 | |
| 2 | Verify the Machine in Domain, on page 334 | |
| 3 | Configure the Domain Manager, on page 324 | |
| 4 | Configure Unified CCE Encryption Utility, on page 340 | |
| 5 | Configure SQL Server, on page 341 | |
| 6 | Configure Secondary Drive, on page 341 | |
| 7 | Configure the Unified CCE Logger, on page 405 | |
| 8 | Configure the Unified CCE Router, on page 405 | |
| 9 | Load Base Configuration, on page 408 | |
| 10 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 11 | Cisco SNMP Setup, on page 334 | |

## 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 500 and 1000 agents deployments, 1-2.
- For 4000 agents deployment, 1-5.
- For 12000 agents deployment, 1-15.

**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 ICM 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.

## 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** Review **Summary** window, and then click **Finish**.

**Note** Do not start service until all ICM components are installed.

### What to Do Next

Set database and log file size, see Database and Log File Size, on page 343.

## Database and Log File Size

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

### Before You Begin

Use DB Estimator Tool to calculate database and log file size.

Alternative option is to size the database and log using the values from Table 61: Data and Log File Size, on page 407. The values in the table for HCS 500 and 1000 agent deployments are sized without considering optional HDS.

### Procedure

**Step 1** Open **SQL Server 2014 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 log files.

**Step 5** Set the initial size of the data and log files according to DB Estimator Tool or from the following table:

***Table 61: Data and Log File Size***

| Database | Data size(MB) | Log Size(MB) | Deployment Type |
|---|---|---|---|
| Side A, Side B | 409600 | 1024 | 500 and 12000 Agent Deployments |
| Side A, Side B | 665600 | 3072 | 1000 Agent Deployment |
| Side A, Side B | 122900 | 1024 | Other HCS Deployments |

## Load Base Configuration

Complete this procedure to upload the following base configuration parameters. For more information on base configuration parameter see Base Configuration Parameters for 4000 Agent Deployment, on page 775.

1. PG Explorer
2. Network VRU Explorer
3. System Information
4. Expanded Call Variable List
5. Network VRU
6. Default Agent Desk Settings
7. Application Instance List
8. Media Class for Multi Channel
9. Media Routing Domain
10. Network VRU Mapping
11. Agent Targeting Rule
12. Outbound Dialer

### Procedure

**Step 1** Download the HCS-10(1)-4000-Agent-Day1-Configuration.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 CCE Rogger on Side A.

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

**Step 5** Select the 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 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 CCE Rogger of source in **Server Name** field and click **OK**.
c) Click **Add** in **Destination** pane.

d) Enter hostname for CCE Rogger of destination in **Server Name** field and click **OK**.
e) Click **Synchronize**.

**Step 13** Click **Start**. After synchronization click **OK**.

# 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 62: Configuring Unified CCE AW-HDS-DDS for Side A and Side B***

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Network Cards, on page 338 | |
| 2 | Validate Network Card, on page 348 | |
| 3 | Configure Unified CCE Encryption Utility, on page 340 | |
| 4 | Configure SQL Server, on page 341 | |
| 5 | Configure Secondary Drive, on page 341 | |
| 6 | AW-HDS-DDS, on page 409 | |
| 7 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 8 | Cisco SNMP Setup, on page 334 | |
| 9 | Final Tasks, on page 346 | |

## AW-HDS-DDS

- Create Instance, on page 410
- Create HDS Database, on page 410
- Configure AW-HDS-DDS, on page 411
- Database and Log File Size, on page 412

## Create Instance

### Procedure

**Step 1** Launch Unified Contact Center Enterprise 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).

### 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) Click **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** Review the Summary window, and click **Finish**.

**Note** Do not start service until all ICM components are installed.

### Database and Log File Size

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

#### Before You Begin

Use DB Estimator Tool to calculate database and log file size.

Alternative option is to size the database and log using the values from Table 63: Data and Log File Size, on page 412.

#### Procedure

**Step 1** Open **Microsoft SQL Server Management Studio**.
**Step 2** Expand the Database in Object Explorer.
**Step 3** Choose **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 log files.
**Step 6** Set the initial size of the data and log files according to DB Estimator Tool or from the following table:

***Table 63: Data and Log File Size***

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

# Configure Unified CCE Agent PG 1

This section explains the configuration procedures you must perform for the Unified CCE Agent PG on both the side A and B.

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Network Cards, on page 338 | |

| Sequence | Task | Done? |
|---|---|---|
| 2 | Verify the Machine in Domain, on page 334 | |
| 3 | Configure Unified CCE Encryption Utility, on page 340 | |
| 4 | Configure CUCM Peripheral Gateway for 4000 Agent Deployment Model, on page 413 | |
| 5 | Configure Media Routing Peripheral Gateway, on page 415 | |
| 6 | Configure CTI Server, on page 417 | |
| 7 | Configure CTI OS Server, on page 332 | |
| 8 | Install JTAPI, on page 333 | |
| 9 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 10 | Cisco SNMP Setup, on page 334 | |

## Configure CUCM Peripheral Gateway for 4000 Agent Deployment Model

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.

- Prepare to Add PIMs, on page 413
- Add PIM1(CUCM PIM), on page 414
- After Creating PIMs, on page 414

### Prepare to Add PIMs

Complete the following procedure to prepare to add PIMs (Peripheral Interface Manager).

#### Procedure

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

**Step 2** Click **Add** in the ICM Instances pane.

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

**Step 4** Enter **0** in the Instance Number field. Click **Save**.

**Step 5** Click **Add** in the **Instance Components** pane, and from the **Component Selection** dialog box choose **Peripheral Gateway**.

**Step 6** In the **Peripheral Gateway Properties** dialog box:

a) Check **Production mode**.

b) Check **Auto start system startup**.

c) Check **Duplexed Peripheral Gateway**.
d) In the **PG Node Properties ID field**, choose **PG1** for Agent PG1 machine or choose **PG2** for Agent PG 2 machine.
e) Click the appropriate Side (**Side A** or **Side B**).
f) Under Client Type pane, add **CUCM** to the selected types.
g) Click **Next**.

### Add PIM1(CUCM PIM)

In the **Peripheral Interface Manager** pane of the **Peripheral Gateway Component Properties** dialog box, click **Add** and configure PIM1 with the Client Type of Unified Communications Manager as follows:

#### Procedure

**Step 1** Check **Enabled**.
**Step 2** In the **Peripheral** name field, enter **CUCM_PG_1** for Agent PG1 or enter **CUCM_PG_2** for Agent PG2.
**Step 3** In the **Peripheral ID** field, enter **5000** for Agent PG1 or enter **5001** for Agent PG2.
**Step 4** In the **Agent extension length** field, enter extension length for this deployment.
**Step 5** In the **CUCM Parameters** pane, configure as follows:
a) In the **Service** field, enter the hostname of Unified Communications Manager Subscriber.
b) In the **User ID** field, enter **pguser** for Agent PG1 or enter **pguser2** for Agent PG2.
c) In the **User password** field, enter the password of the pguser.
d) In the **Mobile Agent Codec** field, choose **G.711** or **G.729**.
**Step 6** Click **OK**.

### After Creating PIMs

#### Procedure

**Step 1** Enter **5000** for Agent PG1 or enter **5001** for Agent PG2 in the **Logical Controller ID** field.
**Step 2** Enter **0** in the **CTI Call Wrapup Data delay** field.
**Step 3** 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 local** in the Side A Properties panel.
c) Choose **Call Router is local** in the Side B Properties panel.
d) Accept the default value in the Usable Bandwidth (kbps) field.

e) Enter **4** in the Heartbeat Interval (100ms) field. Click **Next**.

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

**Step 5** Click the **QoS** button in the private interfaces section for Side A. In the PG Private Link QoS Settings, check the check box **Enable QoS** and click **OK**.
This step applies only to Side A.

**Step 6** Click the **QoS** button in the public interfaces section. In the PG Visible Link QoS Settings, check **Enable QoS** and click **OK**.
This step applies only to Side A.

**Step 7** In the **Peripheral Gateway Network Interfaces** dialog box, click **Next**.

**Step 8** In the **Check Setup Information** dialog box, click **Next**.

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

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

## Configure Media Routing Peripheral Gateway

Complete the following procedures to configure the Unified CCE Media Routing Peripheral Gateway for the Agent PG on Side A and then repeat for Side B. The Media Routing Peripheral Gateway has two PIMs-the MultiChannel PIM and the Outbound PIM.

You must configure this PG, even if Multichannel and Outbound are not used. In that case, this PG remains idle or can be disabled.

### Configure Multichannel and Outbound PIM's 4000 Agent Deployment

Complete the following procedure to configure multichannel and outbound PIM's.

#### Procedure

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

**Step 2** Click **Add** in the **Instance Components** pane, and from the **Component Selection** dialog box choose **Peripheral Gateway**.

**Step 3** In the **Peripheral Gateway Properties** dialog box:

a) Check **Production Mode**.
b) Check **Auto start system startup**.
c) Check **Duplexed Peripheral Gateway**.
d) Choose **PG4** in the **PG node Properties ID** field.
e) Click the appropriate Side (**Side A** or **Side B**).
f) Under Client Type pane, add **Media Routing** to the selected types.
g) Click **Next**.

**Step 4** In the **Peripheral Interface Manager** pane of the **Peripheral Gateway Component Properties** dialog box, click **Add** and configure PIM1 with the Client Type of Media Routing as follows:

a) Check **Enabled**.
b) In the **Peripheral name** field, enter MR.
c) In the **Peripheral ID** field, enter **5018** for Agent PG1 (Do not create any PIM for Agent PG2).
d) In the **Application Hostname (1)**, field, enter the host name or the IP address of the Unified WIM and EIM services server.
e) In the **Application connection port (1)**, field, enter the port number on the Unified WIM and EIM services server that the PIM will use to communicate with the application. The default port is 38001.
f) In the **Application Hostname (2)**, leave the field blank.
g) In the **Application connection port (2)**, leave the field blank.
h) In the **Heartbeat interval (sec)** field, enter 5.
i) In the **Reconnect interval (sec)** field, enter 10.
j) Click **OK**.

**Step 5** Click **Add** and configure **PIM2** with the client type of Media Routing as follows:
a) Check **Enabled**.
b) In the **Peripheral name** field, enter MR2 or a name of your choice.
c) In the **Peripheral ID** field, enter 5019.
d) In the **Application Hostname(1)** field, enter the IP address of Agent PG1 machine on Side A.
e) In the **Application Connection port (1)**, retain the default value.
f) In the **Application Hostname (2)**, field, enter the IP address of Agent PG1 machine on Side B.
g) In the **Application Connection port (2)**, retain the default value.
h) In the **Heartbeat interval (sec)** field, enter 5.
i) In the **Reconnect interval (sec)** field, enter 10 and click **OK**.

**Step 6** Enter **5003** in the **Logical Controller ID** field.

**Step 7** Enter **0** in the **CTI Call Wrapup Data delay** field. Click **Next**.

**Step 8** 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 local** in the Side A Properties panel.
c) Choose **Call Router is local** in the Side B Properties panel.
d) Accept the default value in the Usable Bandwidth (kbps) field.
e) Enter **4** in the Heartbeat Interval (100ms) field. Click **Next**.

**Step 9** In the **Peripheral Gateway Network Interfaces** dialog box, enter the PG Private Interfaces and the PG Public (Visible) Interfaces.
This step applies only to Side A.
a) Click the **QoS** button in the private interfaces section. In the PG Private Link QoS Settings, check the check box **Enable QoS** and click **OK**.
b) Click the **QoS** button in the public(visible) interfaces section. In the PG Visible Link QoS Settings, check the check box **Enable QoS**, click **OK** and click **Next**.

**Step 10** In the **Check Setup Information** dialog box, click **Next**.

**Step 11** In the **Setup Complete** dialog box, click **Finish**.

**Step 12** Click **Exit Setup**.
**Note** Do not start Unified ICM/CC Node Manager until all ICM components are installed.

## Install JTAPI

**Note** This procedure is required for the Unified Contact Center Enterprise Machine having a PG with Unified Communications Manager PIM. However, you must postpone this task until after you Configure Unified Communications Manager, on page 375.

Complete the following procedure to install JTAPI on the Unified Contact Center Enterprise Machine having a PG with Unified Communications Manager PIM for Side A and Side B.

### Procedure

**Step 1** Launch the Unified Communications Manager in a browser (https://{callmanager-hostname}) and log in.

**Step 2** Navigate to **Application** > **Plugins**. Click **Find**.

**Step 3** Download the Cisco JTAPI 32-bit Client for Windows.

**Step 4** Install the downloaded file, accepting all of the default settings.

**Step 5** At the prompt, enter the IP address for the Unified Communications Manager TFTP Server, and click **Next**.

**Step 6** Click **Finish**.

## Configure CTI Server

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

### Procedure

**Step 1** Choose **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.
**Note** Refer to Table 71: Agent PG Table, on page 445, for 12000 agent deployment.
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) For Side A, enter **42027** in the Client Connection Port Number field.

b) For Side B, enter **43027** in the Client Connection Port Number field.

**Step 5** Click **Next**.

**Step 6** In the 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 ICM/CC Node Manager until all ICM components are installed.

# Configure Unified CCE Agent PG 2

This section explains the configuration procedures you must perform for the Unified CCE Agent PG 2 Sides A and B.

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Network Cards, on page 338 | |
| 2 | Verify the Machine in Domain, on page 334 | |
| 3 | Configure Unified CCE Encryption Utility, on page 340 | |
| 4 | Configure CUCM Peripheral Gateway for 4000 Agent Deployment Model, on page 413 | |
| 5 | Configure Outbound PIM for 4000 Agent Deployment, on page 418 | |
| 6 | Configure CTI Server, on page 417 | |
| 7 | Configure CTI OS Server, on page 332 | |
| 8 | Install JTAPI, on page 333 | |
| 9 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 10 | Cisco SNMP Setup, on page 334 | |

## Configure Outbound PIM for 4000 Agent Deployment

Complete the following procedure to configure the outbound PIM.

### Procedure

**Step 1** Choose **Start > All programs > Cisco Unified CCE Tools >Peripheral Gateway Setup**.

**Step 2** Click **Add** in the Instance Components pane, and from the Component Selection dialog box and choose **Peripheral Gateway**.

**Step 3** In the Peripheral Gateway Properties dialog box:

a) Check **Production Mode**.
b) Check **Auto start system startup**.
c) Check **Duplexed Peripheral Gateway**.
d) Choose **PG5** in the PG node Properties ID field.
e) Click the appropriate Side (Side A or Side B).
f) Under Client Type pane, add **Media Routing** to the selected types.
g) Click **Next**.

**Step 4** In the Peripheral Interface Manager pane of the Peripheral Gateway Component Properties dialog box, click **Add** and configure PIM1 with the Client Type of Media Routing as follows:

a) Check *Enabled*.
b) In the peripheral name field, enter *MR1* or a name of your choice.
c) In the Peripheral ID field, enter *5020*.
d) In the Application Hostname(1) field, enter the IP address of Agent PG2 on Side A.
e) The Application Connection port (1), retain the default value.
f) In the Application Hostname (2) field, enter the IP address of Agent PG2 on Side B.
g) The Application Connection port (2), retain the default value.
h) In the Heartbeat interval (sec) field, enter *5*.
i) In the Reconnect interval (sec) field, enter *10* and click **OK**.

**Step 5** Enter **5004** for PG5 in the Logical Controller ID field. Leave all other fields with default values and click **Next**.

**Step 6** 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 local** in the Side A Properties panel.
c) Choose **Call Router is local** in the Side B Properties panel.
d) Accept the default value in the Usable Bandwidth (kbps) field.
e) Enter **4** in the Heartbeat Interval (100ms) field. Click **Next**.

**Step 7** In the Peripheral Gateway Network Interface dialog box, enter the PG Private interface and PG Public (visible) interfaces. Click **Next**.

**Step 8** 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.

**Step 9** Click the **QoS** button in the visible interfaces section. In the PG Visible Link QoS Settings, check **Enable QoS**, click **OK** and click **Next**.
This step applies only to Side A.

**Step 10** Click **Next** on the Check Setup Information dialog box.

**Step 11** In the Setup Complete dialog box, click **Finish**.

**Step 12** Click **Exit Wizard**.

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

# Configure Unified CCE VRU PG

This table lists the configuration procedures you must perform for the Unified CCE VRU PG for Sides A and Side B.

***Table 64: Configure Unified CCE VRU PG for Side A and Side B***

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Network Cards, on page 338 | |
| 2 | Verify the Machine in Domain, on page 334 | |
| 3 | Configure Unified CCE Encryption Utility, on page 340 | |
| 4 | Configure VRU PG, on page 420 | |
| 5 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 6 | Cisco SNMP Setup, on page 334 | |

## Configure VRU PG

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.

- Prepare to Add PIMs, on page 420
- Add VRU PIMs, on page 421
- After Creating PIMs, on page 422

### Prepare to Add PIMs

Complete the following procedure to prepare to add PIMs (Peripheral Interface Manager).

### Procedure

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

**Step 2** Click **Add** in the ICM Instances pane.

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

**Step 4** Enter **0** in the Instance Number field. Click **Save**.

**Step 5** Click **Add** in the **Instance Components** pane, and from the **Component Selection** dialog box choose **Peripheral Gateway**.

**Step 6** In the **Peripheral Gateway Properties** dialog box:

a) Check **Production mode**.
b) Check **Auto start system startup**.
c) Check **Duplexed Peripheral Gateway**.
d) Choose **PG3** in the **PG Node Properties 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**.

## Add VRU PIMs

In the **Peripheral Interface Manager** pane of the **Peripheral Gateway Component Properties** dialog box, click **Add** and configure PIM (total Sixteen PIMs) with the Client Type of VRU as follows:

### Procedure

**Step 1** Check **Enabled.**

**Step 2** In the **Peripheral Name**, **Peripheral ID**, and **VRU host name** fields, enter the following values respective to the CVP servers:

| PIMs | Peripheral Name | Peripheral ID for 4000 Agent Deployment | Peripheral ID for Small Contact Center Agent Deployment | VRU Host name |
|---|---|---|---|---|
| PIM1 | CVP_PG_1A | 5002 | 5001 | IP Address of CVP 1A |
| PIM2 | CVP_PG_1B | 5003 | 5002 | IP Address of CVP 1B |
| PIM3 | CVP_PG_2A | 5004 | 5003 | IP Address of CVP 2A |
| PIM4 | CVP_PG_2B | 5005 | 5004 | IP Address of CVP 2B |
| PIM5 | CVP_PG_3A | 5006 | 5005 | IP Address of CVP 3A |
| PIM6 | CVP_PG_3B | 5007 | 5006 | IP Address of CVP 3B |
| PIM7 | CVP_PG_4A | 5008 | 5007 | IP Address of CVP 4A |
| PIM8 | CVP_PG_4B | 5009 | 5008 | IP Address of CVP 4B |

| PIMs | Peripheral Name | Peripheral ID for 4000 Agent Deployment | Peripheral ID for Small Contact Center Agent Deployment | VRU Host name |
|---|---|---|---|---|
| PIM9 | CVP_PG_5A | 5010 | 5009 | IP Address of CVP 5A |
| PIM10 | CVP_PG_5B | 5011 | 5010 | IP Address of CVP 5B |
| PIM11 | CVP_PG_6A | 5012 | 5011 | IP Address of CVP 6A |
| PIM12 | CVP_PG_6B | 5013 | 5012 | IP Address of CVP 6B |
| PIM13 | CVP_PG_7A | 5014 | 5013 | IP Address of CVP 7A |
| PIM14 | CVP_PG_7B | 5015 | 5014 | IP Address of CVP 7B |
| PIM15 | CVP_PG_8A | 5016 | 5015 | IP Address of CVP 8A |
| PIM16 | CVP_PG_8B | 5017 | 5016 | IP Address of CVP 8B |

**Step 3** In the VRU connect port field, enter **5000**.

**Step 4** In the Reconnect interval (sec) field, enter **10**.

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

**Step 6** In the DSCP field, choose **CS(324)**.

**Step 7** Click **OK**.

**Step 8** Repeat the above steps for the remaining PIMs.

## After Creating PIMs

### Procedure

**Step 1** Enter the appropriate *Peripheral ID* in the **Logical Controller ID** field.

**Step 2** Enter **0** in the **CTI Call Wrapup Data delay** field.

**Step 3** In the **VRU Reporting** pane, select **Service Control** and check **Queue Reporting**. Click **Next**.

**Step 4** 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 local** in the Side A Properties panel.

c) Choose **Call Router is local** in the Side B Properties panel.

d) Accept the default value in the Usable Bandwidth (kbps) field.

e) Enter **4** in the Heartbeat Interval (100ms) field. Click **Next**.

**Step 5** In the **Peripheral Gateway Network Interfaces** dialog box, enter the **PG Private Interfaces** and the **PG Public (Visible) Interfaces**.

**Step 6** Click the **QoS** button in the private interfaces section for Side A. In the PG Private Link QoS Settings, check the check box **Enable QoS** and click **OK**.
This step applies only to Side A.

**Step 7** Click the QoS button in the Public (Visible) Interfaces section. In the PG Visible Link QoS Settings, check the check box **Enable QoS**, click **OK** and click **Next**.
This step applies only to Side A.

**Step 8** In the **Peripheral Gateway Network Interfaces** dialog box, click **Next**.

**Step 9** In the **Check Setup Information** dialog box, click **Next**.

**Step 10** In the **Setup Complete** dialog box, click **Finish**.

**Note** Do not start Unified ICM/CC Node Manager until all ICM 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 381 | |
| 2 | Configure Unified Intelligence Center Subscriber, on page 381 | |
| 3 | Install VMware Tools, on page 252 | |
| 4 | Configure Unified Intelligence Center Reporting, on page 382 | |
| 5 | Configure Unified Intelligence Center Administration, on page 385 | |
| 6 | Configure SNMP, on page 401 | |

# Configure Live Data Reporting System

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Live Data AW-Access, on page 387 | |
| 2 | Configure Live Data Machine Services, on page 388 | |

| Sequence | Task | Done? |
|---|---|---|
| 3 | Configure Live Data Unified Intelligence Data Sources, on page 389 | |
| 4 | Configure Live Data Reporting Interval, on page 390 | |
| 5 | Import Live Data Reports, on page 391 | |
| 6 | Add Certificate for HTTPS Gadget, on page 391 | |

# 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 Contact Center. After each task, return to this page and mark the task “done” and continue the sequence.

***Table 65: Create Customer Instance for core components***

| Sequence | Task | Done |
|---|---|---|
| 1 | Upgrade VMware Tools, on page 320 | |
| 2 | Set Up Virtual Machine Startup and Shutdown, on page 320 | |
| 3 | Create DNS Server for Finesse in Small Contact Center Deployment, on page 436 | |
| 4 | Configure Unified CCE Rogger for Small Contact Center Agent Deployment , on page 425 | |
| 5 | Configure Unified CCE AW-HDS-DDS, on page 409 | |
| 6 | Configure Unified CCE VRU PG, on page 420 | |
| 7 | Configure Unified CVP, on page 347 | |
| 8 | Configure Cisco IOS Enterprise Voice Gateway, on page 369 | |
| 9 | Configure Unified Intelligence Center , on page 423 | |

***Table 66: Configure Dedicated Components Sub Customer Option***

| Sequence | Task | Done |
|---|---|---|
| 1 | Set Up Virtual Machine Startup and Shutdown, on page 320 | |

| Sequence | Task | Done |
|---|---|---|
| 2 | Configure Unified CCE Agent PG for Small Contact Center Agent Deployment, on page 428 | |
| 3 | Configure Unified Communications Manager, on page 375 | |
| 4 | Increase the SW MTP and SW Conference Resources, on page 435 | |
| 5 | Configure Cisco Finesse, on page 392 | |

*Table 67: Configure Shared Components Sub Customer Option*

| Sequence | Task | Done |
|---|---|---|
| 1 | Set Up Virtual Machine Startup and Shutdown, on page 320 | |
| 2 | Configure Unified CCE Agent PG for Small Contact Center Agent Deployment, on page 428 | |
| 3 | Configure Shared Unified Communications Manager, on page 435 | |
| 4 | Configure Cisco Finesse, on page 392 | |

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 473

# 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 338 | |
| 2 | Verify the Machine in Domain, on page 334 | |
| 3 | Configure the Domain Manager, on page 324 | |
| 4 | Configure Unified CCE Encryption Utility, on page 340 | |
| 5 | Configure SQL Server, on page 341 | |
| 6 | Configure Secondary Drive, on page 341 | |
| 7 | Configure the Unified CCE Logger, on page 405 | |
| 8 | Configure Unified CCE Router for Small Contact Center, on page 427 | |

| Sequence | Task | Done? |
|---|---|---|
| 9 | Load Base Configuration for Small Contact Center Agent Deployment , on page 426 | |
| 10 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 11 | Cisco SNMP Setup, on page 334 | |

## Load Base Configuration for Small Contact Center Agent Deployment

Complete this procedure to upload the following base configuration parameters. For more information on base configuration parameter see Base Configuration Parameters for Small Contact Center Agent Deployment, on page 780.

1. PG Explorer
2. Network VRU Explorer
3. System Information
4. Expanded Call Variable List
5. Network VRU
6. Default Agent Desk Settings
7. Application Instance List
8. Media Class for Multi Channel
9. Media Routing Domain
10. Network VRU Mapping
11. Agent Targeting Rule

### Procedure

**Step 1** Download the HCS-10(1)-100-Agent-Day1-Configuration.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 CCE Rogger on Side A.

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

**Step 5** Select the 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 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. Open Data on the menu bar and click **Synchronize**.

a) Enter the hostname for the CCE Rogger on Side A.
b) Enter the database name as <instance name>_sideA for the source side.
c) Enter the hostname for the CCE Rogger on Side B.
d) Enter the database name as <instance name>_sideB for the target side.
e) Click **Synchronize**.

**Step 12** 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** dialog box, enter **1-80** in the Enable Peripheral Gateways field. Click **Advanced** below to expand.

**Step 9** Under Advanced, in the **Enable Peripheral Gateway** dialog box, enter **81-150**. Click **Next** .

**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 ICM components are installed.

# Configure Unified CCE Agent PG for Small Contact Center Agent Deployment

This section explains the configuration procedures you must perform for the Unified CCE Agent PG for small contact center agent deployment Sides A and B.

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Network Cards, on page 338 | |
| 2 | Verify the Machine in Domain, on page 334 | |
| 3 | Configure the Domain Manager, on page 324 | |
| 4 | Configure Unified CCE Encryption Utility, on page 340 | |
| 5 | Configure CUCM Peripheral Gateway for Small Contact Center Agent Deployment Model, on page 429 | |
| 6 | Configure Media Routing Peripheral Gateway for Small Contact Center Agent Deployment Model , on page 432 | |
| 7 | Configure CTI Server for Small Contact Center Agent Deployment Model, on page 432 | |

| Sequence | Task | Done? |
|---|---|---|
| 8 | Configure CTI OS Server, on page 332 | |
| 9 | Install JTAPI, on page 333 | |
| 10 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 11 | Cisco SNMP Setup, on page 334 | |

## Configure CUCM Peripheral Gateway for Small Contact Center Agent Deployment Model

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.

- Add Agent PG Using Unified CCE Configuration Manager , on page 429
- Prepare to Add PIMs, on page 430
- Add PIM1(CUCM PIM), on page 430
- After Creating PIMs, on page 431

### Add Agent PG Using Unified CCE Configuration Manager

Complete the following procedure to add an 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**.

**Step 3** Click **Add PG** and enter the following values in **Logical Controller** pane.

a) In the Peripheral name, enter *CUCM_PG_XX*, where XX is the Agent PG number.
b) In the Client type, choose **CUCM**.

**Step 4** Click on the **Peripheral** under PG and enter the following values in **Peripheral** tab.

a) In the Default desk settings filed, choose **Default_Agent_Desk_settings**.

b) Check **Enable post routing**.

**Step 5** Click on the **Routing client** tab and enter a name for Routing client.

**Step 6** Click **Save** and **Close**.

**Step 7** In the Configuration Manager window, choose **Tools** > **Explorer Tools** > **Network VRU Explorer** .

**Step 8** Choose **Retrieve** > **CVP_Network_VRU** > **Add Label**, enter the routing client you have created in Step 5 and enter the label value as **7777777777** .

**Step 9** Click **Save** and **Close**.

**Step 10** In Configuration Manager window, choose **List Tools** > **Agent Targeting**.

**Step 11** Click **Retrieve** > Select **Add** > In the Attributes field Enter **Name** > Select the **Peripheral** as **CUCM PG** > Select the **Rule Type** as **Agent Extension** > **Routing Client** > **Add** and select the newly added Routing Client and all the CVP routing clients available > **Extension Range** > Add the supported extension range.

**Step 12** Click **Save** and **Close**.

## Prepare to Add PIMs

Complete the following procedure to prepare to add PIMs (Peripheral Interface Manager).

### Procedure

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

**Step 2** Click **Add** in the ICM Instances pane.

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

**Step 4** Enter **0** in the Instance Number field. Click **Save**.

**Step 5** Click **Add** in the **Instance Components** pane, and from the **Component Selection** dialog box choose **Peripheral Gateway**.

**Step 6** In the **Peripheral Gateway Properties** dialog box:

1. Uncheck **Production mode**.
2. Uncheck **Auto start system startup**.
3. Check **Duplexed Peripheral Gateway**.
4. In the **PG Node Properties ID field**, choose **PGXX** where XX is the Agent PG number
5. Click the appropriate Side (**Side A** or **Side B**).
6. Under Client Type pane, add **CUCM** to the selected types.
7. Click **Next**.

## Add PIM1(CUCM PIM)

In the **Peripheral Interface Manager** pane of the **Peripheral Gateway Component Properties** dialog box, click Add and configure PIM1 with the Client Type of Unified Communications Manager as follows:

### Procedure

**Step 1** Check **Enabled**.

**Step 2** In the **Peripheral** name field, enter **CUCM_PG_XX**, where XX is the Agent PG number

**Step 3** In the **Peripheral ID** field, Refer to PG explorer and enter the value.

**Step 4** In the **Agent extension length field**, enter **8** as extension length for this deployment.

**Step 5** In the **CUCM Parameters** pane, configure as follows:

1. In the **Service** field, enter the hostname of Unified Communications Manager Subscriber.
2. In the **User ID** field, enter **pguser**.
3. In the **User password** field, enter the password of the pguser.
4. In the **Mobile Agent Codec** field, choose **G.711** or **G.729**.

**Step 6** Click **OK**.

## After Creating PIMs

### Procedure

**Step 1** Refer to PG Explorer and Enter the value in the **Logical Controller ID** field.

**Step 2** Enter 0 in the **CTI Call Wrapup Data delay** field and Click **Next**.

**Step 3** In the Device Management Protocol Properties dialog box, configure as follows:

1. Click **Side A Preferred**, if you are configuring Side A, or click **Side B Preferred**, if you are configuring Side B.
2. Choose **Call Router is local** in the Side A Properties panel.
3. Choose **Call Router is local** in the Side B Properties panel.
4. Accept the default value in the Usable Bandwidth (kbps) field.
5. Enter **4** in the Heartbeat Interval (100ms) field. Click **Next**.

**Step 4** In the **Peripheral Gateway Network Interfaces** dialog box, enter the Private Interfaces and the Public (Visible) Interfaces.

**Step 5** Click the **QoS** button in the private interfaces section for Side A. In the PG Private Link QoS Settings, check the check box **Enable QoS** and click **OK**.
This step applies only to Side A.

**Step 6** Click the **QoS** button in the public (visible) interfaces section. In the PG Visible Link QoS Settings, check **Enable QoS** and click **OK**.
This step applies only to Side A.

**Step 7** In the **Peripheral Gateway Network Interfaces** dialog box, click **Next**.

**Step 8** In the **Check Setup Information** dialog box, click **Next**.

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

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

# Configure CTI Server for Small Contact Center Agent Deployment Model

### Before You Begin

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

### Procedure

**Step 1** Choose **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**.

1. Uncheck **Production mode**.
2. Uncheck **Auto start at system startup**.
3. Check **Duplexed CTI Server**.
4. Choose **CGXX** where XX is the PG number.
5. Enter XX as ICM System ID where XX is the Agent PG number.
6. Click the appropriate side (Side A or Side B).
7. Click **Next**.

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

1. For Side A, enter 42027 in the Client Connection Port Number field.
2. For Side B, enter 43027 in the Client Connection Port Number field.

**Step 5** Click **Next**.

**Step 6** In the CTI Server Network Interface Properties dialog box, enter the PG private interfaces, CG private interfaces, and CG visible interfaces details and click **Next**.

**Step 7** Under the Check Setup Information page, verify all the settings, and click **Next**.

**Step 8** In the Setup Completed dialog box, click **Finish**.

**Step 9** Click **Exit Setup**.

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

# Configure Media Routing Peripheral Gateway for Small Contact Center Agent Deployment Model

### Add Media Routing PG Using Unified CCE Configuration Manager

Complete the following procedure to add a Media Routing 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**.

**Step 3** Click **Add PG** and enter the following values in **Logical Controller** pane.

a) In the Peripheral name, enter *MR_PG_XX*, where XX is the MR PG number.
b) In the Client type, choose **MediaRouting**.

**Step 4** Click on the **Peripheral** under PG and enter the following values.

a) In the **Peripheral** tab, rename the Name field and Peripheral name field as **MultiMedia_XX** (XX is MR PG number) and Check **Enable post routing**.
b) In the **Routing Client** tab, enter a name for Multimedia Routing client.
c) In the **Advanced** tab, set the Network VRU as MR_Network_VRU

**Step 5** Click **(2) Add Peripheral** button and enter the following values.

a) In the **Peripheral** tab, rename the Name field and Peripheral name field as **Outbound_XX** (XX is MR PG number) andCheck **Enable post routing**.
b) In the **Routing Client** tab, enter a name for Multimedia Routing client.
c) In the **Advanced** tab,set the Network VRU as MR_Network_VRU

**Step 6** Click **Save** and **Close**.

**Step 7** In **Configuration Manager**, Click **List Tools**, Select **Agent Targeting Rule**.

**Step 8** Click **Retrieve**, Select **Add**, In the **Attributes** Tab Enter **Name**, In the **Peripheral** list, Select **CUCM PG**, Select **Rule Type** as **Agent Extension,** In the **Routing Client** section, Select **Add** and select the newly added Outbound Routing Client, Click **OK**. In the Extension Ranges section, Click **Add** and Provide the supported extension range, Click **OK**.

**Step 9** Click **Save** and **Close**.

## Configure Media Routing Peripheral Gateway for Small Contact Center Agent Deployment Model

Complete the following procedure to configure Media Routing Peripheral gateway on Side A and then repeat the same procedure for Side B.

### Procedure

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

**Step 2** Click **Add** in the Instance Components pane, and from the Component Selection dialog box choose **Peripheral Gateway**.

**Step 3** In the Peripheral Gateway Properties dialog box:

a) Check Production Mode.
b) Check Auto start system startup.
c) Check Duplexed Peripheral Gateway.
d) Choose PG in the PG node Properties ID field.

e) Click the appropriate Side (Side A or Side B).
f) Under Client Type pane, add Media Routing to the selected types.
g) Click **Next**.

**Step 4** In the Peripheral Interface Manager pane of the Peripheral Gateway Component Properties dialog box, click Add and configure PIM1 with the Client Type of Media Routing as follows:

a) Check Enabled.
b) In the Peripheral name field, enter MR.
c) In the Peripheral ID field, enter Peripheral ID for Media Routing. Get the ID form PG Explorer tool.
d) In the Application Hostname (1), field, enter the host name or the IP address of the Unified WIM and EIM services server.
e) In the Application connection port (1), field, enter the port number on the Unified WIM and EIM services server that the PIM will use to communicate with the application. The default port is 38001.
f) In the Application Hostname (2), leave the field blank.
g) In the Application connection port (2), leave the field blank.
h) In the Heartbeat interval (sec) field, enter 5.
i) In the Reconnect interval (sec) field, enter 10.
j) Click OK.

**Step 5** Click Add and configure PIM2 with the client type of Media Routing as follows:

a) Check Enabled.
b) In the Peripheral name field, enter MR2 or a name of your choice.
c) In the Peripheral ID field, Get the Peripheral ID from PG explorer.
d) In the Application Hostname(1) field, enter the IP address of Agent PG1 machine on Side A.
e) In the Application Connection port (1), retain the default value.
f) In the Application Hostname (2), field, enter the IP address of Agent PG1 machine on Side B.
g) In the Application Connection port (2), retain the default value.
h) In the Heartbeat interval (sec) field, enter 5.
i) In the Reconnect interval (sec) field, enter 10 and click OK.

**Step 6** Enter the Logical Controller ID field.Get the ID from PG explorer.

**Step 7** Enter 0 in the CTI Call Wrapup Data delay field. Click Next.

**Step 8** 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 local in the Side A Properties panel.
c) Choose Call Router is local in the Side B Properties panel.
d) Accept the default value in the Usable Bandwidth (kbps) field.
e) Enter 4 in the Heartbeat Interval (100ms) field. Click Next.

**Step 9** In the Peripheral Gateway Network Interfaces dialog box, enter the Private Interfaces and the Visible Interfaces details. This step applies only to Side A.

a) Click the QoS button in the private interfaces section. In the PG Private Link QoS Settings, check the check box Enable QoS and click OK.

b) Click the QoS button in the public(visible) interfaces section. In the PG Visible Link QoS Settings, check the check box Enable QoS, click OK and click Next.

**Step 10** In the Check Setup Information dialog box, click Next.

**Step 11** In the Setup Complete dialog box, click Finish.

**Step 12** Click Exit Setup.

**Note** Do not start Unified ICM/CCNodeManager until all ICMcomponents are installed.

# 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)

# 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 375 | |
| 2 | Configure Unified Communications Manager Subscriber, on page 376 | |
| 3 | Install VMware Tools, on page 252 | |

| Sequence | Task | Done? |
|---|---|---|
| 4 | Unified Communications Manager License, on page 377 | |
| 5 | Activate Services , on page 379 | |
| 6 | Validate Clusterwide Domain Configuration, on page 380 | |
| 7 | Install JTAPI on Unified CCE Servers, on page 380 | |
| 8 | Configure SNMP, on page 401 | |
| 9 | Setup Partition, on page 753 | |
| 10 | Setup Calling Search Space, on page 754 | |
| 11 | Associate CSS and Partition with Phones and Lines, on page 754 | |
| 12 | Associate CSS with Trunk, on page 755 | |

# 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. It is recommended to 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 437
- Configure DNS Server, on page 437

## Enable DNS server

### Procedure

**Step 1** Login in the Server machine in Sub customer network
**Step 2** Navigate to **Administrative Tools** > **Server Manager**
**Step 3** On Left side pane, Click **Roles.**
**Step 4** In the Roles window, Click **Add Roles**.
**Step 5** Click **Next** in the Add Roles Wizard.
**Step 6** In Select Server Roles window, Check **DNS Server**. Click **Next**.
**Step 7** In DNS server Window, Click **Next**.
**Step 8** In Confirm Installation Selections, Click **Install** and Close Wizard after installation.

## 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 the below steps should be followed, only if customer is using shared DNS for finesse installation:

1. Customer should add Finesse internal IP (Not the natted IP ) in both Forward and Reverse lookup zone of shared DNS.
2. Customer need to add unique Finesse hostname in DNS server whereas the IP address could be same.
3. Once the finesse primary and secondary installation is Done successfully, remove the host entry only from Reverse look up zone of Finesse Internal IP.
4. The OS customization of Finesse servers for all sub customers should be done in sequential manner not in parallel.

# 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 Contact Center. After each task, return to this page to mark the task "done" and continue the sequence.

***Table 68: Create customer instance for 12000 agent deployment of Cisco HCS for Contact Center***

| Sequence | Task | Done? |
|---|---|---|
| 1 | Upgrade VMware Tools, on page 320 | |
| 2 | Set Up Virtual Machine Startup and Shutdown, on page 320 | |

| Sequence | Task | Done? |
|---|---|---|
| 3 | Create a Domain Controller Server, on page 321 | |
| 4 | Configure Unified CCE Logger , on page 439 | |
| 5 | Configure Unified CCE Router, on page 441 | |
| 6 | Configure Unified CCE AW-HDS, on page 441 | |
| 7 | Configure Unified CCE HDS-DDS, on page 443 | |
| 8 | Configure Unified CCE Agent PG's for 12000 Agent Deployment, on page 445 | |
| 9 | Configure Unified CCE VRU PG's for 12000 Agent Deployment, on page 447 | |
| 10 | Configure Unified CVP, on page 347 | |
| 11 | Configure Cisco IOS Enterprise Voice Gateway, on page 369 | |
| 12 | Configure Unified Communications Manager, on page 375 | |
| 13 | Configure Unified Intelligence Center , on page 423 | |
| 14 | Configure Live Data Reporting System, on page 423 | |
| 15 | Configure Cisco Finesse, on page 392 | |

# 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 338 | |
| 2 | Verify the Machine in Domain, on page 334 | |
| 3 | Configure the Domain Manager, on page 324 | |
| 4 | Configure Unified CCE Encryption Utility, on page 340 | |
| 5 | Configure SQL Server, on page 341 | |
| 6 | Configure Secondary Drive, on page 341 | |
| 7 | Configure the Unified CCE Logger, on page 405 | |
| 8 | Load Base Configuration, on page 440 | |
| 9 | Verify Cisco Diagnostic Framework Portico, on page 346 | |

| Sequence | Task | Done? |
|---|---|---|
| 10 | Cisco SNMP Setup, on page 334 | |

## Load Base Configuration

Complete this procedure to upload the following base configuration parameters. For more information on base configuration parameter see Base Configuration Parameters for 12000 Agent Deployment, on page 783.

1. PG Explorer
2. Network VRU Explorer
3. System Information
4. Expanded Call Variable List
5. Network VRU
6. Default Agent Desk Settings
7. Application Instance List
8. Media Class for Multi Channel
9. Media Routing Domain
10. Network VRU Mapping
11. Agent Targeting Rule
12. Outbound Dialer

### Procedure

**Step 1** Download the HCS-10(1)-12000-Agent-Day1-Configuration.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 CCE Logger on Side A.

**Step 4** Open the ICMDBA Tool on the CCE Logger on Side A.

**Step 5** Select the 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 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. Open Data on the menu bar and click **Synchronize**.

a) Enter the hostname for the CCE Logger on Side A.
b) Enter the database name as <instance name>_sideA for the source side.
c) Enter the hostname for the CCE Logger on Side B.
d) Enter the database name as <instance name>_sideB for the target side.
e) Click **Synchronize**.

**Step 12** 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 338 | |
| 2 | Validate Network Card, on page 348 | |
| 3 | Configure Unified CCE Encryption Utility, on page 340 | |
| 4 | Configure the Unified CCE Router, on page 405 | |
| 5 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 6 | Cisco SNMP Setup, on page 334 | |

# 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 69: Configuring Unified CCE AW-HDS for Side A and Side B***

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Network Cards, on page 338 | |
| 2 | Verify the Machine in Domain, on page 334 | |
| 3 | Configure Unified CCE Encryption Utility, on page 340 | |
| 4 | Configure SQL Server, on page 341 | |
| 5 | Configure Secondary Drive, on page 341 | |

| Sequence | Task | Done? |
|---|---|---|
| 6 | AW-HDS, on page 442 | |
| 7 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 8 | Cisco SNMP Setup, on page 334 | |
| 9 | Final Tasks, on page 346 | |

# AW-HDS

- Create Instance, on page 410
- Create HDS Database, on page 410
- Configure AW-HDS, on page 442
- Database and Log File Size, on page 412

## Configure AW-HDS

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 **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 ICM 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 70: Configuring Unified CCE HDS-DDS for Side A and Side B***

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Network Cards, on page 338 | |
| 2 | Validate Network Card, on page 348 | |
| 3 | Configure Unified CCE Encryption Utility, on page 340 | |
| 4 | Configure SQL Server, on page 341 | |
| 5 | Configure Secondary Drive, on page 341 | |
| 6 | HDS-DDS, on page 443 | |
| 7 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 8 | Cisco SNMP Setup, on page 334 | |

## HDS-DDS

- Create Instance, on page 410

- Create HDS Database, on page 410
- Configure HDS-DDS, on page 444
- Database and Log File Size, on page 412

## 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 ICM components are installed.

# Configure Unified CCE Agent PG's for 12000 Agent Deployment

This section explains the configuration procedures you must perform for the Unified CCE PG side A and B. HCS for CC 12000 Agent Deployment model requires 6 Agent PG servers. Please repeat the configuration procedures for each Agent PG Server.

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Network Cards, on page 338 | |
| 2 | Verify the Machine in Domain, on page 334 | |
| 3 | Configure the Domain Manager, on page 324 | |
| 4 | Configure Unified CCE Encryption Utility, on page 340 | |
| 5 | Configure CUCM Peripheral Gateway for 12000 Agent Deployment, on page 445 | |
| 6 | Configure Media Routing Peripheral Gateway for 12000 Agent Deployment | |
| 7 | Configure CTI Server, on page 417 | |
| 8 | Configure CTI OS Server, on page 332 | |
| 9 | Install JTAPI, on page 333 | |
| 10 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 11 | Cisco SNMP Setup, on page 334 | |

## Configure CUCM Peripheral Gateway for 12000 Agent Deployment

Complete the following tasks to configure the Unified CCE peripheral gateways for the PG Server on SideA and then repeat the same procedure for Side B. HCS for CC 12000 Agent Deployment model requires 6 Agent PG servers. Repeat the configuration procedures for each Agent PG Server that are mentioned below:

***Table 71: Agent PG Table***

| Agent PG Server | PG Node | CG Node | Peripheral ID | Service | User ID | Logical Controller ID |
|---|---|---|---|---|---|---|
| Agent PG 1 | PG1 | CG1 | 5000 | IP Address of CUCM 1 SUB 1 | pguser | 5000 |
| Agent PG 2 | PG2 | CG2 | 5001 | IP Address of CUCM 1 SUB 2 | pguser2 | 5001 |

| Agent PG Server | PG Node | CG Node | Peripheral ID | Service | User ID | Logical Controller ID |
|---|---|---|---|---|---|---|
| Agent PG 3 | PG3 | CG3 | 5002 | IP Address of CUCM 2 SUB 1 | pguser | 5002 |
| Agent PG 4 | PG4 | CG4 | 5003 | IP Address of CUCM 2 SUB 2 | pguser2 | 5003 |
| Agent PG 5 | PG5 | CG5 | 5004 | IP Address of CUCM 3 SUB 1 | pguser | 5004 |
| Agent PG 6 | PG6 | CG6 | 5005 | IP Address of CUCM 3 SUB 2 | pguser2 | 5005 |

### 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) Check **Auto start system startup**.
c) Check **Duplexed Peripheral Gateway**.
d) Refer to Table 71: Agent PG Table, on page 445 and choose the appropriate PG in the PG node Properties ID field.
e) Click the appropriate Side (Side A or Side B).
f) Under Client Type pane, add **CUCM** 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) n the Peripheral ID field, Refer to Table 71: Agent PG Table, on page 445 and choose the appropriate **Peripheral ID**.
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, Refer to Table 71: Agent PG Table, on page 445 and enter the appropriate IP address of Unified Communications Manager Subscriber.
- In the User ID field, Refer to Table 71: Agent PG Table, on page 445 and enter the appropriate **User ID**.

- 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** Refer to Table 71: Agent PG Table, on page 445 and Enter the appropriate value in the Logical Controller ID field.

**Step 7** Enter **0** in the CTI Call Wrapup Data delay field. Click **Next**.

**Step 8** 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 Local in Side A Properties panel.
c) Choose **Call Router** is Local in Side B Properties panel.
d) Accept the default value in the Usable Bandwidth (kbps) field.
e) Enter **4** in the Heartbeat Interval (100ms) field. Click **Next**.

**Step 9** 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 10** In the Check Setup Information dialog box, click **Next**.

**Step 11** In the Setup Complete dialog box, click **Finish**.

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

## Configure Media Routing Peripheral Gateway for 12000 Agent Deployment

Add Media Routing PG Using Unified CCE Configuration Manager , on page 432

# Configure Unified CCE VRU PG's for 12000 Agent Deployment

This section explains the configuration procedures you must perform for the Unified CCE PG side A and B. HCS for CC 12000 Agent Deployment model requires three VRU PG servers. Please repeat the configuration procedures for each Agent PG Server.

***Table 72: Configure Unified CCE Agent PG's for 12000 agent deployment***

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Network Cards, on page 338 | |
| 2 | Verify the Machine in Domain, on page 334 | |

| Sequence | Task | Done? |
|---|---|---|
| 3 | Configure Unified CCE Encryption Utility, on page 340 | |
| 4 | Configure VRU Peripheral Gateway for 12000 Agent Deployment, on page 448 | |
| 5 | Verify Cisco Diagnostic Framework Portico, on page 346 | |
| 6 | Cisco SNMP Setup, on page 334 | |

## Configure VRU Peripheral Gateway for 12000 Agent Deployment

Complete the following tasks to configure the Unified CCE peripheral gateways for the PG Server on SideA and then repeat the same procedure for Side B. HCS for CC 12000 Agent Deployment model requires three VRU PG servers. Repeat the configuration procedures for each Agent PG Server that are mentioned below:

***Table 73: VRU PG Table***

| VRU PG Server | PG Node | Logical Controller ID | PIM | Peripheral ID | VRU Hostname | PIM | Peripheral ID | VRU Hostname |
|---|---|---|---|---|---|---|---|---|
| VRU PG 1 | PG7 | 5006 | PIM1 | 5006 | CVP server 1A | PIM2 | 5007 | CVP server 1B |
| | | | PIM3 | 5008 | CVP server 2A | PIM4 | 5009 | CVP server 2B |
| | | | PIM5 | 5010 | CVP server 3A | PIM6 | 5011 | CVP server 3B |
| | | | PIM7 | 5012 | CVP server 4A | PIM8 | 5013 | CVP server 4B |
| | | | PIM9 | 5014 | CVP server 5A | PIM10 | 5015 | CVP server 5B |
| | | | PIM11 | 5016 | CVP server 6A | PIM12 | 5017 | CVP server 6B |
| | | | PIM13 | 5018 | CVP server 7A | PIM14 | 5019 | CVP server 7B |
| | | | PIM15 | 5020 | CVP server 8A | PIM16 | 5021 | CVP server 8B |

| VRU PG Server | PG Node | Logical Controller ID | PIM | Peripheral ID | VRU Hostname | PIM | Peripheral ID | VRU Hostname |
|---|---|---|---|---|---|---|---|---|
| VRU PG 2 | PG8 | 5007 | PIM1 | 5022 | CVP server 9A | PIM2 | 5023 | CVP server 9B |
| | | | PIM3 | 5024 | CVP server 10A | PIM4 | 5025 | CVP server 10B |
| | | | PIM5 | 5026 | CVP server 11A | PIM6 | 5027 | CVP server 11B |
| | | | PIM7 | 5028 | CVP server 12A | PIM8 | 5029 | CVP server 12B |
| | | | PIM9 | 5030 | CVP server 13A | PIM10 | 5031 | CVP server 13B |
| | | | PIM11 | 5032 | CVP server 14A | PIM12 | 5033 | CVP server 14B |
| | | | PIM13 | 5034 | CVP server 15A | PIM14 | 5035 | CVP server 15B |
| | | | PIM15 | 5036 | CVP server 16A | PIM16 | 5037 | CVP server 16B |
| VRU PG 3 | PG9 | 5008 | PIM1 | 5038 | CVP server 17A | PIM2 | 5039 | CVP server 17B |
| | | | PIM3 | 5040 | CVP server 18A | PIM4 | 5041 | CVP server 18B |
| | | | PIM5 | 5042 | CVP server 19A | PIM6 | 5043 | CVP server 19B |
| | | | PIM7 | 5044 | CVP server 20A | PIM8 | 5045 | CVP server 20B |
| | | | PIM9 | 5046 | CVP server 21A | PIM10 | 5047 | CVP server 21B |
| | | | PIM11 | 5048 | CVP server 22A | PIM12 | 5049 | CVP server 22B |
| | | | PIM13 | 5050 | CVP server 23A | PIM14 | 5051 | CVP server 23B |
| | | | PIM15 | 5052 | CVP server 24A | PIM16 | 5053 | CVP server 24B |

### 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) Check **Auto start system startup**.
c) Check **Duplexed Peripheral Gateway**.
d) Refer to Table 73: VRU PG Table, on page 448 and choose the appropriate PG 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 PIMs (Total Sixteen PIMs) 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 toTable 73: VRU PG Table, on page 448 and enter the value.
d) In the VRU hostname field, Refer to Table 73: VRU PG Table, on page 448 and enter the hostname of 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 Table 73: VRU PG Table, on page 448 and Enter the appropriate 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 Local in Side A Properties panel.
c) Choose **Call Router** is Local in Side B Properties panel.
d) Accept the default value in the Usable Bandwidth (kbps) field.
e) Enter 4 in the Heartbeat Interval (100ms) 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 for Side A. In the PG Private Link QoS Settings, check Enable **QoS** and 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 ICM/CC Node Manager until all ICM components are installed.

# Configure Unified Intelligence Center

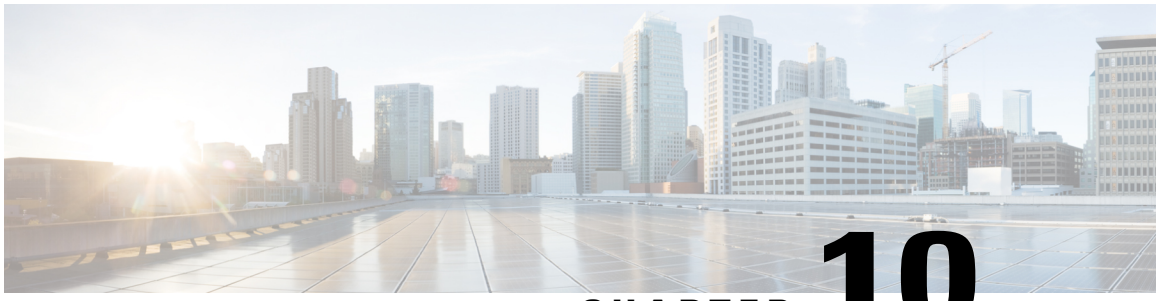
Follow these tasks to configure Unified Intelligence Center.

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Unified Intelligence Center Publisher, on page 381 | |
| 2 | Configure Unified Intelligence Center Subscriber, on page 381 | |
| 3 | Install VMware Tools, on page 252 | |
| 4 | Configure Unified Intelligence Center Reporting, on page 382 | |
| 5 | Configure Unified Intelligence Center Administration, on page 385 | |
| 6 | Configure SNMP, on page 401 | |

# Configure Live Data Reporting System

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure Live Data AW-Access, on page 387 | |
| 2 | Configure Live Data Machine Services, on page 388 | |
| 3 | Configure Live Data Unified Intelligence Data Sources, on page 389 | |
| 4 | Configure Live Data Reporting Interval, on page 390 | |
| 5 | Import Live Data Reports, on page 391 | |

| Sequence | Task | Done? |
|---|---|---|
| 6 | Add Certificate for HTTPS Gadget, on page 391 | |



CHAPTER 10

# Integration of Customer Instance with Shared Management



## Unified CCDM Integration

Unified CCDM will normally be 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

Cisco Unified Contact Center Enterprise (Unified CCE) components must be configured before Unified CCDM can connect to them for Provisioning. Complete the following procedures to configure Unified Contact Center Enterprise for Unified CCDM connectivity

- Establish Two-Way Forest Trust, on page 456
- Setup Unified CCE Servers in Unified CCDM Cluster, on page 458
- Create an Equipment Mapping, on page 460

## 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 the Unified CCE AW for Provisioning, on page 454
- Configure Unified CCE AW Database(AWDB) for Unified CCDM, on page 455

### Configure the Unified CCE AW for Provisioning

Ensure that you create a two-way trust relationship between the Unified CCDM domain and the UCCE domain before configuring AWDB. For more information, see Establish Two-Way Forest Trust, on page 456.

If you use SQL Server Authentication to connect Unified CCDM to Unified Contact Center Enterprise, 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 Contact Center Enterprise.

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 2014 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:

1. In the Login Name field, enter the name for the machine in the following format: <DOMAIN>\<Unified CCDM-HOSTNAME>$.
2. Choose Windows Authentication unless you are connecting to a server on another domain.
3. Select Default language as **English**.

Configure the User Mapping page as follows:

1. In the Users mapped to this login field, check hcs_awdb database.
2. 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 Contact Center Enterprise AW server is dual-sided.

## Configure Unified CCE AW Database(AWDB) for Unified CCDM

For each Unified Contact Center Enterprise instance that Unified CCDM Resource Management connects to must meet the following criteria:

- Unified CCDM Resource Management uses Cisco ConAPI for provisioning connections. This interface should have all the connections made to a primary distributor AW. If the AW is dual-sided, both the sides must be primary distributors.
- Configure an Application Instance on the UCCE distributor machine (AW) for Unified CCDM to connect to Unified Contact Center Enterprise. 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 345. The default name of the Application Instance is **CCDM** as per the Load Base configuration.

- If the AW is dual-sided, each Unified Contact Center Enterprise 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 Contact Center Enterprise instance for each Database Server. This ensures that in a dual-sided system, the alternate side can also connect to the Unified Contact Center Enterprise in a failover scenario.

Complete the following procedure to set up the Configuration Management Service (CMS) server on each Unified Contact Center Enterprise:

#### 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 Contact Center Enterprise 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 Contact Center Enterprise.

#### Procedure

**Step 1** In Cisco 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 Contact Center Enterprise 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 on Unified 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 Contact Center Enterprise AW to connect to.
Preferably, this should be the same as for the Administration & Data Server RMI Registry Port. Each Unified Contact Center Enterprise 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 Contact Center Enterprise Distributor service.

## Establish Two-Way Forest Trust

Create two-way trust between service provider and customer domain controllers for each customer instance of Unified CCDM. Before creating a two-way forest trust, in service provider domain controller and customer domain controller perform the following:

- Create Conditional Forwarders for Customer Domain, on page 457
- Create Forwarders for Customer Domain, on page 457
- Create Conditional Forwarders for Service Provider Domain, on page 457
- Create Forwarders for Service Provider Domain, on page 458

Complete the following procedure to create a two-way forest trust between the service provider domain controller and the customer domain controller:

- Create Two-Way Forest Trust, on page 458

### Create Conditional Forwarders for Customer 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 Service Provider domain.
**Step 6** Click **OK**.

### Create Forwarders for Customer Domain

Complete the following procedure to create forwarders.

#### 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**.

## Setup Unified CCE Servers in Unified CCDM Cluster

Complete the following procedure to configure Unified Contact Center Enterprise 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 209.

**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 Contact Center Enterprise 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 Contact Center Enterprise 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 Contact Center Enterprise 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 455.
- **Remote Registry Port** - Enter the port number of the Unified CCDM Database Server for the Unified Contact Center Enterprise 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 455.
- **Local Port** - Select this as the designated port for live provisioning traffic between the Unified Contact Center Enterprise and Unified CCDM servers. Assign a unique port for each Unified Contact Center

Enterprise. Configure the firewall between the Unified Contact Center Enterprise and Unified CCDM server to allow two-way traffic on this port.

**Note** If Unified Contact Center Enterprise is dual-sided, enter the same port details configured for Side B in Set up CMS Server on Unified Contact Center Enterprise.

**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 Contact Center Enterprise 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 Contact Center Enterprise 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 Contact Center Enterprise Supervisors. The default is **No**. If you select **Yes**, enter the following:

1. 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**.
2. 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 Contact Center Enterprise 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 Contact Center Enterprise equipment.

**Note** To create a equipment mapping for SCC deployment, see Deployment Specific Configurations, on page 466.

### Procedure

**Step 1** Launch **Integrated Configuration Environment** on Unified CCDM Database Server Side A, see Launch the Integrated Configuration Environment, on page 209.

**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 209.

**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:

1. In **Specify Unified CVP Call Server 1 Resource Name** dialog box, enter a name for the call server.
2. 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.
3. 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 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/sub-customer/ISE users from CCDM.

You can also create active directory users in Unified CCE AW, see Create User in UCCE, on page 464

### 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**.

### What to Do Next

Create User, on page 504

## Create User in UCCE

### Procedure

**Step 1** Log in to Unified CCE Admin workstation and open **Configuration Manager**.
**Step 2** Select **List Tools** > **User list** .
**Step 3** Click **Add**.
**Step 4** From **Domain name** drop-down list, select the required UCCE or sub customer domain.
**Step 5** Enter **Username**.

**Example:**
SubCustomer1

**Step 6** Enter the user password and confirm.
**Step 7** Select the appropriate customer definition from **Customer** drop-down list.
**Step 8** Retain the default selection in **Feature control set** drop-down list.
**Step 9** Check both **Configuration** and **Setup** check boxes.
**Step 10** Click **Save**.

**Note** After creating a CCE user, it will automatically create a User in AD domain and also gets imported in CCDM.

### What to Do Next

See, Configure an Imported Unified CCE User, on page 505

# 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 473


- Configure Unified CCE Admin Workstation for Internet Script Editor, on page 465
- Create User, on page 504
- Assign Roles to Users, on page 505
- Install Internet Script Editor , on page 466
- Provision Routing Script Using Internet Script Editor, on page 565


## Configure Unified CCE Admin Workstation for Internet Script Editor

Complete the following procedure to configure Unified 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 User, on page 504
- Assign Permission to Sub-customer Tenant and User, on page 506
- Resource Allocation for Small Contact Center Agent Deployment, on page 468
- Naming Convention for the Resources in Small Contact Center Agent Deployment Model , on page 472

## 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 Contact Center Enterprise 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 458

### 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 contact Center Enterprise 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 UCCE folder that is integrated. In the adjoining pane, check each item of Unified contact Center Enterprise 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 Contact Center Enterprise 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 471
- Map Labels to the Network VRU Type, on page 471


* 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. |

| Parameters | Configuration done by Sub Customer | Configuration done by Service Provider | Notes |
|---|---|---|---|
| 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 |
| Network VRU Script | * | ** & *** | Network VRU Script given in Day1 configuration. Default, it is available under Unallocated Folder.<br>**Note** Since it is mapped to the customer definition “hcs” in day1 config , this can be used by the subcustomer whose customer definition is hcs. Sub customer user creates Network VRU Script specific to sub customer in his own Tenant. |

| Parameters | Configuration done by Sub Customer | Configuration done by Service Provider | Notes |
|---|---|---|---|
| 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 | * | | |
| 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 471. |
| Person | * | | |
| Precision Attribute | * | | |
| Precision Queue | * | | |
| Skill Group | * | | |
| User Variable | * | | |

| Parameters | Configuration done by Sub Customer | Configuration done by Service Provider | Notes |
|---|---|---|---|
| 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 465
- Create User, on page 504
- Assign Permission to Sub-customer Tenant and User, on page 506
- Install Internet Script Editor , on page 466
- Provision Routing Script Using Internet Script Editor, on page 565

# Cisco UCDM Integration

## Basic Configuration of Unified Communication Domain Manager

- Add Customer, on page 473
- Setup Cisco Unified Communication Manager Servers, on page 474
- Configure Network Device List, on page 475
- Add Site, on page 475
- Add Customer Dial Plan, on page 476
- Add Site Dial Plan, on page 476

### 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 587.

## 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** Login 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**.

## 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 476.

### 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

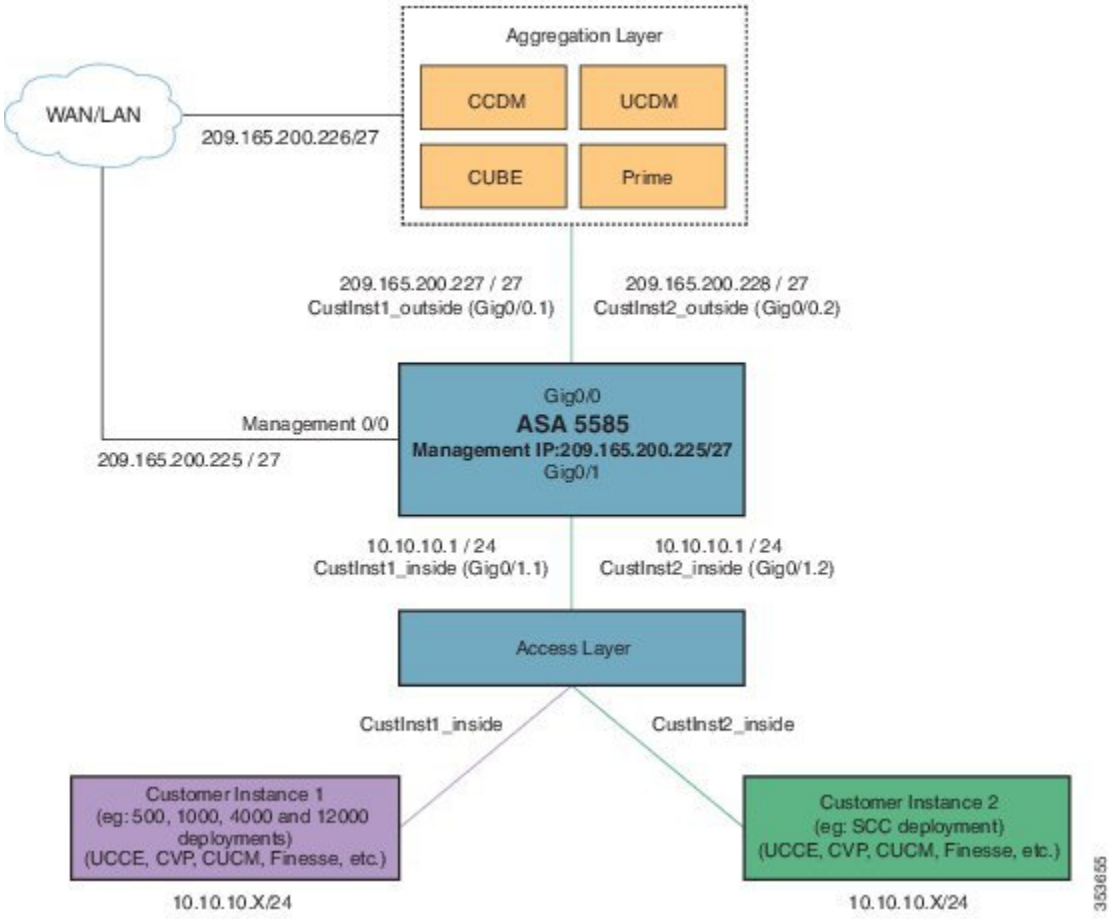
This section covers the configuration procedures required in Cisco ASA to integrate the customer instances for all types of HCS deployment.

• Integration of ASA for Small Contact Center Deployment Model, on page 481

# Integration of ASA for HCS Deployment model

For the 500, 1000, 4000 and 12000 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 67: 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 478
• Configure Security Contexts, on page 479
• Configure Interfaces in the Customer Instance Context, on page 479
• Configure Access-list in the Customer Instance Context, on page 480

• Configure NAT in the Customer Instance Context, on page 480

## 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 500 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 1000 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 500deployment
hostname/500deployment#configure terminal
hostname/500deployment(config)#interface gigabitethernet0/1.1
hostname/500deployment(config-if)#nameif inside
hostname/500deployment(config-if)#ip address 10.10.10.1 255.255.255.0
hostname/500deployment(config-if)#interface gigabitethernet0/0.1
hostname/500deployment(config-if)#nameif outside
hostname/500deployment(config-if)#ip address 209.165.200.227 255.255.255.224
hostname/500deployment(config-if)#exit
hostname/500deployment(config)#exit
hostname/500deployment#changeto context 1000deployment
```

```
hostname/1000deployment#configure terminal
hostname/1000deployment(config)#interface gigabitethernet0/1.2
hostname/1000deployment(config-if)#nameif inside
hostname/1000deployment(config-if)#ip address 10.10.10.1 255.255.255.0
hostname/1000deployment(config-if)#interface gigabitethernet0/0.2
hostname/1000deployment(config-if)#nameif outside
hostname/1000deployment(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.

## Configure NAT in the Customer Instance Context

### Procedure

**Step 1** Configure NAT to enable internet connectivity for inside hosts:

a) Create a network object for the inside network of customer instance.

```
hostname/customer_instance(config)#object network inside_network_name
```

b) Enter the **network id** of inside network with subnet mask.

```
hostname/customer_instance(config-network-object)#subnet network-id subnet-mask
```

c) Enable dynamic NAT for the inside network.

```
hostname/customer_instance(config-network-object)#nat (inside,outside) dynamic interface
```

**Example:**

```
hostname/customer_instance(config)#object network my-inside-net
hostname/customer_instance(config-network-object)#subnet 10.10.10.0 255.255.255.0
hostname/customer_instance(config-network-object)#nat (inside, outside) dynamic interface
```

**Step 2** Configure the static address translation for the customer_instance for CCDM to work withDATASERVER A and B:

a) Create a network object for the DATASERVER-A server address.

```
hostname/customer_instance(config)#object network DATASERVER-A
```

b) Define the DATASERVER-A server address, and configure static NAT with identity port translation.

```
hostname/customer_instance(config-network-object)#host 10.10.10.21
```

c) Open SQL port for DATASERVER-A.

```
hostname/customer_instance(config-network-object)#nat (inside,outside) static
209.165.200.230 service tcp 1433 1433
```

d) Open ConAPI port for DATASERVER-A.

```
hostname/customer_instance(config-network-object)#nat (inside,outside) static
209.165.200.230 service tcp 2094 2094
```

e) Open HTTPS port for DATASERVER-A.

```
hostname/customer_instance(config-network-object)#nat (inside,outside) static
209.165.200.230
service tcp 443 443
```

f) Open SQL port for DATASERVER-B.

```
hostname/customer_instance(config)#object network DATASERVER-B
hostname/customer_instance(config-network-object)#host 10.10.10.22
hostname/customer_instance(config-network-object)#nat (inside,outside) static
209.165.200.231 service tcp 1433 1433
```

g) Open ConAPI port for DATASERVER-B.

```
hostname/customer_instance(config-network-object)#nat (inside,outside) static
209.165.200.231 service tcp 2095 2095
```

h) Open HTTPS port for DATASERVER-B.

```
hostname/customer_instance(config-network-object)#nat (inside,outside) static
209.165.200.231 service tcp 443 443 hostname/customer_instance (config)#route outside
0.0.0.0 0.0.0.0 209.165.200.240
```

**Note** ConAPI ports for DATASERVER A and B should match with the ports configured in the CCDM Cluster.

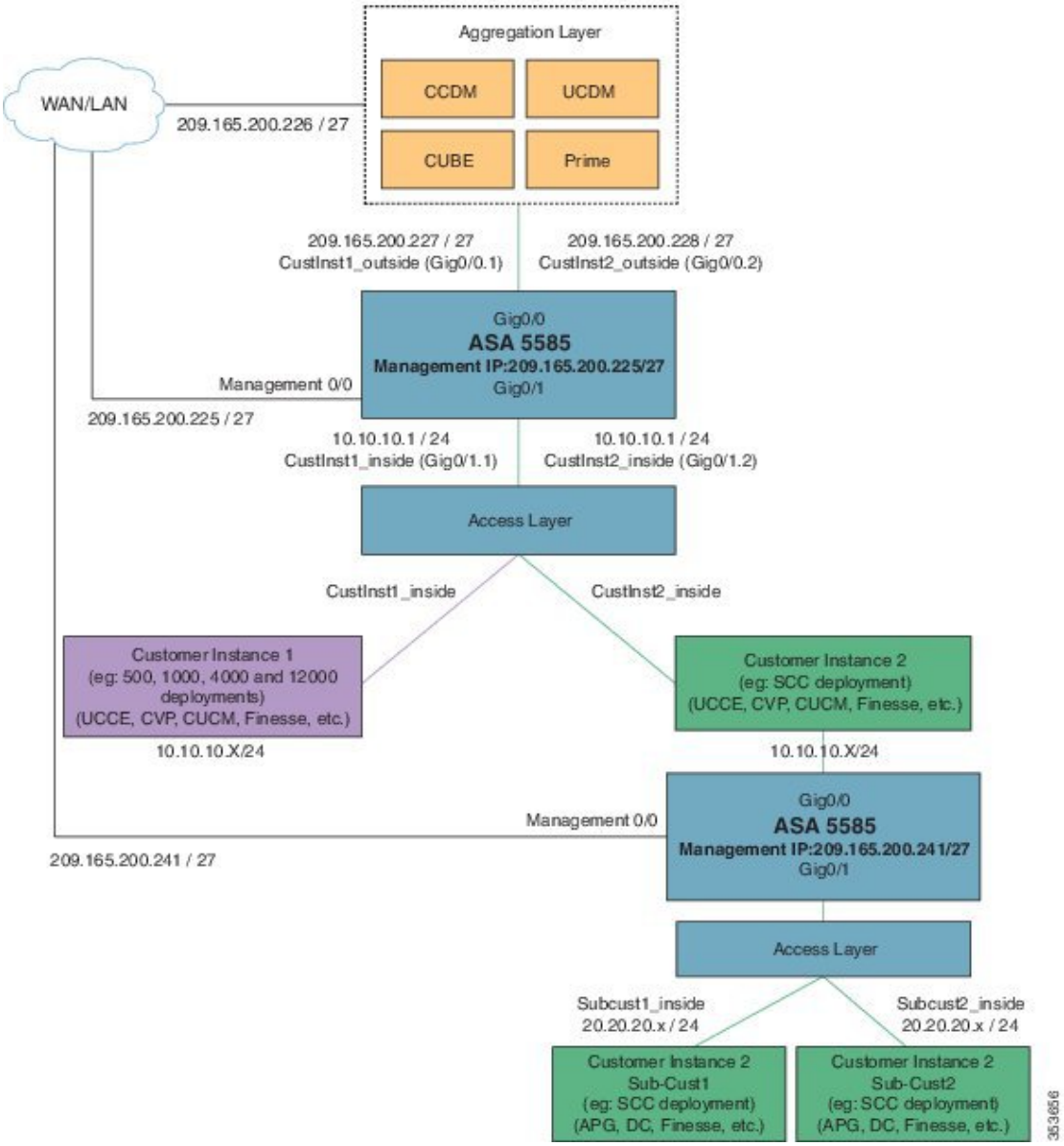
For more information on ports, see Firewall Hardening Considerations, on page 191. Perform NAT and configure the specific ports for respective context.

# 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 500 agent and small contact center instances with two Cisco ASAs.

***Figure 68: Two Customer Instances, for Small Contact Center model Integrated with shared components***




Integrate ASA for Small contact center with shared components, see Install and Configure ASA Firewall and NAT, on page 227

Integrate ASA for Small contact center customer instance with sub-customer instance install and configure ASA, see Install and Configure ASA Firewall and NAT, on page 227. 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 483

- Configure Security Contexts for each Sub-customer Context, on page 484
- Assign MAC Addresses to Context Interfaces Automatically (Optional), on page 230
- Configure Interfaces in each Sub-Customer Instance Context, on page 484
- Configure Access-list in the Sub-customer Instance Context, on page 485
- Configure Static NAT in the Sub-customer instance Context, on page 485


## 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.

## Configure Static NAT in the Sub-customer instance Context

Configure static NAT for integration of sub-customer instances with customer instance :

### Procedure

**Step 1** Create a network object for the sub_cust1 side A.

```
hostname/sub_customer_instance(config)#object network sub_cust_host
```

**Step 2** Define the host IP address and configure static NAT.

```
hostname/sub_customer_instance(config-network-object)#host X.X.X.X
```

**Step 3** Define the outside IP address.

```
hostname/customer_instance(config-network-object)#nat (inside_if_name, outside_if_name)
static X.X.X.X
```

**Example:**

```
hostname/sub-cust1(config)# object network sub-cust1APGA
hostname/sub-cust1(config-network-object)# host 20.20.20.21
hostname/sub-cust1 (config-network-object)# nat(inside,outside) static 10.10.10.121
```

For more information on ports, see Firewall Hardening Considerations, on page 191. Perform NAT and configure the specific ports for respective context.

# Perimeta SBC Integration

This section describes the configuration procedures required in Perimeta SBC to integrate the customer instances.



# Integration of Perimeta SBC for HCS Deployment model



## Configure Service Interface for Customers

To create the service Interface for shared applications, perform the following instructions.

```
config
 system
  service-interface serv4
      description hcscustom
      service-network 4
      port-group-name AccessNetwork
      ipv4
        subnet-prefix-length 24
        gateway-ip-address 10.10.10.2
        local-ip-address 10.10.10.6
          service-address hcscustom
        probes-source-style specific-source
        activate
      vlan-id 60
      network-security trusted
      probes-type none
```

# Configure Adjacencies for Customer Instance

*Table 74: Adjacencies for HCS Deployment Models*

| Sl no | Adjacency Name | Remote Server/Node | Call Flow |
|---|---|---|---|
| 1 | CUST1-CUBE-E | CUBE-E | • Basic Calls from Customer<br>• Internal Help Desk dialing<br>• CCB<br>• Local Breakout Call |
| 2 | CUST1-CUBE-E-OUTBOUND | Outbound Gateway | Agent Based and IVR Based OB calls |


- Add Carrier-Network Adjacency, on page 487
- Add CUBE(E) Adjacency, on page 487


## Add Carrier-Network Adjacency

In this example, the Adjacency is created for one of the customer, CUST1-Carrier-Network.

```
Config
   SBC
     Signaling
      adjacency sip CUST1-Carrier-Network
        description "Trunk to Carrier-Network for CUSTOMER1"
        account cust1
        interop
          preferred-transport tcp
          message-manipulation
            edit-profiles inbound he-dtmf
        force-signaling-peer all-requests
        adjacency-type preset-core
        remote-address-range ipv4 10.10.10.32 prefix-len 32
        service-address SA-shared
          # service-network 10
          # signaling-local-address ipv4 10.10.10.5
        signaling-local-port 5085
        signaling-peer 10.10.10.32
        signaling-peer-port 5060
        statistics-setting summary
       activate
```

## Add CUBE(E) Adjacency

In this example, the adjacency is created for one of the customer, CUST-CUBE-E.

```
Config
   SBC
```

```
Signaling
 adjacency sip CUST-CUBE-E
  description "Trunk to CUBE-E Gateway for HCS CUSTOMER"
  account hcscustom
  interop
   preferred-transport tcp
   message-manipulation
    edit-profiles inbound hcs-dtmf
     ! The list references profiles that do not exist.
   force-signaling-peer all-requests
   adjacency-type preset-core
   remote-address-range ipv4 10.10.10.180 prefix-len 32
   service-address SA-shared
    # service-network 10
    # signaling-local-address ipv4 10.10.10.6
   signaling-local-port 5080
   signaling-peer 10.10.10.180
   signaling-peer-port 5060
   statistics-setting summary
   activate
```

## Configure Call Policy

Here some of the basic calls are covered as part of this call policy.

```
call-policy-set 1
       description first-callpolicy
       first-call-routing-table AdminDomains
       rtg-src-adjacency-table AdminDomains
         entry 1
           match-adjacency Carrier-Network
           dst-adjacency CUST-CUBE-E
           action complete
         entry 2
           match-adjacency CUST-outbound
           dst-adjacency Carrier-Network
           action complete
 complete
      active-call-policy-set
```

# Integration of Perimeta SBC for Small Contact Center Deployment Model



## Configure Service Interface

To create the service Interface for shared application perform the following instructions. This is used for CVP, CUBE-E and for applications that are shared between the sub-customers.

```
config
 System
  service-interface serv3
      description shared
      service-network 3
      port-group-name AccessNetwork
```

```
      ipv4
        subnet-prefix-length 24
        gateway-ip-address 10.10.10.1
        local-ip-address 10.10.10.5
          service-address SA-shared
        probes-source-style specific-source
        activate
      vlan-id 71
      network-security trusted
      probes-type none
```

To create the service Interface for sub-customer perform the following instructions.

```
config
 System
  service-interface serv1
      description customer1
      service-network 1
      port-group-name AccessNetwork
      ipv4
        subnet-prefix-length 24
        gateway-ip-address 20.20.20.1
        local-ip-address 20.20.20.2
          service-address SA-cust1
        probes-source-style specific-source
        activate
      vlan-id 81
      network-security trusted
      probes-type none
```

## Configure Media Address for Sub-customer

Enter the following commands to add media address for sub-customers:

```
sbc
   media
      media-address ipv4 10.10.10.5 service-network 3
        port-range 16384 65535
      media-address ipv4 20.20.20.2 service-network 1
        port-range 16384 65535
      media-address ipv4 20.20.20.2 service-network 2
        port-range 16384 65535
      vmsc global
        activate
```

## Create Account for Enterprise Applications

Enter the following commands to create an account:

```
config
 sbc
  signaling
      burst-rate-limit-period 6 seconds
      account cust1
      account cust2
      account shared
```

## Configure Adjacencies for Sub Customer Instance

*Table 75: Adjacencies for Small Contact Center Deployment*

| SNo | Adjacency Name | Remote Server/Node | Call Flow |
|---|---|---|---|
| 1 | SUBCUST1-CVP | CVP Call Server | • To Route calls to CUCM to connect agent phone<br>• Agent Transfer call<br>• IVR Based OB Call |
| 2 | SUBCUST1-CUBE-E-REFER | CUBE-E | REFER Call flow |
| 3 | SUBCUST1-CUBE-MEDIASENSE-FORK | CUBE-E | CUBE-E to communicate with MediaSense. |
| 4 | SUBCUST1-CUCM-PUB | Customer 1 CUCM Publisher | To route calls to CUCM Publisher for all the callflows |
| 5 | SUBCUST1-CUCM-SUB | Customer 1 CUCM Subscriber | To route calls to CUCM Subscriber for all the callflows |
| 6 | SUBCUST1-MEDIASENSE | MediaSense | MediaSense Callflow |
| 7 | SUBCUST1-CUCM-PUB-CONSULT-TRAN | CUCM Publisher | Consult and transfer call flow |
| 8 | SUBCUST1-CUCM-SUB-CONSULT-TRAN | CUCM Subscriber | Consult and transfer call flow |
| 9 | SUBCUST1-Carrier-Network | Carrier Network | All the calls from cloud to be routed to Customer1 |
| 10 | SUBCUST1-CUCM-PUB-MOBILE-AGENT | CUCM Publisher | Mobile Agents to login |
| 11 | SUBCUST1-CUCM-SUB-MOBILE-AGENT | CUCM Subscriber | Mobile Agents to login |
| 12 | SUBCUST1-LBO-Network | TDM Gateway | LBO Callflows |
| 13 | SUBCUST1-SIP-OUTBOUND-DIALER | Outbound dialer | IVR and Agent based outbound callflow |
| 14 | SUBCUST1-CUBE-E-OUTBOUND-IVR | Dedicated or Shared Outbound gateway | IVR based outbound callflow |
| 15 | SUBCUST1-CUBE-E-OUTBOUND | Shared Outbound gateway | IVR and Agent based callflow |
| 16 | SUBCUST1-CUBE-E-OUTBOUND-AGENT | Shared Outbound gateway | Agent based callflow |
| 17 | SUBCUST1-CUSP | CUSP | To route call to CUCM and CVP for all call flows |

- Configure Adjacencies for Core Components, on page 491
- Configure Adjacencies for Optional Components, on page 496
- Configure Call Policy, on page 488


## Configure Adjacencies for Core Components


- Add CVP Adjacency, on page 491
- Add CUCM-PUBLISHER Adjacency, on page 491
- Add CUCM-SUBSCRIBER Adjacency, on page 492
- Add CUCM PUBLISHER Adjacency for consult and transfer call flow, on page 492
- Add CUCM PUBLISHER Adjacency for consult and transfer call flow, on page 492
- Add CUCM PUBLISHER Adjacency for Mobile agent call flow, on page 493
- Add CUCM SUBSCRIBER Mobile Agent Call flow, on page 493
- Add OUTBOUND-DIALER adjacency, on page 494
- Add CUBE-E-OUTBOUND -IVR, on page 494
- Add CUBE-E OUTBOUND adjacency, on page 495
- Add CUBE-E-OUTBOUND-AGENT adjacency, on page 495


### *Add CVP Adjacency*

In this example, the adjacency is created for one of the sub-customer, that is for SUBCUST1-CVP. This needs to be configured for each CVP and for each sub-customer.

```
config
 sbc
  signaling
   adjacency sip SUBCUST1-CVP
        description "Trunk to CVP for SUBCUSTOMER 1"
        account cust1
        interop
          preferred-transport tcp
          message-manipulation
            edit-profiles inbound he-dtmf
        force-signaling-peer all-requests
        adjacency-type preset-core
        remote-address-range ipv4 10.10.10.10 prefix-len 32
        service-address SA-shared
          # service-network 10
          # signaling-local-address ipv4 10.10.10.5
        signaling-local-port 5082
        signaling-peer 10.10.10.10
        signaling-peer-port 5060
        statistics-setting summary
        activate
```

### *Add CUCM-PUBLISHER Adjacency*

In this example, the adjacency is created for one of the sub-customer, that is for SUBCUST1-CUCM-PUB. This is required to route calls to CUCM publisher for all the call flows.

```
config
 sbc
  signaling
```

```
   adjacency sip SUBCUST1-CUCM-PUB
        description "Trunk to SUBCUSTOMER 1 CUCM-PUBLISHER"
        account cust1
        interop
          preferred-transport tcp
          message-manipulation
            edit-profiles inbound he-dtmf
        force-signaling-peer all-requests
        adjacency-type preset-core
        remote-address-range ipv4 20.20.20.30 prefix-len 32
        service-address SA-cust1
          # service-network 1
          # signaling-local-address ipv4 20.20.20.2
        signaling-local-port 5083
        signaling-peer 20.20.20.30
        signaling-peer-port 5060
        statistics-setting summary
       activate
```

### *Add CUCM-SUBSCRIBER Adjacency*

In this example, the adjacency is created for one of the sub-customer, that is for SUBCUST1-CUCM-SUB. This is required to route calls to CUCM subscriber for all the call flows.

```
config
 sbc
  signaling
   adjacency sip SUBCUST1-CUCM-SUB
        description " Trunk to SUBCUSTOMER 1 CUCM Subsciber"
        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 5083
        signaling-peer 20.20.20.130
        signaling-peer-port 5060
        statistics-setting summary
       activate
```

### *Add CUCM PUBLISHER Adjacency for consult and transfer call flow*

In this example, the adjacency is created for one of the sub-customer, that is SUBCUST1-CUCM-PUB-CONSULT-TRAN. To consult and transfer call flow.

```
config
 sbc
  signaling
   adjacency sip SUBCUST1-CUCM-PUB-CONSULT-TRAN
        description "Trunk SUBCUSTOMER 1 CUCM Publisher for cons and trans call flow"
        account cust1
        interop
          preferred-transport tcp
          message-manipulation
            edit-profiles inbound he-dtmf
        force-signaling-peer all-requests
        adjacency-type preset-core
        remote-address-range ipv4 20.20.20.30 prefix-len 32
        service-address SA-cust1
          # service-network 1
          # signaling-local-address ipv4 20.20.20.2
        signaling-local-port 5090
        signaling-peer 20.20.20.30
        signaling-peer-port 5060
        statistics-setting summary
        activate
```

### *Add CUCM SUBSCRIBER Adjacency for consult and transfer call flow*

In this example, the adjacency is created for one of the sub-customer, that is SUBCUST1-CUCM-SUB-CONSULT-TRAN. To consult and transfer call flow.

```
config
 sbc
  signaling
   adjacency sip SUBCUST1-CUCM-SUB-CONSULT-TRAN
        description "Trunk SUBCUSTOMER 1 CUCM subsc for cons and transr 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 5090
        signaling-peer 20.20.20.130
        signaling-peer-port 5060
        statistics-setting summary
        activate
```

### *Add CUCM PUBLISHER Adjacency for Mobile agent call flow*

In this example, the adjacency is created for one of the sub-customer, that is SUBCUST1-CUCM-PUB-MOBILE-AGENT. For mobile agent login.

```
config
 sbc
  signaling
   adjacency sip SUBCUST1-CUCM-PUB-MOBILE-AGENT
        description "Trunk SUBCUSTOMER 1 CUCM Publisher 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
        remote-address-range ipv4 20.20.20.30 prefix-len 32
        service-address SA-cust1
          # service-network 1
          # signaling-local-address ipv4 20.20.20.2
        signaling-local-port 5078
        signaling-peer 20.20.20.30
        signaling-peer-port 5060
        statistics-setting summary
        activate
```

### *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
```

### *Add OUTBOUND-DIALER adjacency*

In this example, the adjacency is created for one of the sub-customer.

```
config
 system
  adjacency sip SUBCUST1-SIP-OUTBOUND-DIALER
        description "Trunk SUBCUSTOMER 1 SIB OUT BOUND DIALER"
        account cust1
        call-media-policy
          codec-list codec-list-1
          media-address-type both
        interop
          100rel inbound support
          100rel outbound require-add
          preferred-transport none
          message-manipulation
            edit-profiles inbound he-dtmf
        adjacency-type preset-core
        nat autodetect
        remote-address-range ipv4 20.20.20.21 prefix-len 32
        service-address SA-cust1
          # service-network 1
          # signaling-local-address ipv4 20.20.20.2
        signaling-local-port 5087
        signaling-peer 20.20.20.21
        signaling-peer-port 5060
        statistics-setting summary
        default-interop-profile GenericAccess
        activate
```

### *Add CUBE-E-OUTBOUND -IVR*

In this example, the adjacency is created for one of the sub-customer

**Note** CUBE (E) adjacency is required in IVR based outbound call flow for dedicated outbound gateway scenario. This adjacency is used to transfer the call to Unified CVP from outbound gateway for IVR based outbound call flow.

```
cofig
 system
  adjacency sip SUBCUST1-CUBE-E-OUTBOUND-IVR
        description "Trunk to CUBE-E OUT BOUND Gateway for IVR call"
        account cust1
        call-media-policy
          codec-list codec-list-1
          media-address-type both
        interop
          100rel inbound support
          100rel outbound require-add
          preferred-transport none
          message-manipulation
            edit-profiles inbound he-dtmf
        adjacency-type preset-core
        remote-address-range ipv4 10.10.10.180 prefix-len 32
        service-address SA-shared
          # service-network 10
          # signaling-local-address ipv4 10.10.10.5
        signaling-local-port 5091
        signaling-peer 10.10.10.180
```

```
        signaling-peer-port 5060
        statistics-setting summary
        default-interop-profile GenericAccess
        activate
```

### *Add CUBE-E OUTBOUND adjacency*

In this example, the adjacency is created for one of the sub-customer.

**Note** CUBE (E) adjacency is required in agent based outbound call flow that includes shared outbound gateway.

```
config
 system
  adjacency sip SUBCUST1-CUBE-E-OUTBOUND
        description "Trunk to CUBE-E OUT BOUND Gateway for SUB CUSTOMER 1"
        account cust1
        call-media-policy
          codec-list codec-list-1
          media-address-type both
        interop
          100rel inbound support
          100rel outbound require-add
          preferred-transport none
          message-manipulation
            edit-profiles inbound he-dtmf
        adjacency-type preset-core
        remote-address-range ipv4 10.10.10.180 prefix-len 32
        service-address SA-shared
          # service-network 10
          # signaling-local-address ipv4 10.10.10.5
        signaling-local-port 5087
        signaling-peer 10.10.10.180
        signaling-peer-port 5060
        statistics-setting summary
        default-interop-profile GenericAccess
        activate
```

### *Add CUBE-E-OUTBOUND-AGENT adjacency*

In this example, the adjacency is created for one of the sub-customer.

Optional, this is required only if customer chooses to use shared outbound gateway. This adjacency is used to transfer the call to the agent.

```
config
 system
  adjacency sip SUBCUST1-CUBE-E-OUTBOUND-AGENT
        description "Trunk to CUBE-E OUT BOUND Gateway for Agent based call"
        account cust1
        call-media-policy
          codec-list codec-list-1
          media-address-type both
        interop
          100rel inbound support
          100rel outbound require-add
          preferred-transport none
          message-manipulation
            edit-profiles inbound he-dtmf
        adjacency-type preset-core
        remote-address-range ipv4 10.10.10.180 prefix-len 32
        service-address SA-shared
          # service-network 10
          # signaling-local-address ipv4 10.10.10.5
        signaling-local-port 5088
        signaling-peer 10.10.10.180
        signaling-peer-port 5060
        statistics-setting summary
        default-interop-profile GenericAccess
        activate
```

## Configure Adjacencies for Optional Components


- Add CUBE-MEDIASENSE FORK adjacency, on page 496
- Add MEDIASENSE adjacency , on page 496
- Add CUSP Adjacency, on page 497


### *Add CUBE-MEDIASENSE FORK adjacency*

In this example, the adjacency is created for one of the sub-customer SUBCUST1-CUBE-E-MEDIASENSE-FORK.

```
Config
 sbc
  signalling
   adjacency sip SUBCUST1-CUBE-E-MEDIASENSE-FORK
        description "Trunk to CUBE-E Gateway for SUB CUSTOMER 1 MEDIASENSE"
        account cust1
        call-media-policy
          hold-setting hold-sendonly
        interop
          preferred-transport tcp
          message-manipulation
            edit-profiles inbound he-dtmf
        force-signaling-peer all-requests
        adjacency-type preset-core
        remote-address-range ipv4 10.10.10.180 prefix-len 32
        service-address SA-shared
          # service-network 10
          # signaling-local-address ipv4 10.10.10.5
        signaling-local-port 5086
        signaling-peer 10.10.10.180
        signaling-peer-port 5060
        statistics-setting summary
        activate
```

### *Add MEDIASENSE adjacency*

In this example, the adjacency is created for one of the sub-customer SUBCUST1-MEDIASENSE, this is required for mediasense call flows.

```
Config
 sbc
  signalling
   adjacency sip SUBCUST1-MEDIASENSE
        description "Trunk to SUBCUSTOMER 1 MediaSense"
        account cust1
        call-media-policy
          hold-setting hold-sendonly
        interop
          preferred-transport tcp
          message-manipulation
            edit-profiles inbound he-dtmf
        force-signaling-peer all-requests
        adjacency-type preset-core
        remote-address-range ipv4 20.20.20.70 prefix-len 32
        service-address SA-cust1
          # service-network 1
          # signaling-local-address ipv4 20.20.20.2
        signaling-local-port 5086
        signaling-peer 20.20.20.70
        signaling-peer-port 5060
        statistics-setting summary
        activate
```

### *Add CUSP Adjacency*

In this example, the adjacency is created for one of the sub-customer SUBCUST1-CUSP.

```
config
  sbc
   signaling
    adjacency sip SUBCUST1-CUSP
    description "Trunk to CUSP For SUBCUST1-CUSP"
    account cust1
    call-media-policy
    codec-list codec2
    interop
    100rel outbound support-add
    dtmf disable sip notify
    dtmf disable sip info
    media-late-to-early-iw outgoing
    preferred-transport udp
    adjacency-type preset-peering
    remote-address-range ipv4 10.10.10.50 prefix-len 32
    service-address SA-shared
    # service-network 10
    # signaling-local-address ipv4 10.10.10.5
    signaling-local-port 5069
    signaling-peer 10.10.10.5
    signaling-peer-port 5060
    statistics-setting summary
    activate
```

## Configure Call Policy

Here some of the basic calls are covered as part of this call policy.

```
call-policy-set 1
        description first-callpolicy
        first-call-routing-table AdminDomains
        rtg-round-robin-table CUCM-ROUND-ROBIN-SUBCUST1
          entry 1
            dst-adjacency SUBCUST1-CUCM-PUB
            action complete
          entry 2
            dst-adjacency SUBCUST1-CUCM-SUB
            action complete
        rtg-round-robin-table CVP-TO-CUCM-R-ROBIN-SUBCUST1
          entry 1
            dst-adjacency SUBCUST1-CUCM-PUB-CONSULT-TRAN
            action complete
          entry 2
            dst-adjacency SUBCUST1-CUCM-SUB-CONSULT-TRAN
            action complete
        rtg-src-adjacency-table AdminDomains
          entry 1
            match-adjacency SUBCUST1-Carrier-Network
            dst-adjacency SUBCUST1-CUBE-E
            action complete
          entry 2
            match-adjacency SUBCUST1-CVP
            action next-table CUCM-ROUND-ROBIN-SUBCUST1
          entry 3
            match-adjacency SUBCUST1-CUCM-PUB-CONSULT-TRAN
            dst-adjacency SUBCUST1-CVP
            action complete
          entry 3
            match-adjacency SUBCUST1-CUBE-E-MEDIASENSE-FORK
            dst-adjacency SUBCUST1-MEDIASENSE
            action complete
          entry 4
           match-adjacency SUBCUST1-CUSP
           action next-table CUCM-ROUND-ROBIN-SUBCUST1
          entry 5
           match-adjacency SUBCUST1-CUCM-PUB-CONSULT-TRAN
```

```
        dst-adjacency SUBCUST1-CUSP
        action complete
       entry 6
        match-adjacency SUBCUST1-SIP-OUTBOUND-DIALER
        dst-adjacency SUBCUST1-CUBE-E-OUTBOUND
        action complete
       entry 7
        match-adjacency SUBCUST1-CUBE-E-OUTBOUND-IVR
        action next-table CVP-TO-CUCM-R-ROBIN-SUBCUST1
       entry 8
        match-adjacency SUBCUST1-CUBE-E-OUTBOUND-AGENT
        action next-table CUCM-ROUND-ROBIN-SUBCUST1
     complete
   active-call-policy-set 1
   qos sig default
     dscp 24
     marking dscp
   qos video default
     dscp 46
     marking dscp
   qos voice default
     dscp 46
     marking dscp
activate
```

# 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 appropriate 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 the PCA 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, Finesse, 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, VRU Peripheral Gateway, and choose **Finesse** for Finesse.
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.

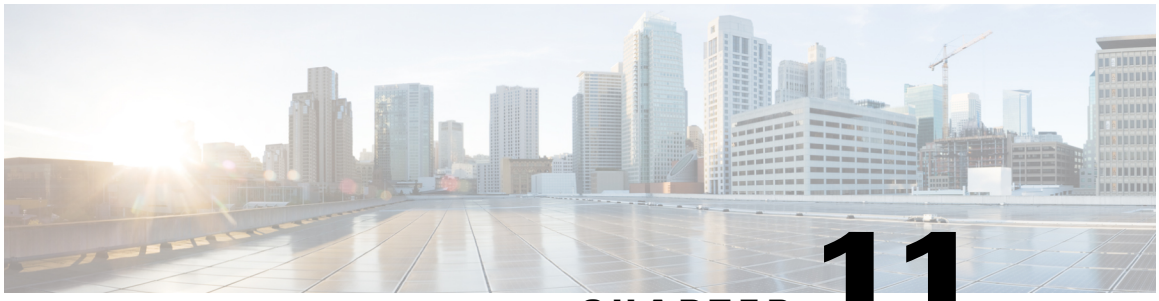
For CVP, CVP OAMP, CVP RSA use User ID as wsmadmin and password configured for OAMP web UI

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, Finesse, VRU Peripheral Gateway, CVP, CVP OAMP, and CVP RSA. Media sense and CUIC is not supported. CUCM will be pushed from CUCDM to HCM-F.



CHAPTER 11

# Administration



# Unified CCE Administration



## Provision Unified CCE Using Unified CCDM

Complete the following procedures to provision the Unified CCE using Unified Contact Center Domain Manager (Unified CCDM).

- Configure Enterprise Skill Group, on page 523
- Configure Expanded Call Variable, on page 524
- Configure Folder, on page 525
- Configure Group, on page 527
- Configure Label, on page 529
- Configure Person, on page 530
- Configure Supervisors , on page 532
- Configure Service, on page 533
- Configure Skill Group, on page 534
- Configure Route , on page 536
- Agent Re-skilling and Agent Team Manager, on page 536
- Configure User Variable, on page 539
- View the Unified CCDM Version, on page 540
- Bulk Operations Using Unified CCDM, on page 540
- Manage Roles , on page 555
- Configure Gadgets, on page 562

## 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 540.

You cannot edit any default resources in CCDM portal.

| Object | Create | Read | Update | Delete | Bulk Upload |
|---|---|---|---|---|---|
| Bucket Interval, see Configure Call Type, on page 513. | | x | | | |
| ECC Variables, see Configure Expanded Call Variable, on page 524. | x | x | x | x | |
| Network VRU Script, see Configure Network VRU Scripts, on page 519. | x | x | x | x | x |
| Call Type, see Create a Call Type, on page 513. | x | x | x | x | x |

| Object | Create | Read | Update | Delete | Bulk Upload |
|---|---|---|---|---|---|
| Dialed Number, see Configure Dialed Number, on page 521. | x | x | x | x | x |
| Skill Group, see Configure Skill Group, on page 534. | x | x | x | x | x |
| Folder, see Configure Folder, on page 525. | x | x | x | x | x |
| Group, see Configure Group, on page 527. | x | x | x | x | |
| Agent, see Configure Agents, on page 508. | x | x | x | x | x |
| Agent Desktop, see Configure Agent Desktop, on page 510. | x | x | x | x | x |
| Agent Team, see Configure Agent Team, on page 512. | x | x | x | x | x |
| Person, see Configure Person, on page 530. | x | x | x | x | x |
| User, see Configure User, on page 504. | x | x | x | x | x |
| User Variable, see Configure User Variable, on page 539. | x | x | x | x | x |
| Enterprise Skill Group, see Configure Enterprise Skill Group, on page 523. | x | x | x | x | x |
| Label, see Configure Label, on page 529. | x | x | x | x | x |
| Attribute, see Configure Precision Attribute, on page 515. | x | x | x | x | x |
| Precision Queue, see Configure Precision Queue, on page 517. | x | x | x | x | x |
| Service, see Configure Service, on page 533 | x | x | x | x | |

# Configure User

Complete the following procedures to configure a user:

- Create User, on page 504
- Assign Roles to Users, on page 505
- Assign Permission to Sub-customer Tenant and User, on page 506
- Edit User, on page 506
- Delete User, on page 506

## Create User

**Note** Login as administrator to create tenant/sub customer user.

### Before You Begin

Create users in active directory domain, see Create Users in Active Directory, on page 463.

### 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**.

**Note** For ISE users or SSO is enabled, login name must be in Username@domain.com format where Username is the name of active directory user and domain.com is the active directory domain.

**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**.

**Note** If SSO is enabled, credential option will be disabled.

## Configure an Imported Unified CCE User

After integration of CCE with Unified CCDM, Unified CCDM import existing 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 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

**Step 1** In Unified CCDM portal, click burger icon in the top-left corner and select **Security** > **Users**.

**Step 2** From the folder tree, select the folder containing the user that you want to edit.

**Step 3** Select the user you want to edit.

**Step 4** Click **Details** tab.

**Step 5** Edit the required details.

**Step 6** Click **Groups** tab, to add or remove the groups.

**Step 7** Click **Save**.

## Delete User

Follow the below procedures to delete users:

### Procedure

**Step 1** In Unified CCDM portal, click burger icon in the top-left corner and select **Security** > **Users**.
**Step 2** From folder tree on left, select the folder containing the user that you want to delete.
**Step 3** Select the user that you want to delete.
**Step 4** Click **Delete** and click **Yes**.

## Configure Departments

To configure a department perform the following instructions.

- Create a Department, on page 507
- Edit a Department, on page 507
- Move a Department, on page 508
- Delete a Department, on page 508

### Create 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** Select the required Folder from the Tenant. Click **Resource** and select **Department**.
**Step 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 508
- Edit an Agent, on page 509
- Delete an Agent, on page 510

### 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.

**Step 5** Click **Supervisor** tab and configure the following:

a) If the agent is a supervisor, check the **Supervisor** check box.
The agent must be associated with a Domain Account (the account they use to log in to a computer on the contact center network).
b) Type in part of the account name, click **Find** and then select the correct account.
**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.

**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) show 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 510
- Edit an Agent Desktop, on page 511
- Delete an Agent Desktop, on page 511

## 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 512
- Edit an Agent Team, on page 512
- Delete an Agent Team, on page 513

## 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, on page 513
- Edit a Call Type, on page 514
- Delete a Call Type, on page 514


### 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 515
- Assign Precision Attribute to an Agent, on page 516
- Configure Precision Queue, on page 517
- Create Routing Scripts, on page 519

## Configure Precision Attribute

Complete the following procedures to configure precision attribute.

- Create Precision Attribute, on page 515
- Edit Precision Attribute, on page 515
- Delete Precision Attribute, on page 516

### *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 517
- Edit Precision Queue, on page 517
- Delete Precision Queue, on page 518

### *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.

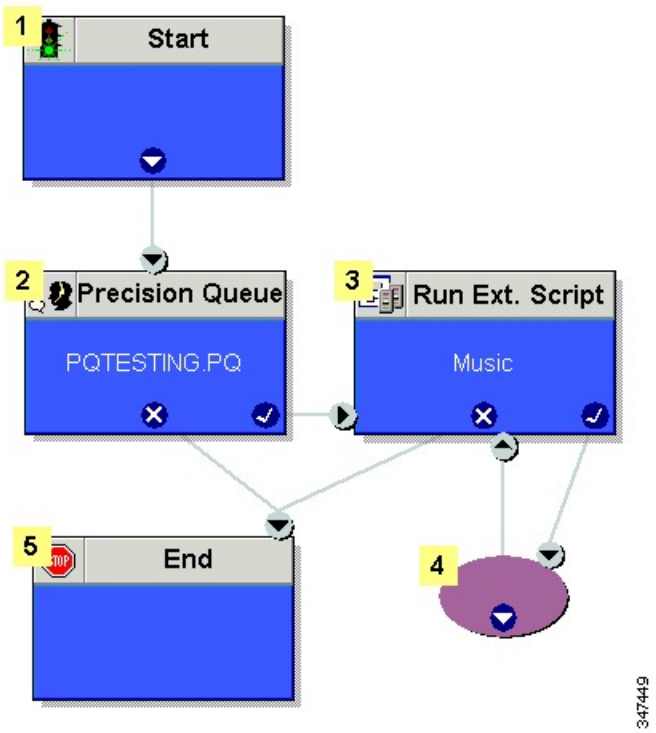
**Step 5** Click **Delete**.

**Step 6** Click **Yes**.

### Create Routing Scripts

See the following illustration to create routing scripts:

*Figure 69: Create Routing scripts*




## Configure Network VRU Scripts

- Create Network VRU Script, on page 519
- Edit Network VRU Scripts, on page 520
- Delete Network VRU Scripts, on page 521

### 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 521
- Edit a Dialed Number, on page 522
- Delete a Dialed Number, on page 522

### 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:**

*7xx*

**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 523
- Edit an Enterprise Skill Group Configuration, on page 523
- Delete an Enterprise Skill Group, on page 523


## 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 524
- Edit an Expanded Call Variable, on page 525
- Delete an Expanded Call Variable, on page 525

### 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 Folder

Complete the following procedures for folder configuration:

- Create Folders, on page 525
- Rename a Folder, on page 526
- Move Folder, on page 526
- Delete Folder, on page 526

### 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 527
- Edit a Group, on page 528
- Move a Group, on page 528
- Delete a Group, on page 528

### 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 529
- Edit a Label, on page 529
- Delete a Label, on page 530

### 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 530
- Edit a Person, on page 531
- Delete a Person, on page 531

### 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 508.

**Step 3** Select **Supervisor** tab and enable Supervisor.

**Step 4** Optional, enable **Associate with Domain Account** as follows:

a) Check **Associate with Domain Account** check-box.

b) Enter Domain\Supervisor(Login) and click **Find**, ensure the login name is already created in the domain controller if not the logon name will not be listed.

**Note** In Precision routing enabling the Associate domain is mandatory for assigning the attribute to a supervisor.

**Step 5** Click **Save**.

# Configure Service

**Note** Complete the following procedures to configure service:

- Create Service, on page 533
- Edit Service, on page 533
- Delete Service, on page 534

## 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 534
- Edit a Skill Group, on page 534
- Delete a Skill Group, on page 535

### Create a Skill Group

Complete the following procedure to create 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** 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 504 and to assign supervisor role, see Assign Roles to Users, on page 505.

### 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 **Skillgroup** 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 **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 539
- Edit a User Variable, on page 539
- Delete a User Variable, on page 540

### 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 in the About This Installation Page.

## 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 native 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.<br>**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. |

| Column Name | Data Type | Required? | Description |
|---|---|---|---|
| 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.<br>**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.<br>**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. |

| Column Name | Data Type | Required? | Description |
|---|---|---|---|
| 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. |
| 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(;).<br>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.<br>**0**: Required<br>**1**: Optional<br>**2**: Not allowed<br>**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.<br>**0**: Required<br>**1**: Optional<br>**2**: Not allowed<br>**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.<br>Default value will be 7200. |
| RemoteAgentType | Numeric | No | Indicates how mobile agents are handled.<br>**0** : No remote access<br>**1** : Use call by call routing<br>**2** : Use nailed connection<br>**3** : Agent chooses routing at login<br>**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. |

| Column Name | Data Type | Required? | Description |
|---|---|---|---|
| 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. |
| 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:<br>0 = Use Default<br>1 = Ignore Abandoned Calls<br>2 = Abandoned Call Has Negative Impact<br>3 = Abandoned Call Has Positive Impact |

| | | | |
|---|---|---|---|
| DefaultEntry | Numeric | No | Normal 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 (;).<br>**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:<br>**1:** Service<br>**2:** Skill Group<br>**7:** Call Type<br>**8:** Enterprise Service<br>**9:** Enterprise Skill Group<br>**11:** Dialed Number<br>**14:** Peripheral<br>**16:** Trunk Group<br>**17:** Route<br>**20:** Master Script<br>**21:** Script Table<br>**29:** Application Gateway<br>**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:<br>• 0: Normal<br>• 1: DNIS Overide<br>• 2: Busy<br>• 3: Ring<br>• 4: Post-Query<br>• 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 |

| Column Name | Data Type | Required? | Description |
|---|---|---|---|
| AdvancedMode | Boolean | No | Determines if the user is advanced or not |
| FirstName | SNC | No | The first name of the user |
| 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:<br>• The login name must correspond to an existing Windows active directory use<br>• 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:<br>3: Boolean (true or false only)<br>4: Proficiency (a numeric range) |

| Column Name | Data Type | Required? | Description |
|---|---|---|---|
| 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. |
| 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 554 |
| AgentOrdering | Numeric | Yes | If more than one agent satisfies the precision queue criteria agents are chosen in the following order to handle the call:<br>1: Agent that has been available the longest.<br>2: Most skilled agent.<br>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. |

| Column Name | Data Type | Required? | Description |
|---|---|---|---|
| ServiceLevelType | Numeric | No | Abandoned calls in service level calculations, calls are handled in the following order:<br>1: Ignore abandoned calls.<br>2: Abandoned calls have negative impact (that is, exceed the service level threshold).<br>3: Abandoned calls have positive impact (that is, meet the service level threshold). |
| 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 |
| 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. | | |

| Global Task Name | Comments | Basic | Advanced |
|---|---|---|---|
| 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 |
| 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 |

| Global Task Name | Comments | Basic | Advanced |
|---|---|---|---|
| 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 563
- Edit Gadget, on page 563
- Delete Gadget, on page 563

## 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 Contact Center Enterprise using Administration Workstation.

**Note**

- The base configuration that you upload using the ICMdba tool will automatically provision other required elements of 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 , on page 564

## 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.

# Unified CVP Administration

• Provisioning Unified CVP Using Unified CCDM, on page 565

## Provisioning Unified CVP Using Unified CCDM

• Uploading the Media File, on page 566
• Uploading the IVR Script, on page 566

### 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 Phones, on page 581
- Configure Regions, on page 583
- Configure Class of Service, on page 585
- Configure Cisco Unified CM Group, on page 578
- Configure Device Pool, on page 578
- Associate Phone to Application User, on page 586
- Disassociate Unified Communication Manager from UCDM, on page 587
- Built-in-Bridge, on page 587
- Bulk Operations Using UCDM, on page 588
- Increase the SW MTP and SW Conference Resources, on page 435

## 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 567

| Object | Create | Read | Update | Delete | Bulk Upload |
|---|---|---|---|---|---|
| Contact Center Servers<br>See, Configure Contact Center Servers, on page 569 | x | x | x | x | x |
| Contact Center Services<br>See, Configure Contact Center Services, on page 570 | x | x | x | x | x |
| SIP Trunks<br>See, Configure SIP Trunks, on page 572 | x | x | x | x | x |

| Object | Create | Read | Update | Delete | Bulk Upload |
|---|---|---|---|---|---|
| Route Group<br>See, Configure Route Groups, on page 573 | x | x | x | x | x |
| Route List<br>See, Configure Route List, on page 575 | x | x | x | x | x |
| Route Patterns<br>See, Configure Route Patterns, on page 577 | x | x | x | x | x |
| Directory Number and Lines<br>See, Configure Directory Number Inventory and Lines, on page 580 | x | x | x | x | x |
| Phones<br>See, Configure Phones, on page 581 | x | x | x | x | x |
| Regions<br>See, Configure Regions, on page 583 | x | x | x | x | x |
| Class of Service<br>See, Configure Class of Service, on page 585 | x | x | x | x | x |
| Device Pools<br>See, Configure Device Pool, on page 578 | 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 569
- Edit Contact Center Servers, on page 570
- Delete Contact Center Servers, on page 570


### *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 571
- Edit Contact Center Services, on page 571
- Delete Contact Center Services, on page 571

### *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 745

### *Edit Contact Center Services*

**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** > **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** 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** > **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 572.

Perform the following instruction to configure route groups.

- Add Route Group, on page 574
- Edit Route Group, on page 574
- Delete Route Group, on page 575

## 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 573.

Perform the following instructions to configure route list:

- Add Route List, on page 575
- Edit Route List, on page 576
- Delete Route List, on page 576

### 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 575.

Perform the following instructions to configure route patterns:

- Add Route Pattern, on page 577
- Edit Route Patterns, on page 577
- Delete Route Pattern, on page 578

## 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 578.

## 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 580
- Edit Lines, on page 581
- Delete Lines, on page 581


### Add Directory Number Inventory

#### Before You Begin

Ensure Site dial plan is created, see Add Site Dial Plan, on page 476.

#### 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 580

Perform the following instructions to configure phones:

- Add Phones, on page 581
- Edit Phones, on page 583
- Delete Phones, on page 583

### Add Phones

Perform the following to add phone for provider, reseller or customer.

- Add Phones as Provider or Reseller, on page 582
- Add Phones as Customer, on page 582

### *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.

**Note** For RSM simphone choose Cisco 7941 sip or above models from 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.

**Note** For RSM simphone choose Cisco 7941 sip or above models from 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 584
- Edit Regions, on page 584

• Delete Regions, on page 585

## 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, on page 585
- Edit Class of Service, on page 586
- Delete Class of Service, on page 586


### 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 581

### 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 588
- Enable or Disable the Built-in-Bridge , on page 588

### 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 588.

#### 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 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 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, Release 10.1(2) Bulk Provisioning Guide*.

## Cisco Unified Communications Domain Manager Administration Tools/Bulkloader


- Export Bulk Load, on page 589
- Bulk Load Sheets, on page 589
- Perform Bulk Upload, on page 590


### *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. Any name can be provided for the workbook and the same filename can be loaded multiple times, although the best practice is 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.

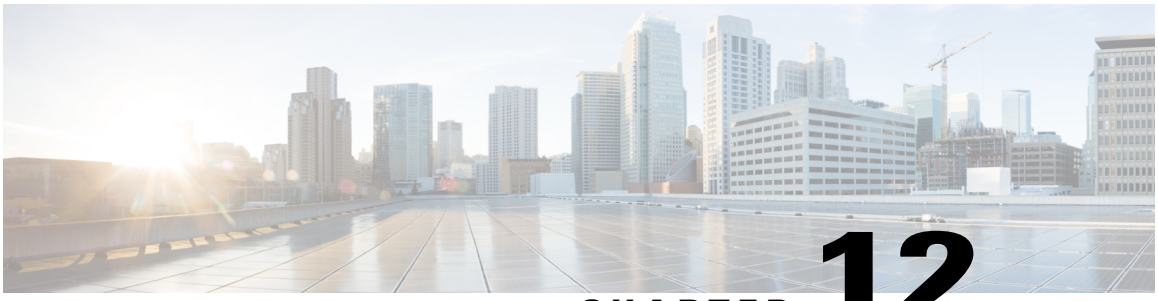
**Step 2** Ensure the hierarchy is set to appropriate level for required UCDM object.

**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**.



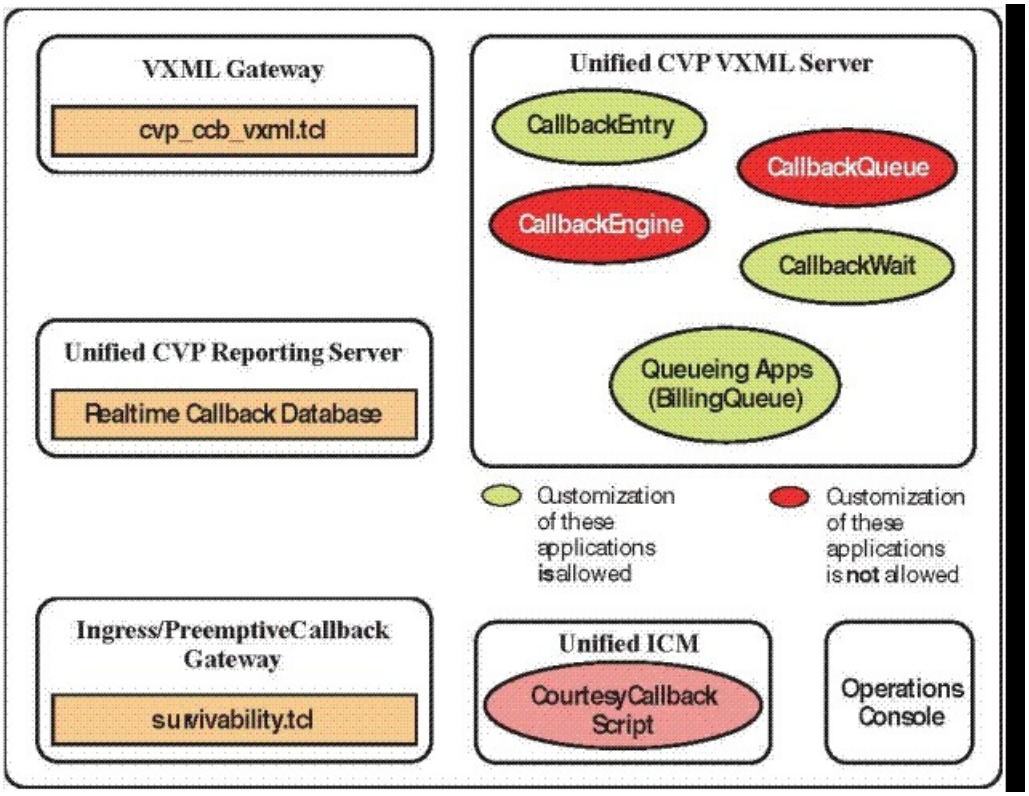
CHAPTER 12

# Configure Core Component Integrated Options

# Configure Courtesy Callback

The following diagram shows the components that you must configure for Courtesy Callback.

***Figure 70: Courtesy Callback components***




Complete the following procedures for Courtesy Callback configurations:

- Configure Gateway, on page 592
- Configure Unified CVP, on page 595
- Configure Unified CCE, on page 600

# 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 ICM, 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.

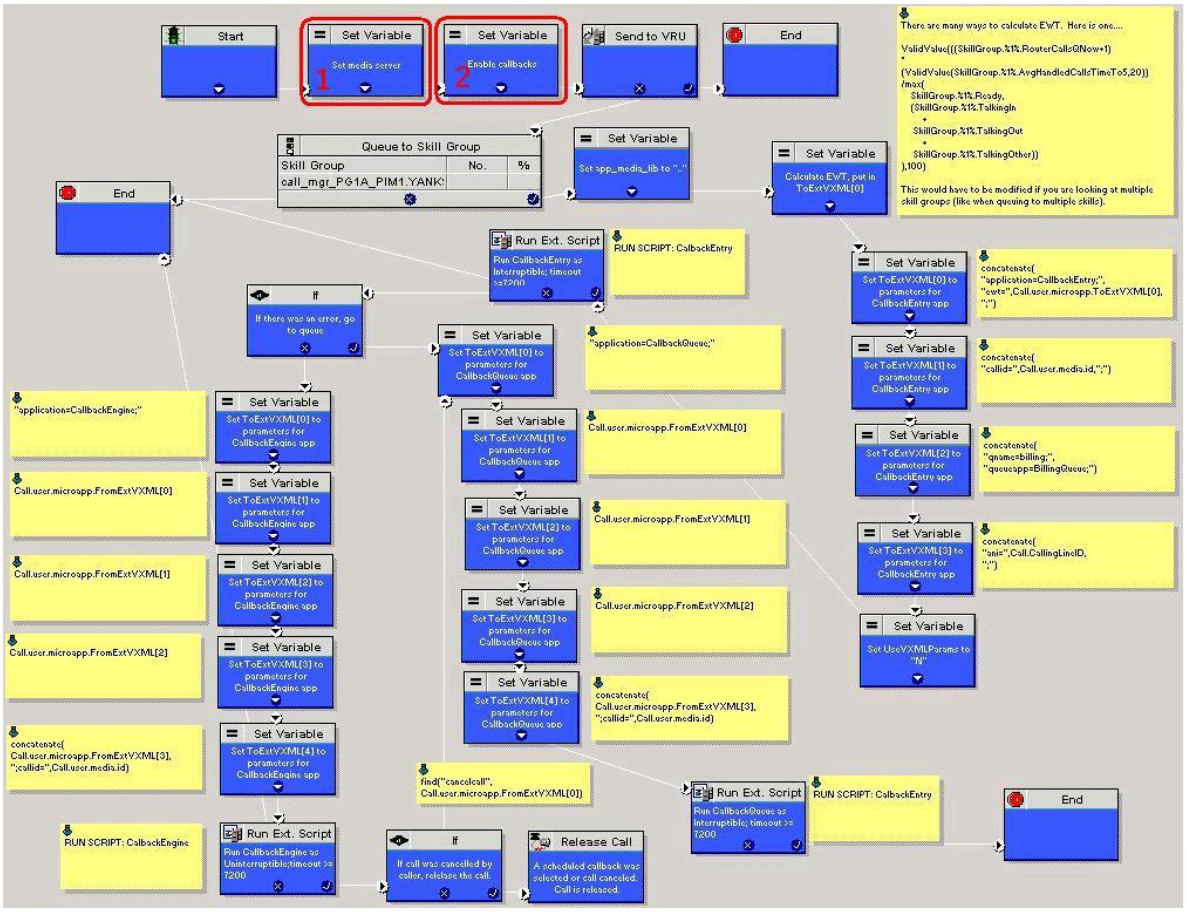
**Step 3** Change the default location of the audio files in the sample scripts to be your media server path.

# Configure Unified CCE

## Configure the ICM Script for Courtesy Callback

Following figure shows the sample Courtesy Callback ICM script.

***Figure 71: 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.

1. Log In to ISE by sub customer user and Click on File>Import Script.
2. 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 71: Sample Courtesy Callback ICM script, on page 600, 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 will be executed:
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 will be executed 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 602
- Configure Unified CVP, on page 603
- Configure Unified CCE, on page 607
- Configure Unified Communications Manager, on page 612

# 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 http://www.cisco.com/en/US/products/sw/custcosw/ps1006/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 603
- Configure the Call Studio Scripts for Record Agent Greeting, on page 605
- Set Content Expiration in IIS (Windows 2012) in Media , on page 606

## 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 hang up 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 http://www.cisco.com/en/US/products/ps7235/tsd_products_support_series_home.html

## 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 2012) in Media

Complete the following procedure to set content expiration in IIS on a Windows 2008 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

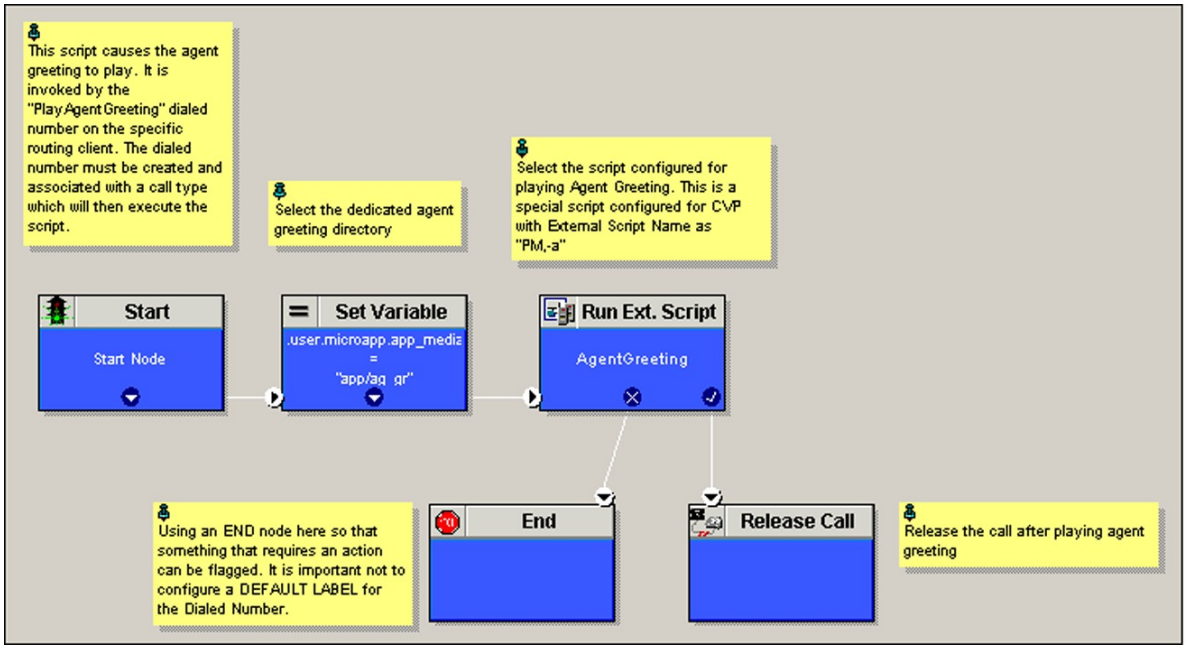
Complete the following procedures for Unified CCE configuration:

- Create Agent Greeting Play Script, on page 608
- Create Agent Greeting Recording Script, on page 608
- Import the Example Agent Greeting Scripts, on page 609

## 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 executes the script.

***Figure 72: Agent Greeting Play Script***

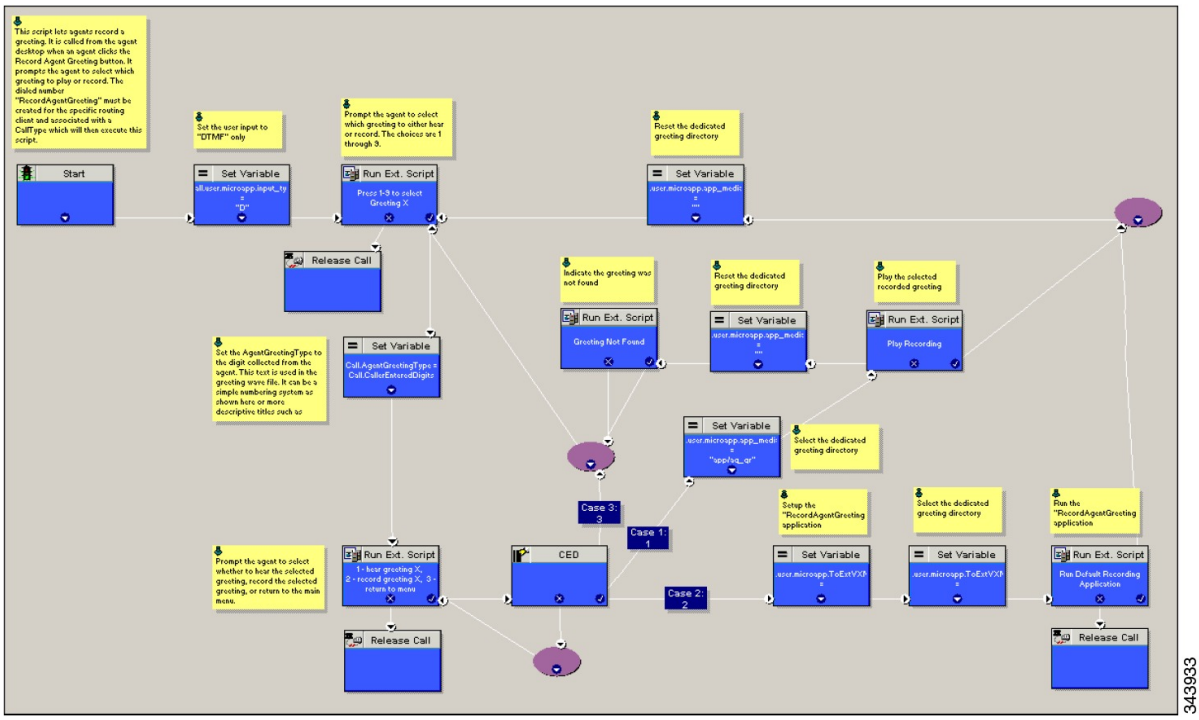



## Create Agent Greeting Recording Script

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 executes this script.

***Figure 73: 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** To enable the ECC variables refer to Configure Expanded Call Variable, on page 524.

# Import the Example Agent Greeting Scripts

To view or use the example Agent Greeting scripts, you must first import them into the Unified CCE Script. 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. To Download the Routing Script, see https://communities.cisco.com/docs/DOC-58859.

**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** Log into **Unified CCDM Portal** and select **System Manager** > **Folder Tree Panel**.

**Step 2** Choose a folder to create the call type.

**Step 3** Select **Resource** > **Call Types**.

**Step 4** Create a call type to record agent greetings and enter **RecordAgentGreeting** as the name.

**Step 5** Create a call type to play agent greetings and enter **PlayAgentGreeting** as the name.

## Configure Dialed Numbers

### Procedure

**Step 1** Log into the Unified CCDM Portal and select **System Manager** > **Folder Tree Panel**.

**Step 2** Select a folder to create the dialed number.

**Step 3** Select **Resource** > **Dialed Number**.

**Step 4** Create a dialed number to record agent greetings and enter **RecordAgentGreeting** as the name.

**Step 5** Create a dialed number to play agent greetings and enter **PlayAgentGreeting** as the name.

**Step 6** Complete the following for each dialed number:

a) Choose **Internal Voice** for 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 will execute.

## 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.

## Deploy Agent Greeting

This chapter 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 362.
**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 602 for Agent Greeting support.
**Step 6** Set the cache size on the VXML Gateway. See Set Cache Size on VXML Gateway, on page 603.
**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 604.
**Step 8** Configure Call Types, on page 610 to record and play agent greetings.
**Step 9** Configure Dialed Numbers, on page 610 to record and play agent greetings.
**Step 10** Schedule the Script, on page 611
**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 609.

**Step 12** Modify the Unified CCE call routing scripts to use Play Agent Greeting script, on page 612.

## 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.
- 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

To enable Built-in Bridge, see Enable or Disable the Built-in-Bridge , on page 588

# Configure Whisper Announcement

Complete the following procedures for Whisper Announcement configuration:


- Configure Gateway, on page 613
- Configure Unified CVP, on page 613
- Configure Unified CCE, on page 614


## 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.

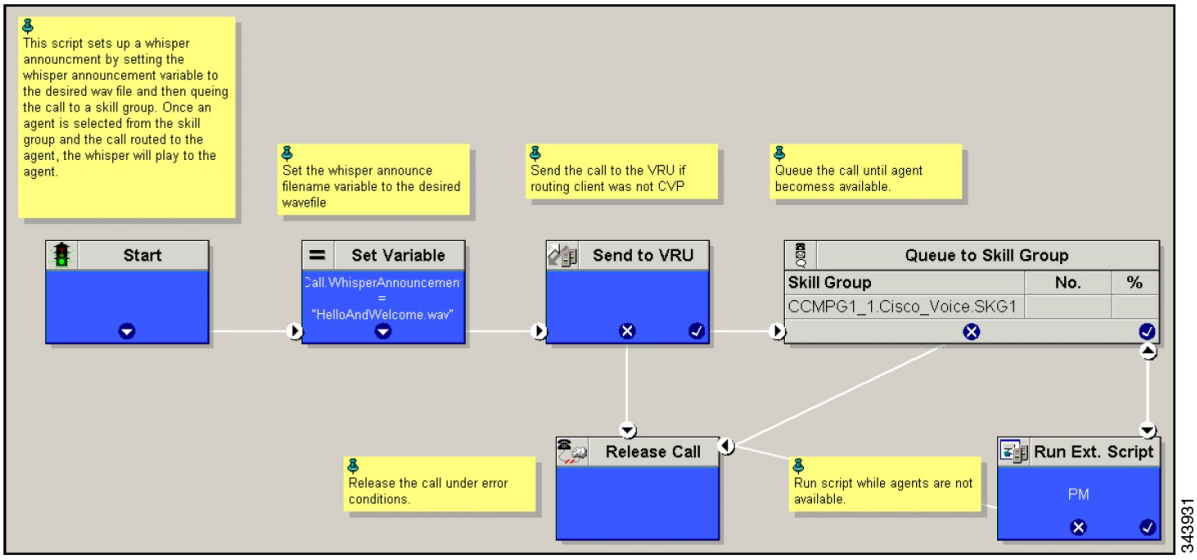
For Whisper Announcement to work, your dial number pattern must cover both of these numbers. The easiest way to ensure coverage is through the use of wild cards such as 9191*. However, if you decide to use an exact dialed number match, then you must specify both 91919191 and 9191919100.

# 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 74: Whisper Announcement Script***




# Configure Database Integration

Complete the following procedures for Database Integration configuration:

- Configure Unified CVP, on page 614
- Configure Unified CCE, on page 617

**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 615
- Add JNDI Context, on page 615
- Configure VXML Studio Script, on page 616
- Create ICM Script, on page 617


## 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}
```

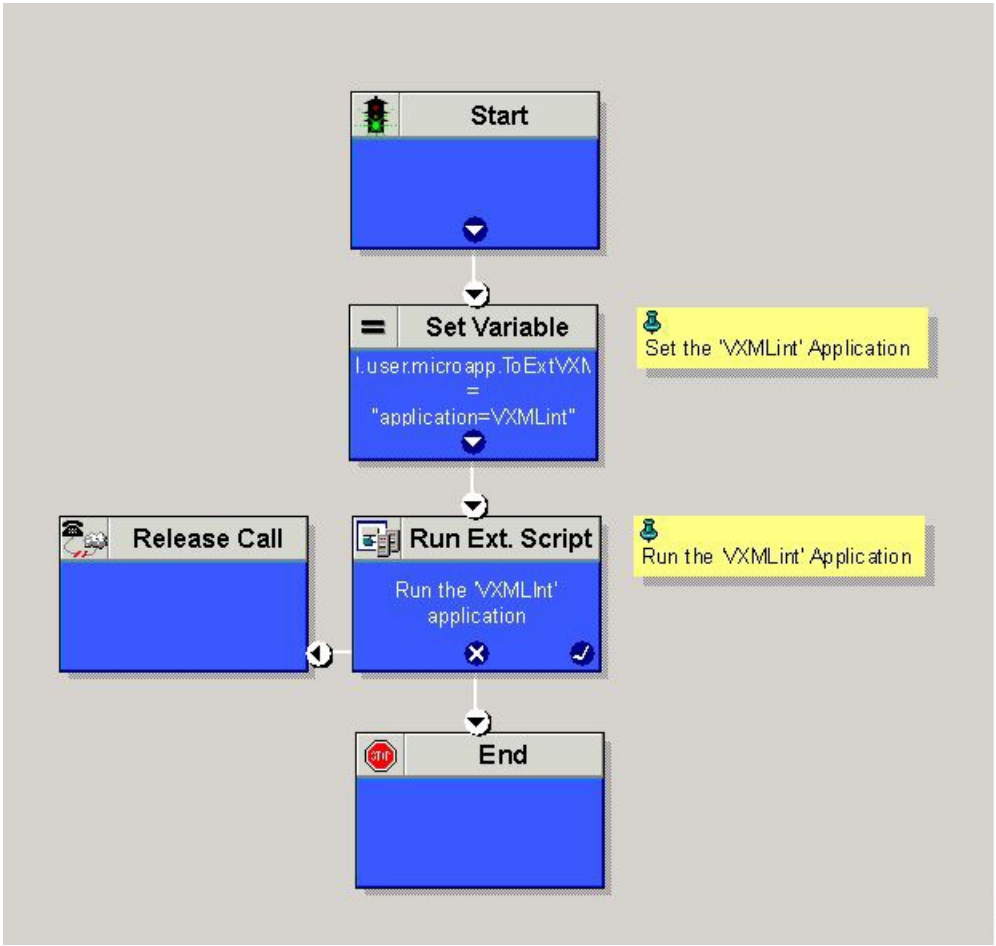
**Step 2** Deploy the script to the local computer or to the remote computer (VXML call server directly) to create CVP Subdialog return element.

**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 75: 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** Configure the following to change the registry settings in Unified CCE:

a) Navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Cisco Systems, Inc. > ICM > <Instance Name> > RouterA > Router > CurrentVersion > Configuration > Database registry**.
**Instance Name** is the name of the Instance that is configured.

b) Set the SQLLogin registry key as shown in the following example:

**Example:**

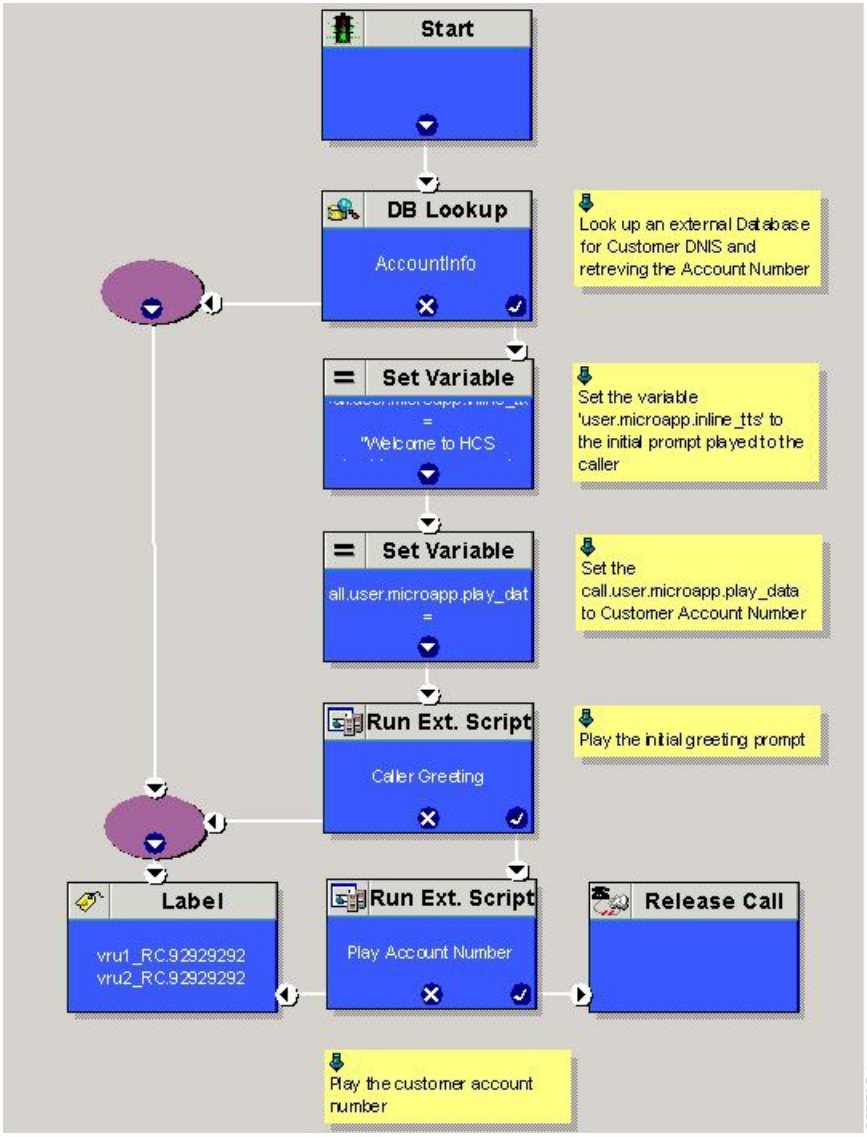
```
\\dblookup1\DBLookup=(sa,sa)
```

Where DBLookup is the external database name and (sa,sa) are the SQL server authentication.

**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 76: Example ICM Database Look Up*




# Configure Unified Mobile Agent


- Configure Unified CCE, on page 620
- Configure Unified Communications Manager, on page 620

# Configure Unified CCE

Complete the following procedure to configure Mobile Agent in Unified CCE:

**Procedure**

**Step 1** Log in to CCDM.

**Step 2** In **System Manager** under the tree panel folder, select a folder where you want to create the agent desktop.

**Step 3** In the Tree panel folder, click **Resource**, and click **Agent Desktop**.

**Step 4** Enter unique name of up to 32 characters for the record.
This name can use alphanumeric characters, periods, and underscores.

**Step 5** Enter the mandatory fields such as **Incoming Work mode**, **Outgoing Work mode**, **Wrap-up time**, and other required fields.

**Step 6** From **Remote Agent Type** drop-down list, select the required routing option.

**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 620
- Tag CTI Ports as Contact Center Agent Lines, on page 623

## Configure CTI Port

Ensure that directory numbers are added. See, Add Directory Number Inventory, on page 580.

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 CUCM clusters.

Complete the following procedure to configure CTI port:

- Configure CTI Port as Provider or Reseller, on page 621
- Configure CTI Port as Customer, on page 622

## 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 620

**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

Complete the following procedure to configure Outbound Dialer:

- Configure Gateway, on page 624
- Configure Unified CVP, on page 626
- Configure Unified CCE, on page 626
- Configure Unified Communications Manager, on page 640

# 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 recommended 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 small contact center agent deployment model if customer opts for shared outbound gateway , session target ip address should point to the Perimeta SBC signaling-address and port configured in the outbound gateway adjacency (SUBCUST1-CUBE-E-OUTBOUND-AGENT). See Configure Adjacencies for Customer Instance, on page 487.
- 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** In small contact center model if customer opts for dedicated outbound gateway , session target ip address should point to the Perimeta SBC signaling-address configured in the outbound gateway adjacency for IVR outbound call flow (SUBCUST1-CUBE-E-OUTBOUND-IVR). See Configure Adjacencies for Customer Instance, on page 487.

**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 all Call Servers.

# Configure Unified CCE



## Add Outbound Database Using ICMDBA Tool

Complete this procedure for Side A only.

**Note**
- For 500 and 1000 agent deployment perform the configurations on Unified CCE Data Server.
- For 4000 and small contact center agent deployment models perform the configurations on Unified CCE Rogger.
- For 12000 agent deployment 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 choose **Create** to create the Outbound database.

**Step 3** In the Create Database dialog box, click **Add** to open the Add Device dialog box. Click **Data**. Choose 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**. Choose 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** and then click **Close.**

## Configure Logger

### Procedure

**Step 1** Launch the Web setup and login.

**Step 2** Edit the Logger component.

**Step 3** Goto **Additional Options** tab.

**Step 4** Check **Enable Outbound Option** check box, in **Outbound Option** panel.

## Configure Outbound Dialer

**Note** The Dialer, MR PG, and MR PIM are pre-configured with the day one configuration database for 500,1000,4000 and 12000 deployment models. Steps 1 to 4 are specific to Small Contact Center only.

### 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, select **Outbound**> **Dialer**.

**Step 3** Click **Retrieve** > **Add** and enter the following details:

- Enter the Dialer name.
- Enter the ICM Pheriperal Name.
- Enter Hangup Delay (1-10) value as **1 Sec**
- Enter Port Throttle value as **10**

**Step 4** Click **Save**.

**Step 5** Click the **Port Map Selection** tab to display the port map configuration.

**Step 6** Click **Add** to configure a set of ports and their associated extensions.

**Step 7** Click **OK**

**Step 8** Click **Save** and **Close**.

**Note** For different sub customers, the port and extension range can be same because separate dialer needs to be created for each sub customer.

## Create Outbound PIM

Perform the following instructions to create outbound PIM:

- Create Outbound PIM for 500 and 1000 Agent Deployment, on page 628
- Create Outbound PIM for 4000 Agent Deployment, on page 628
- Create Outbound PIM for Small Contact Center Deployment , on page 629
- Create Outbound PIM for 12000 Agent Deployment, on page 630

### Create Outbound PIM for 500 and 1000 Agent Deployment

To create Outbound PIM for 500 and 1000 Agent Deployment, see Configure Media Routing Peripheral Gateway, on page 330.

### Create Outbound PIM for 4000 Agent Deployment

- To create Outbound PIM for 4000 Agent Deployment in Agent PG1, See Configure Multichannel and Outbound PIM's 4000 Agent Deployment, on page 415.
- To create Outbound PIM for 4000 Agent Deployment in Agent PG2, See Configure Outbound PIM for 4000 Agent Deployment, on page 418.

## Create Outbound PIM for Small Contact Center Deployment

Complete the following procedure to configure the outbound PIM.

### Procedure

**Step 1** Navigate **Start** > **All programs** > **Cisco Unified CCE Tools**>**Peripheral Gateway Setup** .

**Step 2** Click **Add** in the Instance Components pane, and from the Component Selection dialog box choose **Peripheral Gateway** .

**Step 3** In the Peripheral Gateway Properties dialog box:

a) Check **Production Mode**.
b) Check **Auto start system startup**.
c) Check **Duplexed Peripheral Gateway** .
d) Choose **<PGXXX>** in the PG node Properties ID field.
e) Click the appropriate Side (Side A or Side B).
f) Add **Media Routing** to the selected types, under Client Type pane.
g) Click **Next**.

**Step 4** In the Peripheral Interface Manager pane of the Peripheral Gateway Component Properties dialog box, click **Add** and configure PIM1 with the Client Type of Media Routing as follows

a) Check **Enabled**.
b) Enter *MR1* or a name of your choice, in the peripheral name field.
c) Refer PG explorer and enter the value in the Peripheral ID field.
d) Enter the IP address of Agent PG on Side A, in the Application Hostname(1) field.
e) Retain the default value in the Application Connection port (1).
f) Enter the IP address of Agent PG on Side B in the Application Hostname (2) field.
g) Retain the default value in the Application Connection port (2).
h) Enter *5* in the Heartbeat interval (sec) field.
i) Enter *10* in the Reconnect interval (sec) field and click **OK** .

**Step 5** Refer to PG Explorer and Enter the value in the **Logical Controller ID** field.Leave all other fields with default values and click **Next** .

**Step 6** 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 local** in the Side A Properties panel.
c) Choose **Call Router is local** in the Side B Properties panel.
d) Accept the default value in the Usable Bandwidth (kbps) field.

e) Enter **4** in the Heartbeat Interval (100ms) field. Click **Next** .

**Step 7** In the Peripheral Gateway Network Interface dialog box, enter the PG Private interface and PG Public (visible) interfaces. Click **Next** .

**Step 8** 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.

**Step 9** Click the **QoS** button in the visible interfaces section. In the PG Visible Link QoS Settings, check **Enable QoS** , click **OK** and click **Next**. This step applies only to Side A.

**Step 10** Click **Next** and **Finish**.

**Step 11** Click **Exit Wizard**.

**Note** Do not start Unified ICM/CCNodeManager until all ICMcomponents are installed.

### Create Outbound PIM for 12000 Agent Deployment

To create Outbound PIM for 12000 Agent Deployment, see Configure Media Routing Peripheral Gateway for 12000 Agent Deployment, on page 447.

## Configure SIP Outbound



### Add Import Rule

#### Procedure

**Step 1** Goto **Unified CCE Data Server** or **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 636
- For the import type **Do Not Call**, browse the Do Not Call List file. See, Create Do Not Call List, on page 637

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**.

## Add Query Rule

### Before You Begin

One or more Import rules must be defined. See Add Import Rule, on page 630

### Procedure

**Step 1** Goto **Unified CCE Data Server** or **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.

## Add Campaign


- Add Agent Based Campaign, on page 632
- Add IVR Based Campaign, on page 633


### *Add Agent Based Campaign*

**Procedure**

**Step 1** Goto **Unified CCE Data Server** or **Unified CCE AW-HDS-DDS** machine.

**Step 2** Navigate to **Configuration Manager** > **Outbound Option** > **Camaign** 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**.

*Add IVR Based Campaign*

### Procedure

**Step 1** Goto **Unified CCE Data Server** or **Unified CCE AW-HDS-DDS** machine.

**Step 2** Navigate to **Configuration Manager** > **Outbound Option** > **Camaign** 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:

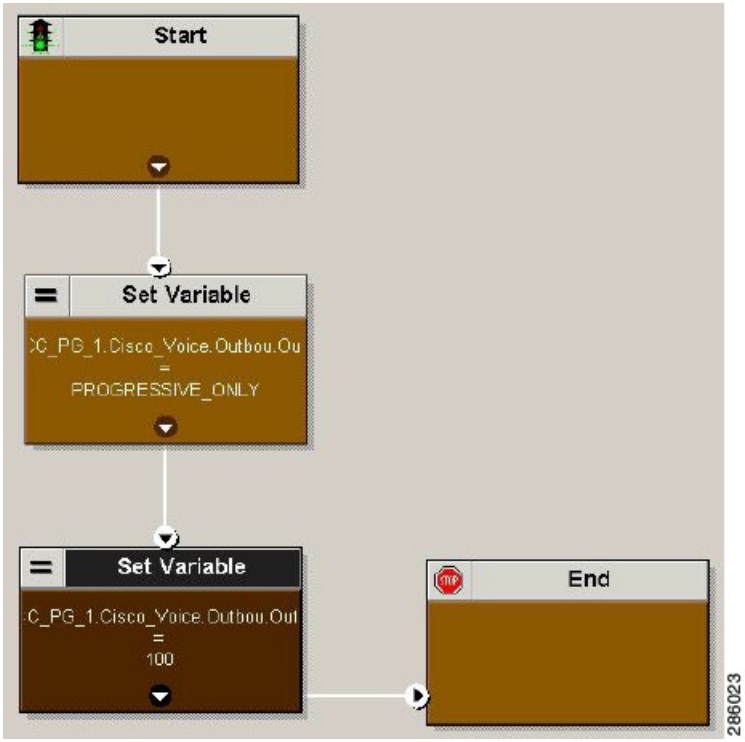
a) Choose appropriate CUCM PG from **Peripheral** drop-down list, click **Retrieve**.
b) Choose **Skill Group** from the drop-down list.
c) Enter **Overflow Agents per Skill** value.
d) Enter **Dialed number**.
e) Enter **Records to cache** value.
f) Enter **Number of IVR Ports**.
g) Click **OK**.

**Step 8** Goto **Call Target** tab, choose **Daylight Savings Zone** from the drop-down list.

**Step 9** Click **Save**.

## Create Admin Script

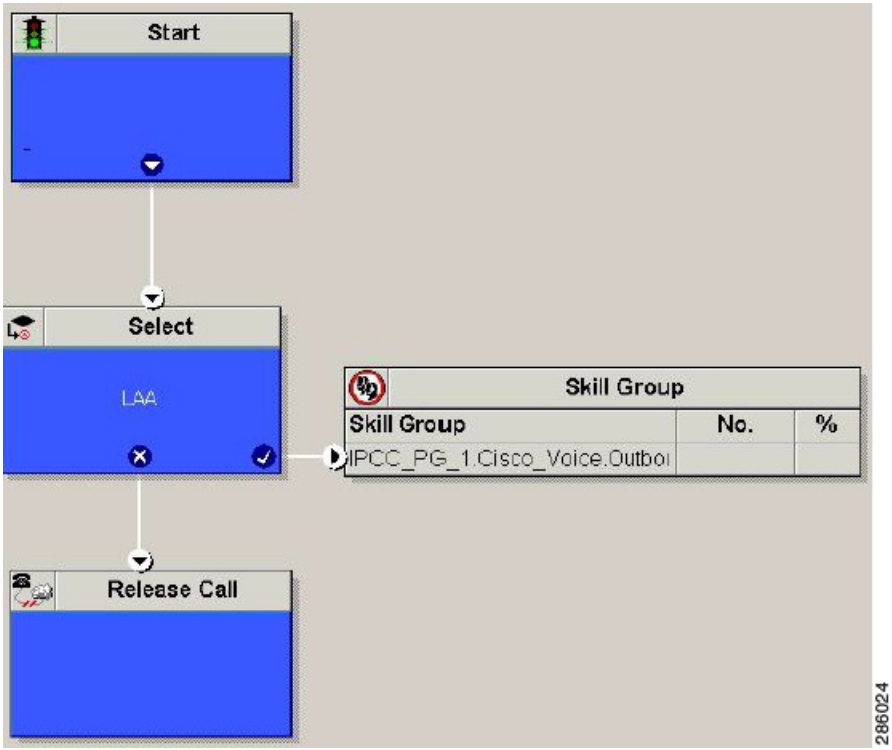
*Figure 77: Create Admin Script*




For more information, see Outbound Option Guide.

## Add Routing Script for Agent Based Campaign

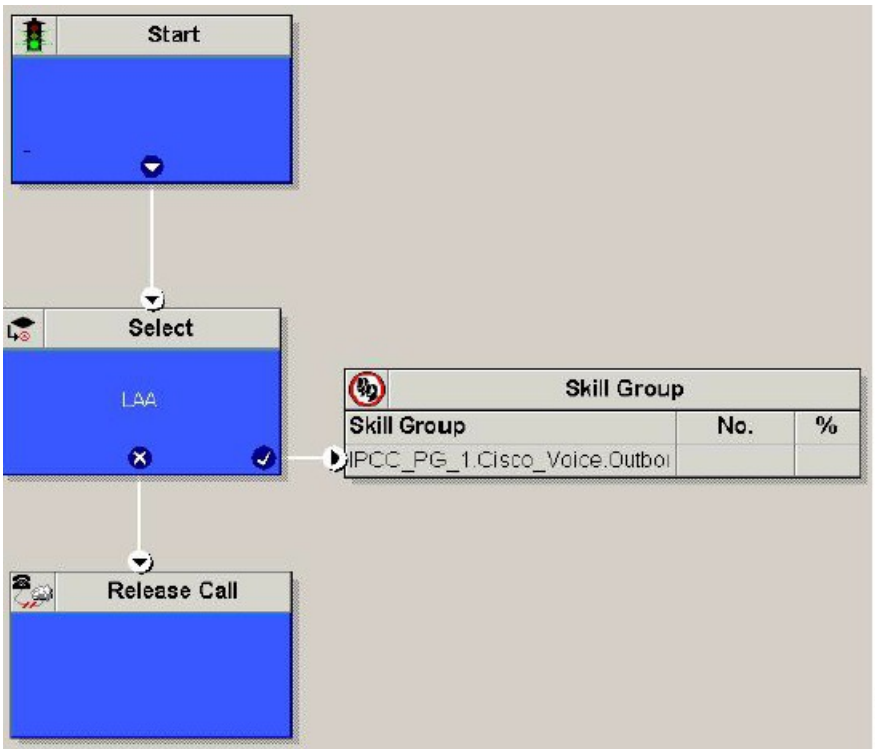
*Figure 78: Add Routing Script for Agent Based Campaign*




For more information, see Outbound Option Guide.

## Add Routing Script for IVR Based Campaign

*Figure 79: 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 IVR Based Campaign, on page 633.

### What to Do Next

- Create Contact Import File, on page 636
- Create Do Not Call List, on page 637

## 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 or Fixed Length, as defined on the Import Rule General Tab Page.

**Step 3** Save the text file to the local server.

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.
- The Do Not Call table can support up to 60 million entries, but note that the information is stored in memory in the Campaign Manager process.
- Each Do Not Call entry uses 16 bytes of memory, so 60 million entries would require approximately 1 gigabyte of memory (960 million bytes) on the Logger Side A platform.

**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 the Do Not Call import files. 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.

When the Campaign Manager starts it automatically imports from the DoNotCall.restore file that is stored in the *<drive>\icm\<instance>\la\bin* directory. When reading Do Not Call import files, the Campaign Manager appends the data to the DoNotCall.restore file. This restore file allows recovery of Do Not Call records after the Campaign Manager stops unexpectedly or for planned maintenance, such as a Service Release installation.

The restore file can grow to approximately 1 GB if 60 million DNC records are imported, each having ten-digit numbers plus five-digit extensions. Sufficient disk space must be available on LoggerA to store the DoNotCall.restore file.

**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

Complete this procedure for both Side A and Side B.

**Note**

- For 500 and 1000 agent deployment perform the configurations on Unified CCE Call Server.
- For 4000 and 12000 agent deployment perform the configurations on Unified CCE Agent PG.

### 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 checked and then click **Next**.

**Step 4** In the SIP Dialer Name field, type the SIP dialer name exactly as it is configured in the Dialer tool under configuration manager.

**Step 5** In SIP Server Type, ensure that **Cisco voice Gateway** is selected.

**Step 6** Provide the Outbound gateway IP in the **SIP Server** field and click **Next**.

**Note** In small contact center agent deployment model if customer opts for shared outbound gateway ,outbound gateway ip address should point to the Perimeta SBC signaling-address and port configured in the sip outbound dialer adjacency (SUBCUST1-SIP-OUTBOUND-DIALER ). See Configure Adjacencies for Sub Customer Instance, on page 490. Otherwise, enter the dedicated outbound gateway ip address and port details.

**Step 7** In the **Campaign Manager Server** field, provide the following IP address.

- For 500/1000 agent deployment enter the Unified CCE Data server side A IP address.
- For SCC/4000 agent deployment enter the Unified Rogger side A IP address.
- For 12000 agent deployment enter the Unified Logger Side A IP address.

**Step 8** In the CTI Server A field, provide the A side CTIOS server IP Address; in the CTI Server Port A field, enter **42027** as the port number.

**Step 9** In the CTI Server B field, provide the B side CTIOS server IP address; in the CTI Server Port B field, enter **43027** as the port number.

**Step 10** Leave all other field as default and click **Next**. In the following window that opens, click **Next** to complete the install.

## 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 524. 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 572. 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.

**Note** In Small Contact Center deployment model if customer chooses for shared outbound gateway, enter Perimeta SBC signaling-address in **Address IPv4** field and select the same port that is configured in the CUCM adjacency (SUBCUST1-CUCM-PUB). See, Configure Adjacencies for Sub Customer Instance, on page 490.

# Configure Post Call Survey

Complete the following procedures to configure post call survey:

- Configure Unified CVP, on page 641
- Configure Unified CCE, on page 642

# Configure Unified CVP

Complete the following procedure to configure Unified CVP.

#### Procedure

**Step 1** Log in to the 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 normal call flow completes.
- 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 ICM 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 core components to support a-law codec:

- Configure Gateway, on page 643

• Configure Unified CVP, on page 645
• Configure Unified Communication Manager, on page 646

# Configure Gateway

• Configure Ingress Gateway, on page 643
• Configure VXML Gateway, on page 644

## Configure Ingress Gateway

### Procedure

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

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

**Example:**

```
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
6. C:\inetpub\wwwroot\en-us\VL (optional, applicable only for RSM)

**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 Built-in Bridge. See, Enable or Disable the Built-in-Bridge , on page 588
- Add Monitoring Calling Search Space for the device, on page 647

# Add Monitoring Calling Search Space for the device

### Before You Begin

Ensure that agent phones are added. See, Add Phones, on page 581.

**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 585.

**Step 3** Edit **Lines**, choose newly added **Calling Search Space** from the drop-down list. See, Edit Lines, on page 581.

**Step 4** Click **Save**.

# Configure Music On Hold

## 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 deployments with less than 1250 users in a CM Cluster.

2 As standalone node (TFTP/MoH Server) for HCS deployments with more than 1250 users in a CM Cluster

- Configure Music On Hold Server Audio Source, on page 648
- Set up Service Parameters for Music on Hold, on page 649
- Set up Phone Configuration for Music on Hold, on page 649

### 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

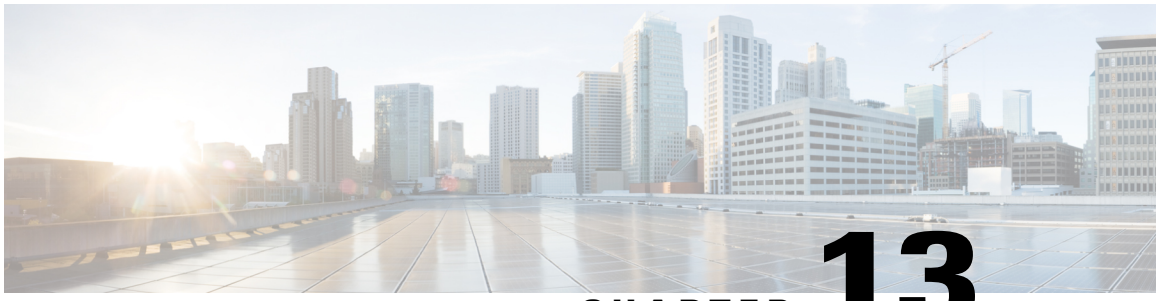
### Procedure

**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 13

# Install and Configure Optional Cisco Components



## SPAN-Based Monitoring



### Install SPAN based Silent Monitoring

**Procedure**

**Step 1** Mount the Cisco CCE CTI ISO image.

**Step 2** Run `setup.exe` file to install SPAN based Silent Monitoring.

**Step 3** On CTIOS Silent Monitoring Service page, Click **Yes** to stop CTIOS Silent Monitor process

**Step 4** In Software License Agreement page Click **Yes** and 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 Choose Destination Location page, browse to the directory where you want to install and click **Next**.

**Step 7** Enter the following information in the Cisco CTIOS Silent Monitor - Install Shield Wizard:

a) Host Name\IP Address: Host Name of the silent monitor server.
b) Port: Enter the port number **42228** on which the Silent Monitor Service listens for incoming connections.
c) **Check** Silent Monitor Server: Select this to allow the Silent Monitor Service to monitor multiple Mobile Agents simultaneously.
d) Enter 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 CTIOS Silent Monitor page, do not check **Enable Security**. Click **OK**.

**Step 10** Click **Finish** to complete the installation.

# 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

Span from Call Manager is recommended 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.

# Unified CCE AW-HDS-DDS

To install Unified CCE AW-HDS-DDS, see Create Golden Template for Unified CCE AW-HDS-DDS, on page 269 and to configure see Configure Unified CCE AW-HDS-DDS, on page 409.

# Cisco RSM



## Create Golden Template for Cisco Remote Silent Monitoring

Follow this sequence of tasks to create the golden template for the Cisco RSM server.

After each task, return to this page to mark the task "done" and continue the sequence.

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download `HCS-CC_11.0(1)_CCE-RSM_vmv9_v1.0.ova`. | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for the Cisco RSM server. | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 5 | | Install antivirus software. | Follow the procedure Install Antivirus Software, on page 253. |
| 6 | | Install the JTAPI Client. | Follow the procedure Install the JTAPI Client, on page 655. |
| 7 | | Configure SNMP Traps for Cisco RSM | Follow the procedure Configuring SNMP Traps for Cisco RSM, on page 656 |
| 8 | | Install the Cisco RSM server. | Follow the procedure Install the Cisco RSM Server , on page 655. |
| 9 | | Convert the virtual machine to a template. | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Cisco RSM server on the destination system. See Configure Cisco RSM, on page 656.

## Install the JTAPI Client

Complete the following procedure to install JTAPI on the Cisco RSM server.

### Procedure

**Step 1** Start the **Unified Communications Manager Administration** application in a browser.

**Step 2** Login using the administrator credentials.

**Step 3** Navigate to **Application** > **Plugins** and then click **Find**.

**Step 4** Download the Cisco JTAPI 32-bit Client for Windows.

**Step 5** Install the downloaded file and accept all the default settings.

**Note**
- In the **Cisco TFTP IP Address** text-box enter the CUCM Subscriber IP Address.
- For Small Contact Center agent deployment model this is optional as RSM needs to be connected to multiple sub customer CUCM clusters

## Install the Cisco RSM Server

Complete the following procedure to install the Cisco RSM Server.

### Procedure

**Step 1** Mount the Cisco RSM ISO image to the virtual machine. For more information, see Mount and Unmount ISO Files, on page 787.

**Step 2** Run the setup.exe file to install the RSM server.
The RSM installer program starts and it displays the Cisco Remote Silent Monitoring(RSM) InstallShield window.

**Step 3** Click **Next**.
It displays the Licence Agreement page.

**Step 4** In the Licence Agreement page, accept the License. Click **Next**.

**Step 5** In the service Login Information page, provide the administrator credentials of RSM Virtual machine. Click **Next**.

**Step 6** In the Launch Configuration Settings page, click **Exit** from the setup. Click **Yes** on the pop-up window.

**Step 7** Click **Finish**.

### What to Do Next

Configure RSM, on page 658

## Configuring SNMP Traps for Cisco RSM

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

Complete the following procedures to configure SNMP traps for use with Cisco RSM:

- Configure SNMP Service for Trap Forwarding, on page 207
- Configure SNMP Agent in MIB , on page 656

### Configure SNMP Agent in MIB

The following information is to connect the RSM SNMP Agent and to root the MIB Object.

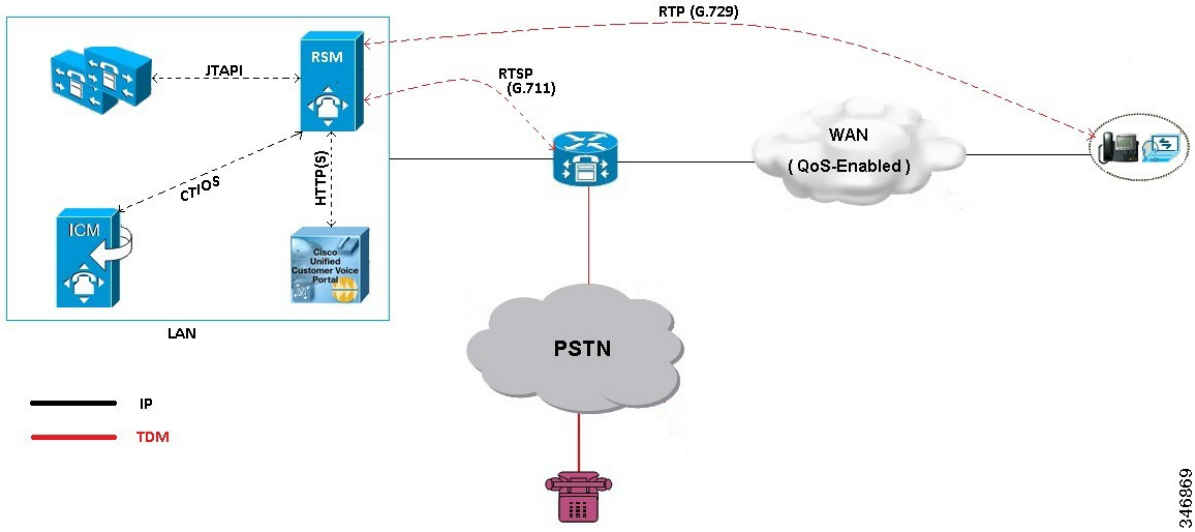
- **RSM SNMP Agent Connection**: < *RSM Server IP* >:33161
- **RSM SNMP Agent Root OID**: .1.3.6.1.4.1.9.9.2776 - ciscoRSMMIB

# Configure Cisco RSM

- Configure Cisco RSM for 500 and 1000 Agent Deployment, on page 657
- Configure Cisco RSM for 4000 Agent Deployment, on page 665
- Configure Cisco RSM for Small Contact Center Deployment, on page 669
- Configure Cisco RSM for 12000 Agent Deployment, on page 668
- Configure Cisco RSM for A-Law Codec, on page 672

The following figure shows the configuration topology for Remote Silent Monitoring.

***Figure 80: Cisco Remote Silent Monitoring Configuration Topology***




## Configure Cisco RSM for 500 and 1000 Agent Deployment

Configure the Cisco RSM (Remote Silent Monitoring) Server for 500 and 1000 agent deployment in the distributed mode, in the following order:

| Required Software | Tasks |
|---|---|
| Configure RSM | Set RSM Configuration Settings for 500 and 1000 Agent Deployment, on page 658 |
| | Configure JTAPI Client Preferences, on page 660 |
| | Edit Registry Settings, on page 660 |
| Configure Gateway | Set Up the VXML Gateway, on page 660 |
| Configure Unified CVP | Upload RSM Prompts, on page 661 |
| | Integrate the CVP Call Flow, on page 661 |
| | Call Flow Deployment, on page 662 |
| Configure Unified CCE | Set the Agent Target Rule, on page 663 |
| | Create the Supervisor Login Account, on page 664 |
| | Create Routing Script for RSM, on page 664 |

| Required Software | Tasks |
|---|---|
| Configure Unified Call Manager | Configure Simulated Phone, on page 665 |
| | Set Up the Login Pool Simphone , on page 665 |
| | Create RSM Application User , on page 767 |

## Configure RSM

*Set RSM Configuration Settings for 500 and 1000 Agent Deployment*

### Procedure

**Step 1** Complete the Mail Server configuration settings:

a) Choose **Start** > **CiscoRSM** > **RSM Configuration Manager**.
b) Check **Send Email Alert** checkbox.
c) Enter the Host Name/IP address of the mail server in **Mail Server Host Name/IP** text box.
d) Enter the email port number in **Port** text box.
e) Enter the sender email ID in **Sender Email Address** text box.
f) Enter the receiver email ID in **Receiver Email Address** text box.
g) Click **Next**.

**Step 2** Complete the Miscellaneous configuration settings:

a) Enter **1800** in **Problem Call Minimum Duration** text box.
b) Enter **4** in **Problem Call Min Holds** text box.
c) Enter **3600** in **Max Stale Call Duration** text box.
d) Set blank value for **CTI OS Trace Mask**.
e) Select **INFO** from the **Log Level** drop down list for VL Engine.
f) Enter **8080** in **HTTP Listen Port** text box for VL Engine.
g) Enter **480** in the **Audio Buffer Len To VRU** text box for PhoneSim.
**Note** The default value of Audio Buffer Len to VRU is 160, for CVP environment the value is set to 480.
h) Select **INFO** from the **Log Level** drop down list for PhoneSim.
i) Enter **29001** in **HTTP Listen Port** text box for PhoneSim.
j) Enter **29554** in **RTSP Listen Port** text box for PhoneSim.
k) Select the **RTSP u-law** for **Audio Encoding** from the drop down list for Phonesim.
l) Select **No** from the **Do HTTP Chunked Transfers** drop down list for PhoneSim.
m) Enter the IP Address of RSM server in the **Host Data IP** text box.
n) Click **Next.**

**Step 3** Define Cluster configuration settings:
These settings are used to configure each Unified Communications Manager cluster with the agents to be monitored by RSM.

a) Click **Add Cluster**
b) Enter a cluster name in **ClusterN_Name** text box.

**Note** Name should be alphanumeric.

c) Enter **5** in **No. of Login Pool Simphones** text box.
d) Enter **60** in **No. of Monitoring Phones** text box. (this is to monitor 60 concurrent).
e) Enter **5000** in the **Peripheral ID** text box.
f) Enter the **rsmuser** in **JTAPI Username** text box.
g) Enter the rsmuser password in **JTAPI Password** text box.
h) Enter the first MAC address to use for auto-generation of MAC range for simphone device names in **Start MAC Range** text box.
i) Enter the first extension number to use for auto-generation of line extension range for simphone DNs in **Start Line Num Range** text box.

**Note**
1. Line extension ranges must not overlap between clusters. Correlates to ClusterN_PhoneSim_StartMACRange value.
2. The Start Line Num Range should be between 4 to 15 digits.

j) Select **TCP** from the **SIP Transport** drop down list.
k) Click **Next**.

**Step 4** Define Unified Communications Manager configuration settings:

a) Enter the host name / IP address of CUCM1 server(Subscriber1) in **Host Name/IP** text box.
b) Enter CUCM1 port as **5060** in **Port** text box.
c) Enter the host name / IP address of CUCM2 server(Subscriber 2) in **Host Name/IP** text box.
d) Enter CUCM2 port as **5060** in **Port** text box.
e) Click **Next**.

**Step 5** In UCCE Integration page select UCCE integrate with CTIOS OR UCCE integrate with CTI

a) If UCCE Integration with CTIOS is selected, perform the following instructions:

1. Enter the host name / IP address of CTIOS 1A in **CTIOS 1A Host Name/IP**.
2. Enter **42028** in **CTIOS 1A Port** text box.
3. Enter the host name / IP address of CTIOS 1B in **CTIOS 1B Host Name/IP**.
4. Enter **42028** in **CTIOS 1B Port** text box.
5. Click **Next**.

a) If UCCE Integration with CTI is selected, perform the following instructions:

1. Enter the host name / IP address of CTI 1A in **CTI 1A Host Name/IP**.
2. Enter **42027** in **CTI 1A Port** text box.
3. Enter the host name / IP address of CTI 1B in **CTI 1B Host Name/IP**.
4. Enter **43027** in **CTI 1B Port** text box.
5. Click **Next**.

**Step 6** Click **Next** and Check **Start PhoneSim Service** and **Start VLEngine Service** check boxes.

**Step 7** Click **Finish**.

### *Configure JTAPI Client Preferences*

**Procedure**

**Step 1** Choose **Start** > **All Programs** > **Cisco JTAPI** and click **Cisco Unified Communications Manager JTAPI Preferences**.

**Step 2** Click **Language** tab.

**Step 3** Select **English** from the Select Language drop-down list.

**Step 4** Enter the **TFTP Server IP Address**.

**Step 5** Click **OK**.

### *Edit Registry Settings*

RSM requires numeric supervisor accounts, so that users can log in through the telephone. However, Unified CCE supervisor agent accounts are also Active Directory user accounts and an Active Directory security policy can prevent numeric-only accounts. To resolve this issue, modify the "VLEngine_PassPrefix" parameter.

**Procedure**

**Step 1** Access the Registry Editor, **Start** > **Run** > **regedit**.

**Step 2** Navigate to **HKEY_Local_Machine** > **Software** > **Wow6432Node** > **Cisco Systems, Inc.** > **Remote Silent Monitoring**.

**Step 3** Set**VLEngine_PassPrefix** with a string that prepends the password before it submits for CTI OS Validation. For Example: If "VLEngine_PassPrefix" String is set to **RSM1RSM** and you want a supervisor to log in with PIN **1234**, then set supervisor's password to **RSM1RSM1234**.

**Note** The valid values are any string of letters, numbers, and valid password symbols (no whitespace and control characters).

## Configure Gateway

### *Set Up the VXML Gateway*

RSM is supported on any VXML gateway models and versions of Cisco IOS supporting CVP. The Ingress/VXML gateway can be shared between RSM and other features.

To set up the VXML gateway for RSM, make sure that the IVR prompt memory is at least 8 Mb, by issuing the **ivr prompt memory 8000** command.

**Note** If the gateway is shared with RSM along with other features, the gateway performance reduces by 20%.

## Configure Unified CVP

### *Upload RSM Prompts*

**Procedure**

**Step 1** Navigate to your media server directory, at C:\inetpub\wwwroot\en-us\, and create a new directory labeled VL.

**Step 2** Navigate to your RSM server and copy prompts.zip from C:\ CiscoRSM\callflows and unzip the contents into the VL directory of the media server.

**Step 3** Right-click the VL directory, then click **Properties**.

**Step 4** Click the Security tab, click **Advanced** and click **Change Permission**.

**Step 5** Select **Include inheritable permission from object's parent** and **Replace all child object permission with inheritable permissions from this object** check-boxes.

**Step 6** Click **OK** and click **Yes** on the windows security pop up window.

**Step 7** Open your web browser and navigate to the VL directory of your media server, that is http://<SERVER IP>/en-us/VL. Ensure that the prompt files are listed and accessible.

### *Integrate the CVP Call Flow*

**Procedure**

**Step 1** Navigate to the C:\CiscoRSM\callflows\vxml-cvp folder on the RSM server.

**Step 2** Copy all the contents from the folder to a directory that can be accessed by the desktop machine hosting Cisco Unified Call Studio software (for example, C:\RSM-Callflow).

**Step 3** Launch the Call Studio. Navigate to **File**> **Import**> **Call Studio**>**Existing Call Studio Project** in the menu bar to import the RSM project into the workspace and click **Next**.

**Step 4** Browse the vxml-cvp folder and click **Finish**.

**Step 5** Navigate to the **DoLogin** page in the Callflow Editor Navigator pane for RSM Project.

**Step 6** Select the SetBaseSessionVars element, and then click **Data** under **Element Configuration**.

**Step 7** Modify the **VoiceXML Variable settings** for RSM Project as follows:

**Note** Ensure that you click **Update** after modifying the variable settings below; else, the fields will be set with default values.

- **VL_VLENGINE_HOSTNAME—** Hostname or IP address of the server running on VLEngine service.
- **VL_VLENGINE_PORT—** Port number used by the VLEngine service. Port value is 8080.
- **VL_PHONESIM_HOSTNAME—** Hostname or IP address of the server running on PhoneSim service. Value is same as VL_VLENGINE_HOSTNAME.
- **VL_PHONESIM_RTSP_PORT—** RTSP port number used by PhoneSim service. This is usually 29554.
- **VL_PHONESIM_HTTP_PORT—** HTTP port number used by PhoneSim service. This is usually 29001.

- **MAX_NUM_LOGIN_ATTEMPTS—** Maximum number of failed login attempts allowed before RSM disconnects user.
- **CVP_MEDIASVR_AUDIO_PATH—** Points to the URL path where RSM prompts are uploaded (for example, /en-us/VL).

  **Note** This path, and the Path component specified in the RSM CVP project's **Audio Settings - Default Audio Path URL** text field, should be identical.
- **CVP_MEDIASVR_HOSTNAME—** Hostname or IP address of the CVP media server with RSM prompts, as found in the /en-us/VL directory.
- **MAIN_MENU_TIMEOUT—** Time, in seconds. This is usually 12 seconds.
- **CVP_VXMLSVR_HOSTNAME—**Hostname or IP address of the server running on VXML server.
- **CVP_VXMLSVR_PORT—**Port number used by the VXML server.
- **CVP_MEDIASVR_PORT—**Port number of the media server domain. This is usually port 80.
- **MONITOR_NEWEST_REPOLL_PERIOD—**Time, in seconds, before monitoring any new agent conversations. This value is normally set to 4 seconds.
- **MONITOR_NEWEST_PROMPT_TO_END_EVERYN—**Number of pollings before the progress prompt is stated to the caller (that is, “System is still busy. Press any key to return to main menu or continue to hold.”). This value is normally set to 3.
- **SUPERVISOR_LOGIN_TIMEOUT—**Time out for Supervisor Login. This value is normally set to 1500.

**Step 8** Click **Save** to save the RSM Project.

**Step 9** Right-click **RSM Project** in the navigator pane then click **Properties**.

**Step 10** Under **Call Studio**, click **Audio Settings**.

**Step 11** Navigate to the Default Audio Path URI text field and enter the VL directory on your media server, for example, `http://<cvp_media_server_IP_address>/en-us/VL` . Click **OK**.

**Step 12** Repeat the above steps to create RSM project for each CVP Server in your deployment.

**Note** For small contact center deployment, repeat the steps 1 through 11 for creating unique RSM projects for each sub customer in each CVP server.

### *Call Flow Deployment*

Once the call flow script is installed on the CVP server, it must be deployed for use by CVP VXML Server.

Perform the procedure to deploy the call flow script.

**Note** Deploy the VXML script in all the CVP boxes with the appropriate CVP_VXMLSVR_HOSTNAME

### Procedure

**Step 1** Open Cisco Unified Call Studio.

**Step 2** Right-click **RSM Project** in the navigator pane, then click **Deploy**.

**Step 3** Select **Archive File** radio button.

**Step 4** Browse to the loction where you want to save the VXML Application file.

**Step 5** Click **Finish**. The call flow script will be saved at the specified location.

**Step 6** Open the CVP OAMP portal.

**Step 7** Navigate to **Bulk Administration** > **File Transfer** > **VXML application**.

**Step 8** Choose the desired CVP VXML servers from **Available** to **Selected** and browse the VXML application file that you saved in step 4.

**Step 9** Click **Transfer** and click **File Transfer Status** to check the status.

**Step 10** Go to the SCC-CVP-SVR-A server and navigate to the C:\Cisco\CVP\VXMLServer\applications\RSM\admin Directory in CVP call server, then double-click the **deployApp.bat** file. The batch file is executed in a separate DOS window.

**Step 11** Enter **Y** for yes when prompted to deploy the application. The call flow script is now accessible from the CVP VXML Server.

**Step 12** Configure the appropriate micro applications on your VXML gateway (VXML Gateway dial peers, Unified Communication Manager route patterns, and so on) so they can access the script.

## Configure Unified CCE

*Set the Agent Target Rule*

**Note** Ignore this procedure, if Unified CCE Day 1 configuration includes the Extension range.

### Procedure

**Step 1** From the Administration Workstation (AW), click **Start** > **All Programs** > **Configuration Manager**.

**Step 2** Expand **Tools**, then expand **List Tools**. Double-click **Agent Targeting Rule**.

**Step 3** Click **Retrieve** to return a list of all existing agent targets in the environment.

**Step 4** Highlight the existing agent targeting rule. Under extension ranges click **Add**. A blank extension range section appears.

**Step 5** Add the range of extension, that is the DN and then click **OK**.

**Step 6** Click **Save**.

**Note** In 4000 deployment there are two CUCM PGs configured according to CUCM application user. ATRs are configured based on CUCM PG. Therefore, two ATRs are pre-configured as a part of load base configuration and extensions should be added to ATRs based on the Application user.

### *Create the Supervisor Login Account*

You must create a new account for each supervisor who will be using RSM, according to your current CTI OS supervisor/agent accounts. If CTI OS authentication is used, separate supervisor agent accounts must be created in the Unified CCE environment, to allow dialed-in supervisors to log in to the system.

To create a supervisor login account, follow this procedure Create an Agent, on page 508

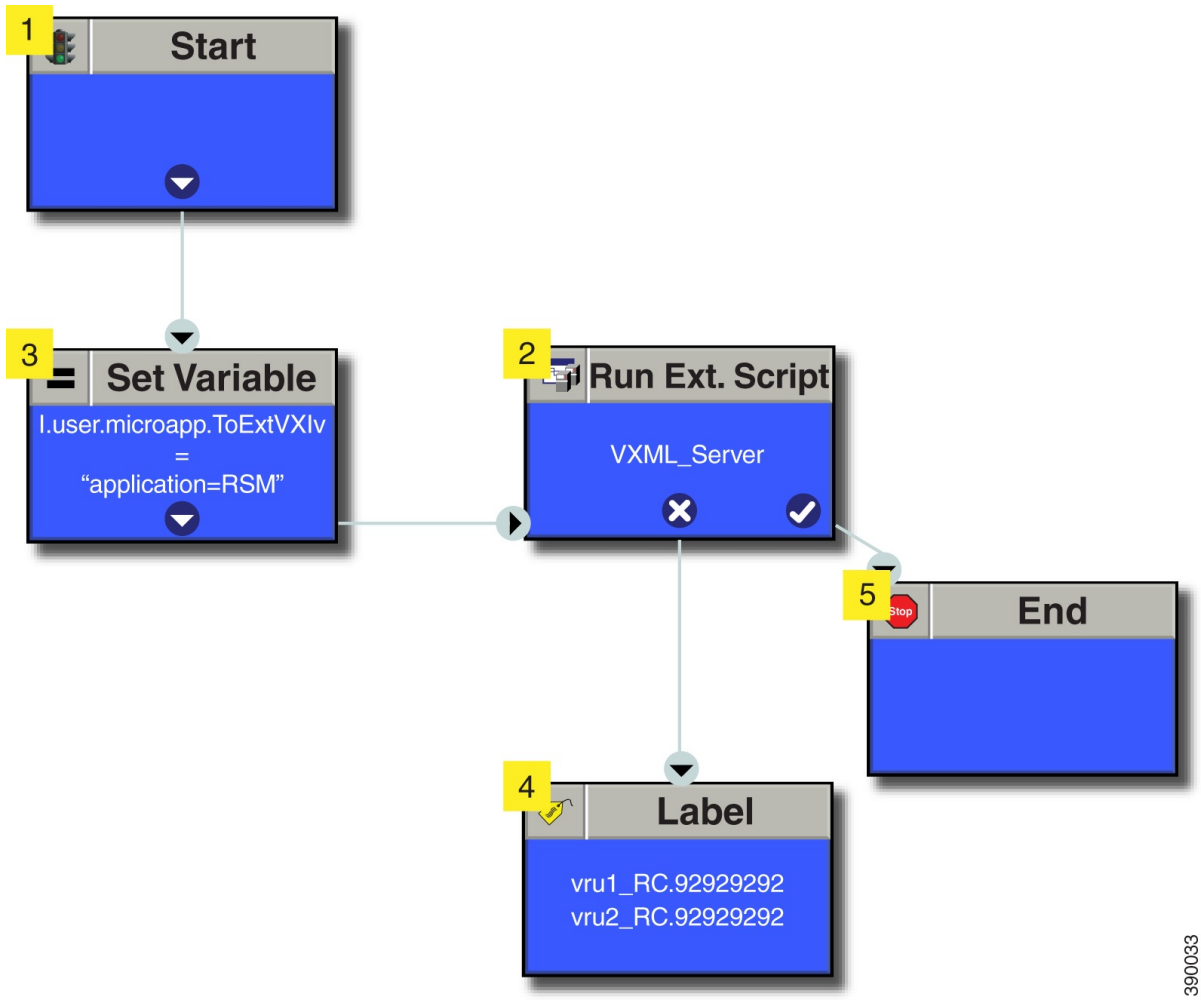
**Note**

1. Check the Supervisor check box and ensure that the supervisor password should meet AD Password Policy.
2. Ensure that the agent password is numeric of any length.
3. Ensure that the Supervisor is added to Team List.

### *Create Routing Script for RSM*

The following Routing Scripts are used for Cisco RSM.

***Figure 81: Routing Scripts used for Cisco RSM***



### Configure Unified Communication Manager

#### *Configure Simulated Phone*

**Before You Begin**

You must determine the number of simulated phones ( also called as simphones) to assign to each Unified Communication Manager cluster. Each cluster must have a number of simphones greater than or equal to the maximum number of agents that will be simultaneously monitored through RSM for the cluster. This section provides the following information:

- Configure the simphone device dependencies
- Create the simphone devices

Perform the following steps to add new cluster in RSM:

Create Simphone Device Dependencies

Perform the below steps to create Simphone device dependencies:

- Configure Cisco Unified CM Group, on page 578
- Add Regions, on page 584
- Add Device Pool, on page 579

Create Simphone Device

Perform the below steps to create Simphone devices:

- Add Phones, on page 581
- Disable Built-in Bridge see, Enable or Disable the Built-in-Bridge , on page 588

#### *Set Up the Login Pool Simphone*

The first five simphone devices that are created for each cluster are automatically assigned to the VLEngine login pool. The login pool performs a test login to CTI OS when a caller is authenticated by RSM, to support the VLEngine authentication mechanism. Because CTI OS logins are performed on these simphone devices, they must be associated with the pguser account on each Unified Communications Manager cluster. They must also have Cisco Unified Intelligent Contact Management Enterprise device targets created.

**What to Do Next**

- Create RSM Application User , on page 767
- Associate first five phones to application user. see, Associate Phone to Application User, on page 586

.

## Configure Cisco RSM for 4000 Agent Deployment

Configure the Cisco RSM (Remote Silent Monitoring) Server for 4000 agent deployment in the distributed mode, in the following order:

| Required Software | Tasks |
|---|---|
| Configure RSM | Set RSM Configuration Settings for 4000 and 12000 Agent Deployment, on page 666 |
| | Configure JTAPI Client Preferences, on page 660 |
| | Edit Registry Settings, on page 660 |
| Configure Gateway | Set Up the VXML Gateway, on page 660 |
| Configure Unified CVP | Upload RSM Prompts, on page 661 |
| | Integrate the CVP Call Flow, on page 661 |
| | Call Flow Deployment, on page 662 |
| Configure Unified CCE | Set the Agent Target Rule, on page 663 |
| | Create the Supervisor Login Account, on page 664 |
| | Create Routing Script for RSM, on page 664 |
| Configure Unified Call Manager | Configure Simulated Phone, on page 665 |
| | Set Up the Login Pool Simphone , on page 665 |
| | Create RSM Application User , on page 767 |

## Set RSM Configuration Settings for 4000 and 12000 Agent Deployment

### Procedure

**Step 1** Complete the Mail Server configuration settings:

a) Choose **Start** > **CiscoRSM** > **RSM Configuration Manager**.
b) Check **Send Email Alert** check box.
c) Enter the Host Name/IP address of the mail server in **Mail Server Host Name/IP** text box.
d) Enter the email port number in **Port** text box.
e) Enter the sender email ID in **Sender Email Address** text box.
f) Enter the receiver email ID in **Receiver Email Address** text box.
g) Click **Next**.

**Step 2** Complete the Miscellaneous configuration settings:

a) Enter **1800** in **Problem Call Minimum Duration** text box.
b) Enter **4** in **Problem Call Min Holds** text box.
c) Enter **3600** in **Max Stale Call Duration** text box.

d) Set blank value for **CTI OS Trace Mask**.
e) Select **INFO** from the **Log Level** drop down list for VL Engine.
f) Enter **8080** in **HTTP Listen Port** text box for VL Engine.
g) Enter **480** in the **Audio Buffer Len To VRU** text box for PhoneSim.
**Note** The default value of Audio Buffer Len to VRU is 160, for CVP environment the value is set to 480.
h) Select **INFO** from the **Log Level** drop down list for PhoneSim.
i) Enter **29001** in **HTTP Listen Port** text box for PhoneSim.
j) Enter **29554** in **RTSP Listen Port** text box for PhoneSim.
k) Select the **RTSP u-law** for **Audio Encoding** from the drop down list for Phonesim.
l) Select **No** from the **Do HTTP Chunked Transfers** drop down list for PhoneSim.
m) Enter the IP Address of RSM server in the **Host Data IP** text box.
n) Click **Next.**

**Step 3** Define first Cluster configuration settings:
These settings are used to configure the Unified Communications Manager cluster with the agents to be monitored by RSM.

a) Click **Add Cluster**
b) Enter a cluster name in **ClusterN_Name** text box.
**Note** Name should be alphanumeric.
c) Enter **5** in **No. of Login Pool Simphones** text box.
d) Enter **60** in **No. of Monitoring Phones** text box. (this is to monitor 60 concurrent).
e) Enter **5000** in the **Peripheral ID** text box.
f) Enter the **rsmuser1** in **JTAPI Username** text box.
g) Enter the rsmuser1 password in **JTAPI Password** text box.
h) Enter the first MAC address to use for auto-generation of MAC range for simphone device names in **Start MAC Range** text box.
i) Enter the first extension number to use for auto-generation of line extension range for simphone DNs in **Start Line Num Range** text box.
**Note**
**1** Line extension ranges must not overlap between clusters. Correlates to ClusterN_PhoneSim_StartMACRange value.
**2** The Start Line Num Range should be between 4 to 15 digits.
j) Select **TCP** from the **SIP Transport** drop down list.
k) Click **Next**.

**Step 4** Define Unified Communications Manager configuration settings for first cluster:

a) Enter the host name / IP address of CUCM1 server(Subscriber1) in **Host Name/IP** text box.
b) Enter CUCM1 port as **5060** in **Port** text box.
c) Enter the host name / IP address of CUCM2 server(Subscriber 2) in **Host Name/IP** text box.
d) Enter CUCM2 port as **5060** in **Port** text box.
e) Click **Next**.

**Step 5** In UCCE Integration page select UCCE integrate with CTI

a) Enter the host name / IP address of CTI 1A in **CTI 1A Host Name/IP**.
b) Enter **42027** in **CTI 1A Port** text box.
c) Enter the host name / IP address of CTI 1B in **CTI 1B Host Name/IP**
d) Enter **43027** in **CTI 1B Port** text box.

e) Click **Next**.

**Step 6** Define second Cluster configuration settings:
These settings are used to configure the Unified Communications Manager cluster with the agents to be monitored by RSM.

a) Click **Add Cluster**
b) Enter a cluster name in **ClusterN_Name** text box.
**Note** Name should be alphanumeric.
c) Enter **5** in **No. of Login Pool Simphones** text box.
d) Enter **60** in **No. of Monitoring Phones** text box. (this is to monitor 60 concurrent).
e) Enter **5001** in the **Peripheral ID** text box.
f) Enter the **rsmuser2** in **JTAPI Username** text box.
g) Enter the rsmuser2 password in **JTAPI Password** text box.
h) Enter the first MAC address to use for auto-generation of MAC range for simphone device names in **Start MAC Range** text box.
i) Enter the first extension number to use for auto-generation of line extension range for simphone DNs in **Start Line Num Range** text box.
**Note** **1** Line extension ranges must not overlap between clusters. Correlates to ClusterN_PhoneSim_StartMACRange value.
**2** The Start Line Num Range should be between 4 to 6 digits.
j) Select **TCP** from the **SIP Transport** drop down list.
k) Click **Next**.

**Step 7** In UCCE Integration page select **UCCE integrate with CTI**

a) Enter the host name / IP address of CG 2A in **CTI 1A Host Name/IP**.
b) Enter **42027** in **CTI 1A Port** text box.
c) Enter the host name / IP address of CG 2B in **CTI 1B Host Name/IP**.
d) Enter **43027** in **CTI 1B Port** text box.
e) Click **Next**.

**Step 8** Check **Start PhoneSim Service** and **Start VLEngine Service** check boxes.

**Step 9** Click **Finish**.
**Note** For 12000 agent deployment model, repeat the steps from step 3 to add new clusters.

## Configure Cisco RSM for 12000 Agent Deployment

Configure the Cisco RSM (Remote Silent Monitoring) Server for 12000 agent deployment in the distributed mode, in the following order:

| Required Software | Tasks |
|---|---|
| Configure RSM | Set RSM Configuration Settings for 4000 and 12000 Agent Deployment, on page 666 |
| | Configure JTAPI Client Preferences, on page 660 |
| | Edit Registry Settings, on page 660 |
| Configure Gateway | Set Up the VXML Gateway, on page 660 |
| Configure Unified CVP | Upload RSM Prompts, on page 661 |
| | Integrate the CVP Call Flow, on page 661 |
| | Call Flow Deployment, on page 662 |
| Configure Unified CCE | Set the Agent Target Rule, on page 663 |
| | Create the Supervisor Login Account, on page 664 |
| | Create Routing Script for RSM, on page 664 |
| Configure Unified Call Manager | Configure Simulated Phone, on page 665 |
| | Set Up the Login Pool Simphone , on page 665 |
| | Create RSM Application User , on page 767 |

## Configure Cisco RSM for Small Contact Center Deployment

Configure the Cisco RSM (Remote Silent Monitoring) Server for Small Contact Center deployment in the distributed mode, in the following order.

**Note** Each Sub customer will have Individual RSM configured.

| Required Software | Tasks |
|---|---|
| Configure RSM | Set RSM Configuration Settings for Small Contact Center Deployment, on page 670 |
| | Configure JTAPI Client Preferences, on page 660 |
| | Edit Registry Settings, on page 660 |
| Configure Gateway | Set Up the VXML Gateway, on page 660 |

| Required Software | Tasks |
|---|---|
| Configure Unified CVP | Upload RSM Prompts, on page 661 |
| | Integrate the CVP Call Flow, on page 661 |
| | Call Flow Deployment, on page 662 |
| Configure Unified CCE | Set the Agent Target Rule, on page 663 |
| | Create the Supervisor Login Account, on page 664 |
| | Create Routing Script for RSM, on page 664 |
| Configure Unified Call Manager | Configure Simulated Phone, on page 665 |
| | Set Up the Login Pool Simphone , on page 665 |
| | Create RSM Application User , on page 767 |

## Set RSM Configuration Settings for Small Contact Center Deployment

### Procedure

**Step 1** Complete the Mail Server configuration settings:

a) Choose **Start** > **CiscoRSM** > **RSM Configuration Manager**.
b) Check **Send Email Alert** check box.
c) Enter the Host Name/IP address of the mail server in **Mail Server Host Name/IP** text box.
d) Enter the email port number in **Port** text box.
e) Enter the sender email ID in **Sender Email Address** text box.
f) Enter the receiver email ID in **Receiver Email Address** text box.
g) Click **Next**.

**Step 2** Complete the Miscellaneous configuration settings:

a) Enter **1800** in **Problem Call Minimum Duration** text box.
b) Enter **4** in **Problem Call Min Holds** text box.
c) Enter **3600** in **Max Stale Call Duration** text box.
d) Set blank value for **CTI OS TraceMask**.
e) Select **INFO** from the **Log Level** drop down list for VL Engine.
f) Enter **8080** in **HTTP Listen Port** text box for VL Engine.
g) Enter **480** in the **Audio Buffer Len To VRU** text box for PhoneSim.

**Note** The default value of Audio Buffer Length to VRU is 160, for CVP environment the value is set to 480.

h) Select **INFO** from the **Log Level** drop down list for PhoneSim.
i) Enter **29001** in **HTTP Listen Port** text box for PhoneSim.
j) Enter **29554** in **RTSP Listen Port** text box for PhoneSim.

k) Select the **RTSP u-law** for **Audio Encoding VRU** from the drop down list for Phonesim.
l) Select **No** from the **Do HTTP Chunked Transfers** drop down list for PhoneSim.
m) Enter the IP Address of RSM server in the **Host Data IP** text box.
n) Click **Next.**

**Step 3** Define Cluster configuration settings:
These settings are used to configure the Unified Communications Manager cluster with the agents to be monitored by RSM.

a) Click **Add Cluster**
b) Enter a cluster name in **ClusterN_Name** text box.
**Note**
- Name should be alphanumeric.
- N represents the cluster number.

c) Enter **5** in **No. of Login Pool Simphones** text box.
d) Enter **10** in **No. of Monitoring Phones** text box. (this is to monitor 10 concurrent).
e) Enter the Peripheral ID of Agent PG in the**Peripheral ID** text box.
f) Enter the **rsmuser** in **JTAPI Username** text box.
g) Enter the rsmuser password in **JTAPI Password** text box.
h) Enter the first MAC address to use for auto-generation of MAC range for simphone device names in **Start MAC Range** text box.
i) Enter the first extension number to use for auto-generation of line extension range for simphone DNs in **Start Line Num Range** text box.
**Note**
1. Line extension ranges must not overlap between clusters. Correlates to ClusterN_PhoneSim_StartMACRange value.
2. The Start Line Num Range should be between 4 to 15 digits.

j) Select **TCP** from the **SIP Transport** drop down list.
k) Click **Next**.

**Step 4** Define Unified Communications Manager configuration settings for the cluster:

a) Enter the host name / IP address of CUCM1 server(Publisher) in **Host Name/IP** text box.
b) Enter CUCM1 port as **5060** in **Port** text box.
c) Enter the host name / IP address of CUCM2 server(Subscriber 1) in **Host Name/IP** text box.
d) Enter CUCM2 port as **5060** in **Port** text box.
e) Click **Next**.

**Step 5** Select **UCCE Integration with CTI** in UCCE Integration window and enter the following:

a) Enter the host name / IP address of Agent PG 1A in **CTI 1A Host Name/IP** .
b) Enter **42027** in **CTI 1A Port** text box.
c) Enter the host name / IP address of Agent PG 1B in **CTIOS 1B Host Name/IP**.
d) Enter **43027** in **CTI 1B Port** text box.
e) Click **Next**.

**Step 6** Check **Start PhoneSim Service** and **Start VLEngine Service** check boxes.

**Step 7** Click **Finish**.

## Configure Cisco RSM for A-Law Codec


- Configure RSM, on page 672
- Configure Gateway, on page 672
- Configure Unified CVP, on page 672
- Configure Unified Communications Manager, on page 672


### Configure RSM

For more information about configuring Cisco RSM, see Configure RSM, on page 658.

**Note** Ensure that you select **rtsp-alaw** for **Miscellaneous configuration settings** (**Step 2-k**) in RSM configuration.

### Configure Gateway

For more information, see Configure Gateway, on page 643.

### Configure Unified CVP

For more information, see Configure Unified CVP, on page 645.

### Configure Unified Communications Manager


- Configure Service Parameters, on page 672
- Configure Regions, on page 583


*Configure Service Parameters*

For more information, see Configure Unified Communication Manager, on page 646.

# Cisco MediaSense


- Create Golden Template for Cisco MediaSense, on page 672
- Automated Cloning and OS Customization, on page 300
- Configure Cisco MediaSense, on page 673


# Create Golden Template for Cisco MediaSense

Follow the below sequence of tasks to create the golden template for Cisco MediaSense. After each task, return to this page to mark the task "done" and continue the sequence:

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Download cms_11.0_vmv8_v1.0.ova. | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine from the OVA. | Follow the procedure that is documented in, Create Virtual Machines, on page 251. |
| 3 | | Install Cisco MediaSense. | Follow the procedure for installing VOS applications for golden templates. See Install Unified Communications Voice OS based Applications, on page 264. |
| 4 | | Convert the virtual machine to a Golden Template. | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After creating all the golden templates, you can run the automation process Automated Cloning and OS Customization, on page 300. After you run the automation process, you can configure Cisco MediaSense on the destination system. See Configure Cisco MediaSense, on page 673.

# Configure Cisco MediaSense



## Cisco MediaSense Primary

## Configure Cisco MediaSense Primary

### Before You Begin

If there is a value in the optional DNS_IP_NIC1 cell of the automation spreadsheet, configure the DNS server by adding the machine in forward and reverse lookup. For more information, see Configure DNS Server, on page 437.

### Procedure

**Step 1** Ensure that **Connect at Power On** is checked for the network adapters and the floppy drive and click **OK**.

**Step 2** Power on the Primary. 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 3** 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 4** 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

After rebooting, the VM installation is complete with all the parameters provided in the spreadsheet for the VM.

## Complete Setup for Primary Server

Follow this procedure to complete the setup for the primary server in any MediaSense deployment:

### Procedure

**Step 1** After you complete the installation procedure, the system automatically restarts. Sign in to MediaSense Administration for the primary server. `(https://<server>:8443/oraadmin)`
Welcome screen of the MediaSense First Server Setup wizard is displayed.

**Step 2** When you are ready to proceed, click **Next**.
The **Service Activation** screen is displayed.

**Step 3** The system internally verifies the IP address of this server and automatically begins enabling the MediaSense feature services in this server. Wait until all the features services show as enabled in the Service Activation window. After all the services are successfully enabled, click **Next**.

After you click **Next**, the **AXL Service Provider** screen appears.

**Step 4** Enter the AXL service provider (IP address) and the AXL administrator username and password in the respective fields for the Unified CM that should communicate with MediaSense and click **Next**, the **Call Control Service Provider** screen appears. The AXL authentication allows you to enter the Unified CM cluster and retrieve the list of Unified CM servers within that cluster.
The AXL administrator username may not be same as the Unified CM Administrator username for that cluster. Make sure to add the username for the AXL Administrator to the Standard Unified CM Administrators group and "Standard AXL API Access" roles in Unified CM.

**Step 5** Select and move the Unified CM IP address for Call Control Service from Available Call Control Service Providers window to **Selected Call Control Service Providers** window and click **Next**.

**Step 6** The MediaSense Setup Summary window appears with successfully configured services. Click Done to complete the initial setup for the primary server.
When you finish the post-installation process for any MediaSense server, you must access the Unified CM server for your deployment and you will need to configure the SIP trunk, route pattern, route group, route list, recording profile and end user.

You have now completed the initial setup of the primary server for MediaSense.

Before you install MediaSense on a secondary server or an expansion server, you must configure details for these servers on the primary server. You configure details for these servers using the MediaSense Administration user interface.

**Step 7** Login to **MediaSense Administration** > **API User Configuration**

**Step 8** Select the available Unified CM User and add it to MediaSense API Users list.
Using this user you can login to Search and Play.

### What to Do Next

Configure Incoming Call, on page 675.

## Configure Incoming Call

### Procedure

**Step 1** Login to Cisco MediaSense Administration page.

**Step 2** Goto **Incoming Call Configuration** page.

**Step 3** Click **Add**.

**Step 4** Enter recording profile number created in CUCM in **Address** field.

**Step 5** Choose **Record** from **Action** drop-down list.

**Step 6** Click **Save**.

# Cisco MediaSense Secondary

### Before You Begin

If there is a value in the optional DNS_IP_NIC1 cell of the automation spreadsheet, configure the DNS server by adding the machine in forward and reverse lookup. See Configure DNS Server, on page 437.

### Procedure

**Step 1** Ensure that **Connect at Power on** is checked for the network adapters and the floppy drive and click **OK**.

**Step 2** Power on the Secondary. 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 3** Click the **Console tab** for the VM. Log in to the secondary machine, using the credentials for the Administration User. The machine opens to the CLI interface.

**Step 4** Right-click the VM and choose **Edit settings** and uncheck **Connect at Power on for the floppy drive**. During the customization of the secondary node, the username and the password are modified as follows. The customer should change the password.

- Default Password for OS Administrator: cisco@123
- Application UserName: Administrator
- Default Password for Application User: cisco@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 theVM.

## Add Secondary Node

### Procedure

**Step 1** Login to the web portal of MediaSense

**Step 2** From the **System** menu on the left, select **MediaSense Server Configuration**.

**Step 3** In the **MediaSense Server Configuration** screen, click **Add MediaSense Server**.
The **Add MediaSense Server** screen in the primary node opens.

**Step 4** If your installation uses DNS suffixes, enter the hostname of the server that you want to add.

**Step 5** If your installation does not use DNS suffixes, enter the IP address of the server that you want to add.

**Step 6** Enter the description of the server that you want to add (Optional).

**Step 7** Enter the MAC address of the server that you want to add (Optional).

**Step 8** Click **Save**.

**Step 9** Click **Back to MediaSense Server List**.

MediaSense displays a confirmation message. You see the configuration details of the server that you added in the **MediaSense Server List**.

**Note** You can not assign the server type in this web page. You can assign the server type only during the post-installation procedure. Between the time that a new server is added to the MediaSense Server list and until the time that its post-installation is successfully completed, the type for the new server remains unknown.

## Configure Cisco MediaSense Secondary

### Before You Begin

If there is a value in the optional DNS_IP_NIC1 cell of the automation spreadsheet, configure the DNS server by adding the machine in forward and reverse lookup. See Configure DNS Server, on page 437.

### Procedure

**Step 1** In the client computer where the automation tool was run, navigate to `C:\GoldenTemplateTool_10\PlatformConfigRepository\MediaSense`.

**Step 2** Copy the file named `MEDIASENSE_SECONDARY_platformConfig.xml`.

**Step 3** Paste it to another location and rename it to `platformConfig.xml`.

**Step 4** Launch WinImage and select **File** > **New** > **1.44 MB** and click **OK**.

**Step 5** Drag and drop `platformConfig.xml`into WinImage.

a) Click **Yes** at the message asking if you want to inject the file

b) Select **File** > **Save** as and save the file as a Virtual Floppy Image with the filename `platformConfig.flp`.

**Tip** If drag and drop does not work, select **Image** > **Inject**.Then browse to the file.

**Step 6** Open vSphere infrastructure client and connect to the vCenter. Go to the customer ESXi host where the VMs are deployed.

**Step 7** Navigate to the Configuration tab and in the storage section right click on the Datastore and choose Browse Datastore.

**Step 8** Create the folder `CMS_SEC` and upload `platformConfig.flp` to it.

**Step 9** Edit the Virtual Machine settings for the Unified Communications Manager Subscriber VM.

**Step 10** On the **Hardware** tab, click the floppy drive, choose the radio button **Use The Existing Floppy Image in Datastore** and mount the `platformConfig.flp` from the `CMS_SEC` folder on the data store.

**Step 11** Ensure that **Connect at Power On** is checked for the network adapters and the floppy drive. Click **OK** and then power on the VM.
This begins the installation and customizes the installation based on the information in the `.flp` file.

**Step 12** If there is a value in the optional DNS_IP_NIC1 cell of the automation spreadsheet, configure the DNS server by adding the machine in forward and reverse lookup.

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

**Step 13** After you complete the installation 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.

After rebooting, the VM installation is complete with all the parameters provided in the spreadsheet for the VM.

### Complete Setup for Secondary Server

Follow this procedure to complete the setup for the secondary server in any MediaSense deployment:

#### Procedure

**Step 1** After you complete the installation procedure of the previous section, the system restarts automatically and you must sign in to MediaSense Administration for secondary servers. When you sign in, the **Welcome** screen of the MediaSense Secondary Server Setup wizard appears.

**Step 2** When you are ready to proceed, click **Next**.
You determine the type of server in this Welcome screen.

Select the server type **Secondary** and click **Next**. The **Service Activation** screen is displayed.

**Step 3** After the services are enabled, click **Finish** to complete the initial setup for a subsequent server.

The **MediaSense Setup Summary** window displays the result of the initial setup and MediaSense restarts. You have now completed the initial setup of a subsequent server. This subsequent server is ready to record.

Repeat this setup procedure for each expansion server in the cluster.

## Configure MediaSense Forking

- Provisioning Cisco Unified CM for Cisco MediaSense BIB Forking, on page 678
- Provisioning Cisco Unified Border Element for Cisco MediaSense CUBE Forking, on page 679
- Provisioning TDM Gateway for Media Forking, on page 686

### Provisioning Cisco Unified CM for Cisco MediaSense BIB Forking

| Sequence | Task | Done? |
|---|---|---|
| 1 | Set Up SIP Options, on page 746 | |
| 2 | Add SIP Trunks, on page 572 | |
| 3 | Add Route Pattern, on page 577 | |
| 4 | Set up Recording Profile, on page 751 | |
| 5 | Configure Device, on page 679 | |

| Sequence | Task | Done? |
|---|---|---|
| 6 | Disable iLBC, iSAC and g.722 for Recording Device , on page 751 | |
| 7 | Configure End User, on page 679 | |

### *Configure Device*

**Procedure**

**Step 1** Login to Cisco Unified Communication Domain Manager as provider.
**Step 2** Ensure that hierarchy is set to appropriate customer level.
**Step 3** Navigate to **Subscriber Management** > **Phones**.
**Step 4** Choose the phone from the list that you want to configure.
**Step 5** Choose **ON** from **Built-in Bridge** drop-down list to enable Built-in Bridge.
**Step 6** In **Lines** tab, choose **Automatic Call Recording Enabled** from **Recording Flag** drop-down list.
**Step 7** Enter **Recording Profile Name**.
**Note** Enter the exact name of recording profile created in CUCM.
**Step 8** Click **Save**.

### *Configure End User*

**Procedure**

**Step 1** Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.
**Step 2** Ensure that hierarchy is set to appropriate customer/site.
**Step 3** Navigate to **Subscriber Management** > **Subscribers**.
**Step 4** Click **Add**.
**Step 5** Enter unique **Userid** and **Last Name**, in **User** tab.
**Step 6** Enter **Password** and **Repeat Password**.
**Step 7** Click **Save**.

## Provisioning Cisco Unified Border Element for Cisco MediaSense CUBE Forking

- Provisioning Cisco Unified Border Element for Cisco MediaSense CUBE Forking for HCS Deployment Models, on page 680
- Provisioning Cisco Unified Border Element for Cisco MediaSense CUBE Forking for SCC Deployment Models, on page 683

*Provisioning Cisco Unified Border Element for Cisco MediaSense CUBE Forking for HCS Deployment Models*

| Sequence | Task | Done? |
|---|---|---|
| 1 | Setup Global Level , on page 680 | |
| 2 | Dial-Peer Level Setup , on page 681 | |
| 3 | Set Up CUBE Dial-Peers for MediaSense Deployments , on page 681 | |

Setup Global Level

### Procedure

**Step 1** Connect to your CUBE gateway using SSH or Telnet.

**Step 2** Enter the global configuration mode.

```
cube# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
cube(config)#
```

**Step 3** Enter VoIP voice-service configuration mode.

```
cube(config)# voice service voip
cube(config-voi-serv)#
```

**Step 4** Calls may be rejected with a 403 Forbidden response if Toll Fraud security is not configured correctly. The solution is to add the IP address as a trusted endpoint, or else disable the IP address trusted list authentication altogether using the following configuration entry:

```
cube(config-voi-serv)# no ip address trusted authenticate
```

**Step 5** Enable CUBE and CUBE Redundancy.

```
cube(config-voi-serv)# mode border-element
cube(config-voi-serv)# allow-connections sip to sip
cube(config-voi-serv)# sip
cube(config-voi-serv)# asymmetric payload full
cube(config-voi-serv)# video screening
```

In the example above, the final 3 lines are only required if video calls are to be passed through CUBE.

**Step 6** At this point, you will need to save the CUBE configuration and reboot CUBE.

**Caution** Be sure to reboot CUBE during off-peak hours.

a) Save your CUBE configuration.

```
cube# copy run start
```

b) Reboot CUBE.

```
cube# reload
```

**Step 7** After you reboot CUBE, configure the media class to determine which calls should be recorded.

```
cube(config-voi-serv)# media class 3
cube(config-voi-serv)# recorder parameter
cube(config-voi-serv)# media-recording 3000
```

**Step 8** Exit the VoIP voice-service configuration mode.

```
cube(config-voi-serv)# exit
```

**Step 9** Create one voice codec class to include five codecs (including one for video). These codecs will be used by the inbound and outbound dial-peers to specify the voice class.

```
cube(config)# voice class codec 3
cube(config)# codec preference 1 mp4a-latm
cube(config)# codec preference 2 g711ulaw
cube(config)# codec preference 3 g722-64
cube(config)# codec preference 4 g729br8
cube(config)# video codec h264
```

In the example above, the first codec preference and video codec definition are only required if AAC-LD/LATM media is part of the customer's call flow.

**Step 10** To simplify debugging, you must synchronize the local time in CUBE with the local time in Cisco MediaSense servers. For example, if you specify the NTP server as 10.10.10.5, then use the following command in CUBE:

```
cube(config)# ntp update-calendar
cube(config)# sntp server 10.10.10.5
```

Dial-Peer Level Setup

**Note** This information describes a sample configuration. CUBE may be deployed in multiple ways.

Each Cisco MediaSense deployment for CUBE contains three dial-peers:

- Inbound dial-peer: In this example, the unique name is 1000
- Outbound dial-peer: In this example, the unique name is 2000
- Forking dial-peer: In this example, the unique name is 3000

Before you begin this procedure, obtain the details for these three dial-peers from your CUBE administrator.

**Note** The order in which you configure these three dial-peers is not important.

Set Up CUBE Dial-Peers for MediaSense Deployments

This procedure provides an example of how to set up the three dial peers. The specific names and values used are for illustrative purposes only.

**Caution** This procedure is not a substitute for the actual CUBE documentation. It is a tutorial to provide detailed information about configuring CUBE for MediaSense. See your CUBE documentation at http://www.cisco.com/go/cube for the latest information.

### Procedure

**Step 1** Configure media forking on an inbound dial peer.

a) Assign a unique name to the inbound dial-peer. In this example, the name is set to '1000'.

```
cube(config)# dial-peer voice 1000 voip
```

The command places you in the dial-peer configuration mode to configure a VoIP dial-peer named '1000'.

b) Specify the session protocol for this inbound dial-peer as 'sipv2' (this value is not optional).
```
cube(config-dial-peer)# session protocol sipv2
```
This command determines if the SIP session protocol on the endpoint is up and available to handle calls. The session protocols and VoIP layers depend on the IP layer to give the best local address and use the address as a source address in signaling or media or both—even if multiple interfaces can support a route to the destination address.

c) Specify the SIP invite URL for the incoming call. In this example, we assume that inbound, recordable calls will have six digits. Here, we assign the first three digits as '123' and the last three digits are arbitrarily chosen by the caller (as part of the destination DN being dialed). This command associates the incoming call with a dial-peer.
```
cube(config-dial-peer)# incoming called-number 123...$
```

d) When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to apply the class to individual dial-peers. In this example, the tag used is '1'.
```
cube(config-dial-peer)# voice-class codec 1
```
This tag uniquely identifies this codec. The range is 1 to 10000.

e) If call is transferred, be sure to propagate the metadata to MediaSense.You can do so by enabling the translation to PAI headers in the outgoing header on this dial-peer.
```
cube(config-dial-peer)# voice-class sip asserted-id pai
```

f) Specify that everything that is going through the inbound dial-peer can be forked. Use the same number that you used to set up global forking (see Set up Global Level). In this example, the number media class is '3'.
```
cube(config-dial-peer)# media-class 3
```

g) Exit the configuration of this inbound dial-peer.
```
cube(config-dial-peer)# exit
cube(config)#
```

**Step 2** Configure the outbound dial-peer.

a) Assign a unique name to the outbound dial-peer. In this example, the name is set to '2000'.
```
cube(config)# dial-peer voice 2000 voip
```
The command places you in the dial-peer configuration mode to configure a VoIP dial-peer named '2000'.

b) Specify the session protocol for this outbound dial-peer as 'sipv2' (this value is not optional).
```
cube(config-dial-peer)# session protocol sipv2
```

c) Specify the destination corresponding to the incoming called number. In this example, it is '123...'.
```
cube(config-dial-peer)# destination-pattern 123...$
```

d) When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to apply the class to individual dial-peers. Use the same tag used for the inbound dial-peer. In this example, the tag used is '1'.
```
cube(config-dial-peer)# voice-class codec 1
```

e) Specify the primary destination for this call. In this example, we set the destination to 'ipv4:10.1.1.10:5060'.
```
cube(config-dial-peer)# session target ipv4:10.1.1.10:5060
```

f) Exit the configuration of this outbound dial-peer.
```
cube(config-dial-peer)# exit
cube(config)#
```

**Step 3** Configure the forking dial-peer.

a) Assign a unique name to the forking dial-peer. In this example, the name is set to '3000'.
```
cube(config)# dial-peer voice 3000 voip
```

The command places you in the dial-peer configuration mode to configure a VoIP dial-peer named '3000'. Optionally, provide a description for what this dial-peer does using an arbitrary English phrase.

```
cube(config-dial-peer)# description This is the forking dial-peer
```

b) Specify the session protocol for this forking dial-peer as 'sipv2' (this value is not optional).

```
cube(config-dial-peer)# session protocol sipv2
```

c) Specify an arbitrary destination pattern with no wildcards. Calls recorded from this CUBE will appear to come from this extension. (In the MediaSense Incoming Call Configuration table, this number corresponds to the address field.) In this example, we set it to '3000'.

```
cube(config-dial-peer)# destination-pattern 3000
```

d) When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to apply the class to individual dial-peers. Use the same tag used for the inbound dial-peer. In this example, it is '1'.

```
cube(config-dial-peer)# voice-class codec 1
```

e) Provide the IP address of one of the MediaSense expansion servers (if available) as a destination for the CUBE traffic. In this example, we use a MediaSense server at IP address 10.2.2.20.

**Note**
- Avoid using the primary or secondary MediaSense servers for this step as these servers carry the CUBE load and it is best to avoid adding load to the database servers.
- In Small contact center deployment model , provide the signaling IP address of CUBE(E) adjacency configured in the Perimeta SBC for Mediasense forking. See Add CUBE-MEDIASENSE FORK adjacency, on page 496

```
cube(config-dial-peer)# session target ipv4:10.2.2.20:5060
```

f) Set the session transport type (UDP or TCP) to communicate with MediaSense. The default is UDP. The transport protocol specified with the session transport command, and the protocol specified with the transport command, must be identical.

```
cube(config-dial-peer)# session transport tcp
```

g) Configure a heartbeat mechanism to monitor connectivity between end points. A generic heartbeat mechanism allows Cisco Unified Border Element to monitor the status of MediaSense servers or endpoints and provide the option of timing-out a dial-peer if it encounters a heartbeat failure.

**Note** If you have configured an alternate dial-peer for the same destination pattern, the call fails over to the next preferred dial-peer. Otherwise, the call is rejected. If you have not configured a fail over dial-peer, then do not configure options-keep alive.

```
cube(config-dial-peer)# voice-class sip options-keepalive
```

h) Prevent CUBE from sending multi part body in INVITE to MediaSense.

```
cube(config-dial-peer)# signaling forward none
```

i) Exit the configuration of this forking dial-peer.

```
cube(config-dial-peer)# exit
cube(config)#
```

j) Exit the configuration mode.

```
cube(config)# exit
cube#
```

k) Save your CUBE configuration.

```
cube# copy run start
```

*Provisioning Cisco Unified Border Element for Cisco MediaSense CUBE Forking for SCC Deployment Models*

| Sequence | Task | Done? |
|---|---|---|
| 1 | Setup Global Level , on page 680 | |

| Sequence | Task | Done? |
|---|---|---|
| 2 | Dial-Peer Level Setup , on page 681 | |
| 3 | Set Up CUBE Dial-Peers for Small Contact Center Deployment, on page 684 | |

Set Up CUBE Dial-Peers for Small Contact Center Deployment

The inbound dialpeer for MediaSense should be created for each sub customer . Follow the below steps to create the inbound dialpeer:

### Procedure

**Step 1** Configure media forking on an inbound dial peer.

a) Assign a unique name to the inbound dial-peer. In this example, the name is set to '1000'.
```
cube(config)# dial-peer voice 1000 voip
```
The command places you in the dial-peer configuration mode to configure a VoIP dial-peer named '1000'.

b) Specify the session protocol for this inbound dial-peer as 'sipv2' (this value is not optional).
```
cube(config-dial-peer)# session protocol sipv2
```
This command determines if the SIP session protocol on the endpoint is up and available to handle calls. The session protocols and VoIP layers depend on the IP layer to give the best local address and use the address as a source address in signaling or media or both—even if multiple interfaces can support a route to the destination address.

c) Specify the SIP invite URL for the incoming call. In this example, we assume that inbound, recordable calls will have six digits. Here, we assign the first three digits as '123' and the last three digits are arbitrarily chosen by the caller (as part of the destination DN being dialed). This command associates the incoming call with a dial-peer.
```
cube(config-dial-peer)# incoming called-number 123...$
```

d) When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to apply the class to individual dial-peers. In this example, the tag used is '1'.
```
cube(config-dial-peer)# voice-class codec 1
```
This tag uniquely identifies this codec. The range is 1 to 10000.

e) If call is transferred, be sure to propagate the metadata to MediaSense. You can do so by enabling the translation to PAI headers in the outgoing header on this dial-peer.
```
cube(config-dial-peer)# voice-class sip asserted-id pai
```

f) Specify that everything that is going through the inbound dial-peer can be forked. Use the same number that you used to set up global forking (see Set up Global Level). In this example, the number media class is '3'.
```
cube(config-dial-peer)# media-class 3
```

g) Exit the configuration of this inbound dial-peer.
```
cube(config-dial-peer)# exit
cube(config)#
```

**Step 2** Configure the forking dial-peer.

a) Assign a unique name to the forking dial-peer. In this example, the name is set to '3000'.
```
cube(config)# dial-peer voice 3000 voip
```

The command places you in the dial-peer configuration mode to configure a VoIP dial-peer named '3000'. Optionally, provide a description for what this dial-peer does using an arbitrary English phrase.

```
cube(config-dial-peer)# description This is the forking dial-peer
```

b) Specify the session protocol for this forking dial-peer as 'sipv2' (this value is not optional).

```
cube(config-dial-peer)# session protocol sipv2
```

c) Specify an arbitrary destination pattern with no wildcards. Calls recorded from this CUBE will appear to come from this extension. (In the MediaSense Incoming Call Configuration table, this number corresponds to the address field.) In this example, we set it to '3000'.

```
cube(config-dial-peer)# destination-pattern 3000
```

d) When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to apply the class to individual dial-peers. Use the same tag used for the inbound dial-peer. In this example, it is '1'.

```
cube(config-dial-peer)# voice-class codec 1
```

e) Provide the IP address of one of the MediaSense expansion servers (if available) as a destination for the CUBE traffic. In this example, we use a MediaSense server at IP address 10.2.2.20.

**Note**
- Avoid using the primary or secondary MediaSense servers for this step as these servers carry the CUBE load and it is best to avoid adding load to the database servers.
- In Small contact center deployment model , provide the signaling IP address of CUBE(E) adjacency configured in the Perimeta SBC for Mediasense forking. See Add CUBE-MEDIASENSE FORK adjacency, on page 496

```
cube(config-dial-peer)# session target ipv4:10.2.2.20:5060
```

f) Set the session transport type (UDP or TCP) to communicate with MediaSense. The default is UDP. The transport protocol specified with the session transport command, and the protocol specified with the transport command, must be identical.

```
cube(config-dial-peer)# session transport tcp
```

g) Configure a heartbeat mechanism to monitor connectivity between end points. A generic heartbeat mechanism allows Cisco Unified Border Element to monitor the status of MediaSense servers or endpoints and provide the option of timing-out a dial-peer if it encounters a heartbeat failure.

**Note** If you have configured an alternate dial-peer for the same destination pattern, the call fails over to the next preferred dial-peer. Otherwise, the call is rejected. If you have not configured a fail over dial-peer, then do not configure options-keep alive.

```
cube(config-dial-peer)# voice-class sip options-keepalive
```

h) Prevent CUBE from sending multi part body in INVITE to MediaSense.

```
cube(config-dial-peer)# signaling forward none
```

i) Exit the configuration of this forking dial-peer.

```
cube(config-dial-peer)# exit
cube(config)#
```

j) Exit the configuration mode.

```
cube(config)# exit
cube#
```

k) Save your CUBE configuration.

```
cube# copy run start
```

## Provisioning TDM Gateway for Media Forking

The following section will provide detailed guidelines on how to configure media recording for calls on TDM trunks. CUBE (E), being an integrated platform can provide TDM trunk connectivity and act as a session border controller at the same time.

For this solution to work, calls from the PSTN are looped back to itself thus creating an inbound VoIP SIP leg to the CUBE. It then sends the call to the call agent in the enterprise network creating an outbound VoIP SIP leg. Thus, the gateway is used to terminate the TDM leg, and originate an IP leg towards the call agent.

**Note** In this flow ,calls will effectively halve the stated capacity of the router, thus requiring twice as much router capacity for the same number of calls. If you intended to use the full capacity of the router for calls, you will need two routers. It is better to configure two routers for their individual purposes, rather than using both routers for both purposes.

Follow the below sequence to configure TDM gateway

| Sequence | Task | Done? |
|---|---|---|
| 1 | Configure translation rule and profile | |
| 2 | Configure loopback interface | |
| 3 | Configure media class | |
| 4 | Configure dial-peers | |

### Procedure

**Step 1** Configure translation rule and profile

a) Configure translation rules for the calling number (ANI) or called number (DNIS) digits for a voice call

```
voice translation-rule 1
rule 1 /^966//8966/
voice translation-rule 2
rule 2 /^8966//966/
```

The first rule defined is rule 1, in which 966 is the pattern that must be matched and replaced, and 8966 is the pattern that is substituted for 966.

b) Configure translation-profile

The translation rules replace a sub string of the input number if the number matches the match pattern, number plan, and type present in the rule

```
voice translation-profile prefix
translate called 1
voice translation-profile strip
translate called 2
```

Translation profile prefix will add prefix to the called number based on the translation rule 1.Similarly translation profile strip will remove the prefix from the called number based on the translation rule 2.

**Step 2** Configure loopback interface

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
```

**Step 3** Configure media class

Configure the media class to determine which calls should be recorded.

```
cube(config-voi-serv)# media class 3
cube(config-voi-serv)# recorder parameter
cube(config-voi-serv)# media-recording 20
```

**Step 4** Configure dial-peers

a) Configure the pots dial-peer for incoming PSTN call

```
dial-peer voice 1 pots
description Incoming dial peer for PSTN calls
translation-profile incoming prefix
incoming called-number 9660000001
port 0/2/1:23
```

b) Configure the voip dial-peer to loop back the incoming PSTN call.

```
dial-peer voice 8966 voip
description To loop incoming PSTN calls back to itself.
destination-pattern 89660000001
session protocol sipv2
session target ipv4:1.1.1.1 # loop back Ip address of the TDM gateway
session transport tcp
voice-class codec 1
dtmf-relay rtp-nte
no vad
```

c) Configure the inbound dial-peer for newly originated SIP call leg

```
dial-peer voice 89660 voip
description inbound dial-peer for the newly originated SIP call leg
translation-profile incoming strip
session protocol sipv2
session target sip-server
session transport tcp
incoming called-number 89660000001
voice-class codec 1
dtmf-relay rtp-nte
no vad
```

d) Configure the outbound dial-peer for newly originated SIP call

```
dial-peer voice 9660 voip
description Outgoing dial peer for looped call to contact center
destination-pattern 9660000001
session protocol sipv2
session target ipv4:192.1.10.1 #IP address of CVP server
session transport tcp
voice-class codec 1
dtmf-relay rtp-nte
media-class 3
no vad
```

e) Configure the outbound dial-peer for forking call leg

```
dial-peer voice 20 voip
description Forking leg to MediaSense server.
```

```
preference 1
destination-pattern 99999
signaling forward none
session protocol sipv2
session target ipv4:192.1.9.1 #Ip address of MediaSense server
session transport tcp
voice-class sip options-keepalive
```

# 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, on page 692
- Using the CLI to Install the Cisco Unified SIP Proxy Release 8.5.7 Licenses, on page 693
- Using the Licensing Portal to Obtain Licenses for Additional Features or Applications, on page 692


### 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 694 |
| Configure Gateway | Configure Gateway, on page 701 |
| Configure Unified CVP | Configure Unified CVP, on page 701 |
| Configure Unified Call Manager though UCDM | Configure Cisco Unified Communications Manager , on page 702 |

# Configure Cisco Unified SIP Proxy

Perform the following procedures to configure Unified SIP Proxy

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 1 | | Configure Networks, on page 694 | |
| 2 | | Configure Triggers, on page 695 | |
| 3 | | Configure Server Groups, on page 695 | |
| 4 | | Configure Route Tables, on page 696 | |
| 5 | | Configure Route Policies, on page 697 | |
| 6 | | Configure Route Triggers, on page 698 | |

For complete configuration details of Cisco Unified SIP Proxy, see Full Configuration for Cisco Unified SIP Proxy, on page 698

***Table 76: 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 76: Example CUSP Deployment Details, on page 694.

**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 76: Example CUSP Deployment Details, on page 694.

**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 77: Example Route Table***

| Key | Description | Host / Server Group (FQDN) | Network |
|---|---|---|---|
| 4000 | Agent Extension | ccm.hcsdc1.icm<br>**Note** For Small Contact Center deployment model use Perimeta SBC signaling address: 10.10.10.49 | 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 |

| Key | Description | Host / Server Group (FQDN) | Network |
|---|---|---|---|
| 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 77: Example Route Table, on page 696.
**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 76: Example CUSP Deployment Details, on page 694.
**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

```
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 702
- Add Trunk to CUSP, on page 703

### 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** In the **CTI Server A** text box, enter **A side CTIOS server IP Address**; in the **CTI Server Port A** text box, enter **42027** as the port number.
**Step 9** In the **CTI Server B** text box, enter **B side CTIOS server IP address**; in the **CTI Server Port B** text box, enter **43027** as the port number.
**Step 10** 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 706
- Configure Avaya PG, on page 706

# 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 HCS-CC_11.0(1)_CCDM-CCE-CVP_vmv9_v1.0.ova. | Follow the procedure Open Virtualization Format Files, on page 54 . |
| 2 | | Create the virtual machine for the Unified CCE Avaya PG | Follow the procedure Create Virtual Machines, on page 251. |
| 3 | | Install Microsoft Windows Server | Follow the procedure Install Microsoft Windows Server 2012 R2 Standard Edition, on page 252. |
| 4 | | Install Antivirus Software | Follow the procedure Install Antivirus Software, on page 253. |
| 5 | | Install the Unified Contact Center Enterprise | Follow the procedure Install Unified Contact Center Enterprise, on page 254. |
| 6 | | Convert the virtual machine to a template. | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, you can configure the Avaya PG server on the destination system. See Configure Avaya PG, on page 706.

# 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 338. |
| 2 | | Verify the Machine in Domain | Follow the procedure Verify the Machine in Domain, on page 334. |
| 3 | | Configure Unified CCE Encryption Utility | Follow the procedure Configure Unified CCE Encryption Utility, on page 340. |

| Sequence | Done? | Tasks | Notes |
|---|---|---|---|
| 4 | | Add Avaya PG from Configuration Manager | Follow the procedure Add Avaya PG, on page 707. |
| 5 | | Setup Avaya PG | Follow the procedure Setup Avaya PG, on page 708. |
| 6 | | Configure CTI server | Follow the procedure Configure CTI Server, on page 329. |
| 7 | | Configure CTI OS server | Follow the procedure Configure CTI OS Server, on page 332. |
| 8 | | Configure Avaya ACD | Follow the procedure in section 2 of ACD Configuration. |
| 9 | | Verify Cisco Diagnostic Framework Portico | Follow the procedure Verify Cisco Diagnostic Framework Portico, on page 346. |
| 10 | | Cisco SNMP Setup | Follow the procedure Cisco SNMP Setup, on page 334. |

# 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.

# 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, on page 709
- Create Service, on page 710
- Configure Translation Route, on page 710
- Configure Script, on page 711


### Enable Network Transfer Preferred

Perform the below 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**
Displays **Configuration Manager** window.

**Step 2** Expand **Tools** > **Explorer Tools** > **PG Explorer**.

**Step 3** Choose appropriate PG from the list and expand the PG.

**Step 4** Choose appropriate PIM from the list.

**Step 5** Goto **Routing Client** tab, check **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

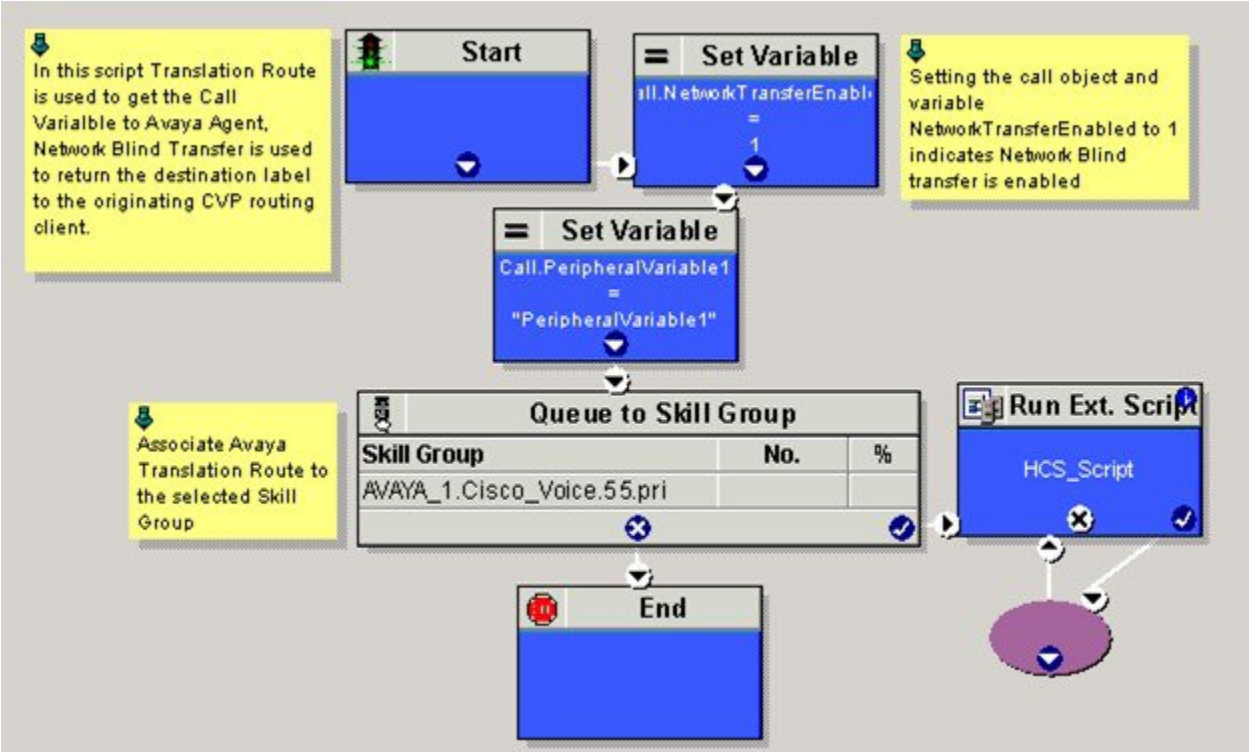
**Step 1** In Unified CCE Admin Workstation Server, navigate to **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**
Displays **Configuration Manager** window.
**Step 2** Expand **Tools** > **Explorer Tools** > **Translation Route Explorer**.
**Step 3** In **Translation Route** tab:
a) Enter **Name**.
b) Choose **DNIS** in **Type** drop-down list.
**Step 4** Click **Add Route**.
**Step 5** In **Route** tab:
a) Enter **Name**
b) Choose newly created service from **Service** drop-down list.
**Step 6** Click **Add Peripheral Target**
**Step 7** In **Peripheral Target** tab:
a) Enter **DNIS**
**Note** DNIS should be same as label.
b) Choose **Network Trunk Group** from drop-down list.
**Step 8** Click **Add Label**.
**Step 9** In **Label** tab:
a) Choose **Routing Client** from drop-down list.
b) Enter **Label**.
**Note** Post route VDN should be created as label for CVP routing client

**Step 10** Click **Save**.

### Configure Script

Following illustration explains to configure scripts.

***Figure 82: Configure Scripts***




# Cisco Virtualized Voice Browser



## 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 `VB_11.0_vmv8_v2.5.ova` | See Open Virtualization Format Files, on page 54. |
| 2 | | Create the virtual machine for Cisco Virtualized Voice Browser. | Follow the procedure that is documented in, Create Virtual Machines, on page 251. |
| 3 | | Install Cisco Virtualized Voice Browser. | Follow the procedure for installing VOS applications for golden templates. See Install Unified Communications Voice OS based Applications, on page 264. |
| 4 | | Convert the virtual machine to a Golden Template. | Follow the procedure Convert the Virtual Machine to a Golden Template, on page 255. |

After you create all golden templates, you can run the automation process ( Automated Cloning and OS Customization, on page 300). After you run the automation process, configure Cisco Virtualized Voice Browser. See Configure Cisco Virtualized Voice Browser, on page 713.

# Configure Unified CVP

- Add Cisco Virtualized Voice Browser, on page 713
- Associate Dialed Number Pattern, on page 713

## Add Cisco Virtualized Voice Browser

### Procedure

**Step 1** Login CVP operation console.
**Step 2** Navigate to **Device Management** > **Gateway**.
**Step 3** Enter **IP Address** and **Hostname** of unified 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 **Route to Device** drop-down list, select Virtualized Voice Browser IP.
**Step 5** Click **Save**.
**Step 6** Click **Deploy**.

# Configure Cisco Virtualized Voice Browser


- Access Virtualized VB Administration Web Interface, on page 714
- Access Virtualized VB Serviceability Web Page , on page 714
- Add a SIP Trigger , on page 714
- Configure Agent Greeting, on page 715
- Configure Whisper Announcement, on page 715
- Configure ASR and TTS, on page 715
- Configure Courtesy Callback for Cisco VVB, on page 717

## 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 603
- Configure Unified CCE, on page 607
- Configure Unified Communications Manager, on page 612

## Configure Whisper Announcement

### Procedure

**Step 1** Login Voice Browser Administration page.
**Step 2** Navigate to **Application** > **Application Management**.
**Step 3** Ensure **ringtone** application is listed and associated with the trigger `919191*`.

### What to Do Next

- Configure Unified CVP, on page 613
- Configure Unified CCE, on page 614

## Configure ASR and TTS

Virtualized Voice Browser supports ASR and TTS through two subsystems. Follow the below procedure to configure ASR and TTS subsystems:

- Configure ASR Subsystem, on page 716

• Configure TTS Subsystem, on page 716

## 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.

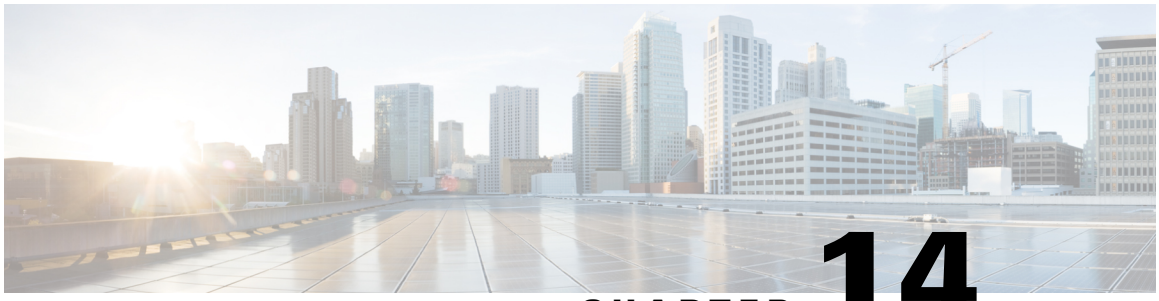
**Step 2** Select **Application** > **Application Management**.

**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, see Configure Courtesy Callback, on page 592



CHAPTER 14

# Remote Deployment Options



# Global Deployments

Global Deployments allows Service Providers to deploy remote data centers with centralized management. The following Global deployment topologies are supported with standard HCS deployment models.


- Remote CVP Deployment, on page 719
- Remote CVP and CUCM Deployment, on page 724


## Remote CVP Deployment

The Remote CVP deployment requires the following servers deployed at the remote Data centers. The maximum RTT with central controller over the WAN is restricted up to 400ms.

**Prerequisite: Standard HCS deployment model at the Core Data center.**


- Unified CVP Servers for Remote CVP Deployment, on page 719
- Unified CCE Servers for Remote CVP Deployment, on page 722
- Configure Cisco IOS Enterprise Voice Gateway, on page 369


### 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 Data center.

#### Configure Remote CVP Server

To configure the remote CVP servers, See Configure Unified CVP Server, on page 348

### 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 348 | |
| 2 | Enable Unified CVP Operations Console, on page 360 | |
| 3 | Configure Unified CVP Call Server for Remote Deployment, on page 720 | |
| 4 | Configure Unified CVP VXML Server Component, on page 361 | |
| 5 | Configure Unified CVP Reporting Server, on page 361 | |
| 6 | Configure Unified CVP Media Server, on page 362 | |
| 7 | Install Unified CVP licenses, on page 363 | |
| 8 | Configure Gateways, on page 363 | |
| 9 | Add Unified CCE Devices, on page 365 | |
| 10 | Add Unified Communications Manager Devices, on page 365 | |
| 11 | Add Unified Intelligence Center Devices , on page 366 | |
| 12 | Transfer Scripts and Media Files, on page 364 | |
| 13 | Configure SNMP, on page 364 | |
| 14 | Configure SIP Server Group for Remote Deployment, on page 721 | |
| 15 | Configure Dialed Number Patterns, on page 367 | |

*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 Data center.

### Modify Unified CCE Router

See Configure the Unified CCE Router, on page 405 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 ICM/CC Node Manager until all ICM components are installed.

# Remote CVP and CUCM Deployment

The Remote CVP and CUCM deployment requires the following servers deployed at the remote Data centers. The maximum RTT with central controller over the WAN is restricted up to 400ms. Use the Golden Template tool to deploy the remote CCE, CVP, CUCM and Finesse servers from the Golden templates.

Prerequisite: Standard HCS deployment model at the Core Data center

- Configure Unified CVP, on page 347
- Unified CCE Servers for Remote CVP and CUCM Deployment, on page 724
- Configure Unified Communications Manager, on page 375
- Configure Cisco IOS Enterprise Voice Gateway, on page 369
- Configure Cisco Finesse, on page 392

## Unified CCE Servers for Remote CVP and CUCM Deployment

Use the Golden Template tool to deploy the remote CCE Generic PG from the Golden templates. This section explains the procedures to configure Unified CCE servers at Remote Data center.

### Modify Unified CCE Router

See Configure the Unified CCE Router, on page 405 and modify the value in **Enable Peripheral Gateways** dialog box by incrementing the value.

### Add Remote Generic PG Using Unified CCE Configuration Manager

Complete the following procedure to add remote Generic 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 Generic 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 Generic 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 Generic PG routing clients.

## Configure Generic 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 ICM/CC Node Manager until all ICM components are installed.

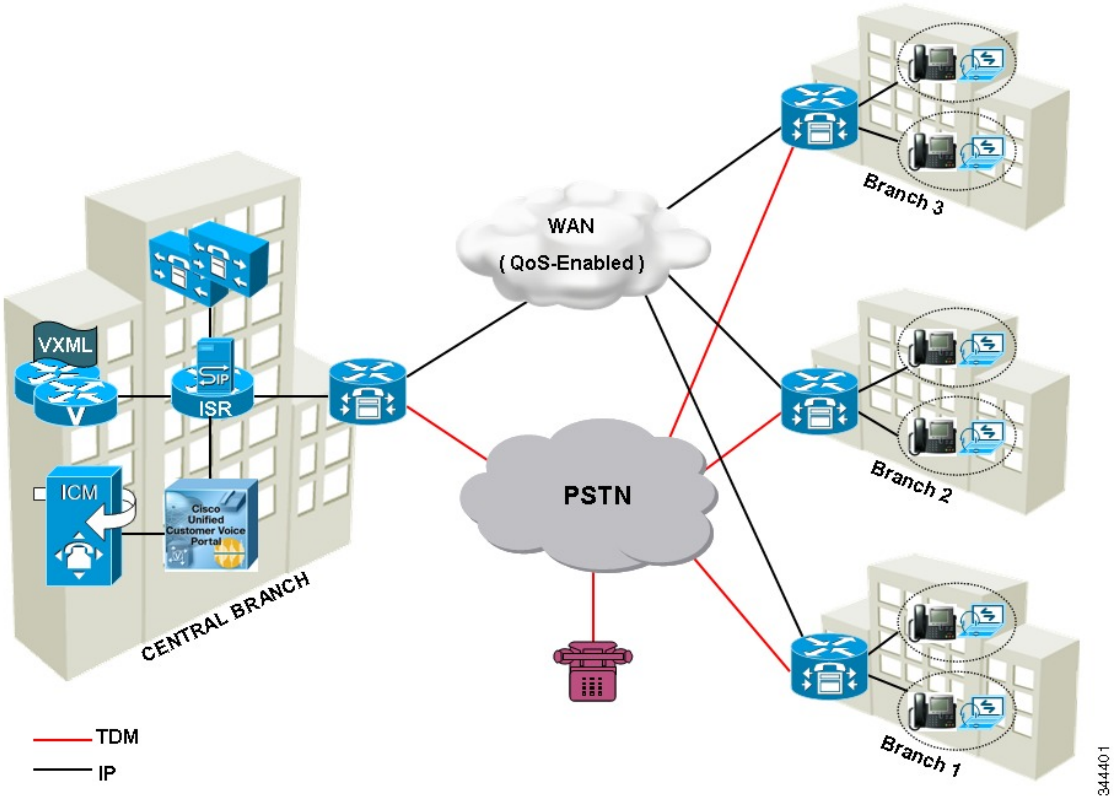
# Configure Local Trunk

Complete the following procedures to configure Local Trunk.

- Configure Unified CVP, on page 727
- Configure Unified Communications Manager, on page 728

The following figure shows the Local Trunk configuration.

***Figure 83: 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 728
- Verify Application User Roles, on page 729
- Configure SIP Profile for LBCAC, on page 729
  - Deploy SIP Trunk for Central Branch , on page 730
  - Deploy SIP Trunk for Local Branches, on page 730
- Configure Location Bandwidth Manager, on page 730


## 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 581.

## 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 759.

**Step 2** Create a SIP Trunk towards the CVP/SIP proxy server.

**Note**
1. In step 5 of creating SIP Trunk procedure, select **Run On All Active Unified CM Nodes** check-box.
2. Associate the new SIP profile with the SIP trunk. See, Create SIP Trunk, on page 759.

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 577.

### 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**
1. In step 5 of creating SIP Trunk procedure, select **Run On All Active Unified CM Nodes** check-box.
2. Associate the new SIP profile with the SIP trunk. See, Create SIP Trunk, on page 759.

## Configure Location Bandwidth Manager

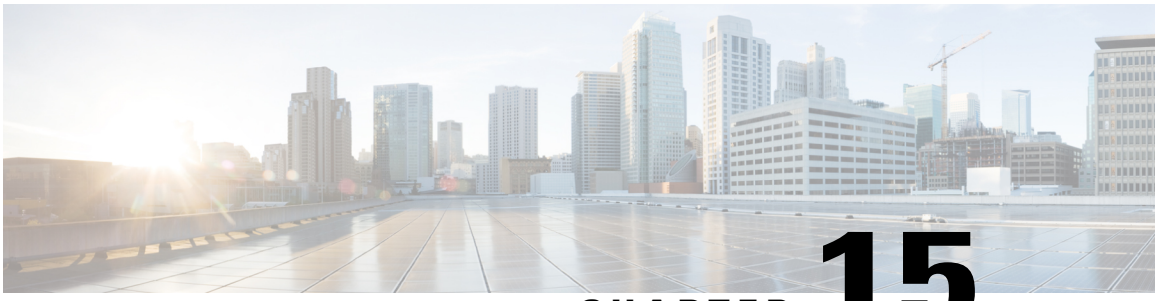
#### Procedure

**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 15

# Solution Serviceability



# Monitor System Performance

Monitoring system performance is one way to help maintain the system. Use vCenter to monitor the following critical Cisco HCS 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 78: 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. | 60% |
| | CPU Usage in MHz (Average) | The CPU usage average in MHz. | 95 percentile is less than 60% of the total MHz available on the VM.<br>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 memory from 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 RAM swap. | 0 |

| Category | Counter | Description | Threshold |
|---|---|---|---|
| Disk | Disk Usage (Average) | Disk Usage = Disk Read rate + Disk Write rate | Ensure that your SAN is configured to handle this amount of disk I/O. |
| | Disk Usage Read rate | The rate of reading data from the disk. | Ensure that your SAN is configured to handle this amount of disk I/O. |
| | Disk Usage Write rate | The rate of writing data to the disk. | Ensure that your SAN is configured to handle this amount of disk I/O. |
| | Disk Commands Issued | The number of disk commands issued on this disk in the period. | Disk IO per second<br>IOPS = Disk Commands Issued / 20<br>Ensure that your SAN is configured to handle this amount of disk I/O. |
| | Stop Disk Command | The number of disk commands aborted on this disk in the period. The disk command aborts 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 79: 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 Used by VMKernel | Memory Used by VMKernel | 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 |
| | SwapUsed | 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<br>IOPS = Disk Commands Issued / 20 |
| | Disk Commands Aborts | Number of disk commands aborted on this disk in the period.<br>Disk command aborts 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.<br>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.

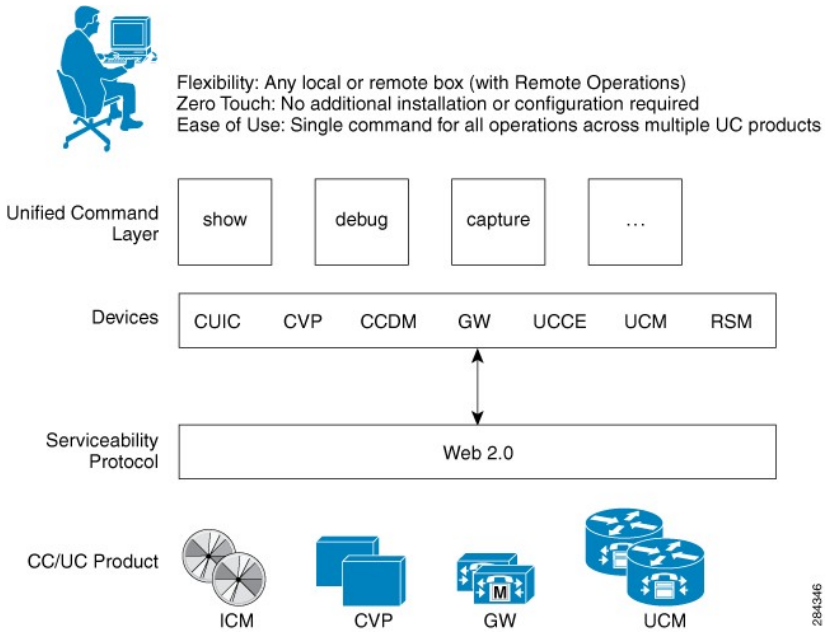
For example, you can use the System CLI if you suspect a call is not handled correctly. In this case you use the **show tech-support** system command to collect data and send the data to Cisco support.

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.
- Executes as a Windows scheduled job.

The following figure shows the devices and Cisco Unified products that the Unified System CLI interacts with.

***Figure 84: 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 736
- Run Unified System CLI in the Remote Machine, on page 737

# 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

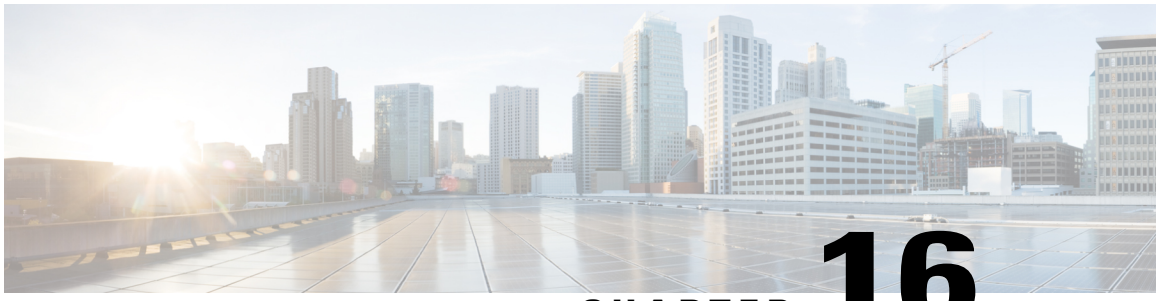
**Step 1** Install the Unified CVP Operations Console Resource Manager (ORM) component on a separate network management virtual machine to ensure that performance of critical components is not affected during log collections.

**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 365
- Add Unified Communications Manager Devices, on page 365
- Add Unified Intelligence Center Devices , on page 366
- Configure Unified CVP Reporting Server, on page 361

**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 16

# 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** Verify the change of Domain in Administrator and Workstation Database (AWDB) and instance name in all Unified CCE components.

# Supported Gadgets and API

• Supported API for HCS, on page 741

# Supported API for HCS

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.

**Note** Agents can only perform attribute update.

The following tables show the supported API for the HCS deployment model.

***Table 80: Supported API for HCS***

| API | Create | Read | Update | Delete |
|---|---|---|---|---|
| Active Directory Domain | | x | | |
| Agent | | x | x (only attribute assignment) | |
| Agent State Trace | | x | x | |
| Asynchronous | x | | x | x |
| Attribute | x | x | x | x |
| Bucket Interval | x | x | x | x |
| Congestion Control | | x | x | |
| Context Service Configuration | | x | x | |
| Context Service Registration | | x | x | |
| Deployment Type Info | | x | x | |
| Machine Inventory | 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 |
| Scan | | | x | |

| API | Create | Read | Update | Delete |
|---|---|---|---|---|
| Serviceability | | x | | |
| Status | | x | | |

# Supported Gadgets for HCS

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 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 |
| Context Service | | x | x | |
| Deployment | 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 | |
| System Information | | 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

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 configured 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 the 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 750. Unified CCE defines the user ID as pguser.

**Step 4** Enter **cisco** in the Password field.

**Note** If you change this user ID or password in Unified CCE, you must also change the Unified Communications Manager application user configuration.

**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 745.
**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 745.
**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.hcscc.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 for MediaSense, 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

Cisco MediaSense recording sessions using the following supported Codecs:

- Audio recordings: g.711 (aLaw or μLaw) or g.729(a or b) codecs

- Video recordings: h.264 baseline (48k Hz sampling rate only) codecs

**Caution** Cisco MediaSense does not support internet Low Bit Rate Codec (iLBC) or internet Speech Audio Codec (iSAC). Consequently, you must disable these features in Unified CM before you proceed with the Cisco MediaSense configuration.

### 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 754.

## 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, on page 759
- Create SIP Trunk, on page 759

## 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 493.

**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 deployments with less than 1250 users in a CM Cluster
2. An MoH server is deployed as standalone node (TFTP/MoH Server) for HCS deployments with more than 1250 users in a CM Cluster


- Configure Music on Hold Server Audio Source, on page 760
- Configure Service Parameters for Music on Hold , on page 760
- Modify Phone configuration for Music On Hold , on page 761


### *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**

# Provision Cisco Unified Communication Manager for Optional Cisco Components


- Configure RSM, on page 761
- Configure MediaSense, on page 768


## Configure RSM

Configure the Cisco Remote Silent Monitoring (RSM) Server in distributed mode, through Cisco Unified Communications Manager.


- Configure Simulated Phone , on page 761
- Set Up Login Pool Simphone , on page 766
- Create RSM User Group , on page 766
- Create RSM Application User , on page 767
- Set Up Agent Phone Device , on page 767


### Configure Simulated Phone

You must determine how many simulated phones( also called as simphones) to assign to each Unified Communications Manager cluster. Each cluster must have a number of simphones greater than or equal to the maximum number of agents that will be simultaneously monitored through RSM for the cluster. This section provides the following information:

- To configure the simphone device dependencies, to create a Unified Communications Manager group, RSM region, device pool, route partition, and calling search space.
- To create the simphone devices and assign MAC addresses.
- To add line DNs to the simphone devices.

The procedures describe how to create one simphone and its associated line DN. Additional simphones can be created by using Unified Communications Manager's super copy feature or by creating a batch file.

**Note** You must be logged in to the Administration interface of a Unified Communications Manager cluster before you can configure your simphones as described in the following procedure.

*Create Simphone Device Dependencies*

### Procedure

**Step 1** To create a Unified Communications Manager group:

a) Navigate to **System** > **Cisco Unified CM Groups**.
b) Click **Add New**.
c) Enter **RSMSimPhone** for the Unified Communications Manager group name.
d) Assign the necessary Unified Communications Managers to the group. If you have more than one Unified Communications Manager in the cluster, select the subscribers to be part of the group but do not select the publisher.
e) Click **Save**.

**Step 2** To create a simphone region:

a) Navigate to **System** > **Region Information** >**Region**.
b) Click **Add New**.
c) Enter **RSMSimPhone** for the region name, adding prefix or suffix naming conventions, if required.
d) Click **Save**.
e) Add relationships with agent phones to the regions in your environment. Note that calls between simphones and agent phones must use the G.729 codec.
f) Click **Save**.

**Step 3** To create a simphone device pool:

a) Navigate to **System** > **Device Pool**.
b) Click **Add New**.
c) Enter **RSMSimPhone** for the device pool name, adding prefix or suffix naming conventions, if required.
d) Select the **RSMSimPhone** Communications Manager group from the **Device Pool Settings** > **Cisco Unified Communications Manager Group** drop-down list.
e) Select **RSMSimPhone** region from the **Roaming Sensitive Settings** > **Region** drop-down list.
f) Enter the remaining parameters, according to your configuration (for example, date/time group and user locale.)
g) Click **Save**.

**Step 4** To create a Device Feature Group

a) Choose **General Administration** > **Feature Groups**.
b) Select the customer instance. For example, Customer_1.
c) Click **Add** and enter the following values:

1. Name - **CC-RSM**.
2. Description - **Contact Center RSM Group**.
3. Outbound calls limitations - **National24Hrs-Standard-wCC**.
4. Call forward limitations - **Default CoS**.
5. Voicemail Template - **Basic voicemail service type**.

6 Inbound call options - **Allow two Direct Dial Inward lines**.
7 Number of extensions or lines - **Two Numbers: DDI or Extension**.
8 Idle URL: None.

d) Under the Value Add panel, select features as required.
e) Under Common Line Settings (Line Feature) panel, check the Contact Center Agent Line feature.
f) Under Private line settings (phone line feature) panel, check **Recording Option**,**Recording Profile**, **Call waiting busy trigger**, **Max calls waiting**
g) Under Handset panel check **Built-in Bridge** check-box.
h) Click **Submit**.

**Step 5** To create a simphone route partition:
a) Navigate to **Call Routing > Class of Control > Partition**.
b) Click **Add New**.
c) Enter **RSMSimPhone** in the text box, adding prefix or suffix naming conventions, if required.
d) Click **Save**.

**Step 6** To create a simphone calling search space:
a) Navigate to **Call Routing > Class of Control > Calling Search Space**.
b) Click **Add New**.
c) Enter **RSMSimPhone** for the calling search space name, adding prefix or suffix naming conventions, if required.
d) Select the route partition containing the agent phones that RSM will monitor from the Available Partitions selection box, and move them to the Selected Partitions selection box.
e) Click **Save**.

**Note** For 4000 agent deployment, repeat this procedure for the second PG.

### *Create Simphone Device*

**Procedure**

**Step 1** Navigate to **Device** > **Phone**.
**Step 2** Click **Add New** to create a new phone device.
**Step 3** Select **Cisco 7941** for the phone type, then click **Next**.
**Step 4** Choose **SIP** for the device protocol, then click Next. The Phone Configuration page appears.
**Step 5** Enter the MAC address.
**Step 6** Enter the parameters:

| Parameter | Setting |
|---|---|
| Device Pool | RSMSimPhone |
| Phone Button Template | Standard 7941 SIP |
| Location | Relevant environment |
| Built In Bridge | Off |

| Parameter | Setting |
|---|---|
| Phone Personalization | Disabled |
| Allow Device Control through CTI | Yes |
| Presence Group | Standard |
| Device Security Profile | Cisco 7941 Standard Non-Secure SIP |
| SIP Profile | Standard |
| Maximum Calls | 2 (two) |
| Busy Trigger | 1 (one) |

**Step 7** Click **Save**.
The simphone device is created.

**Note** Parameters not listed can be left to their default settings.

### *Associate a Line DN to Simphone Device*

**Procedure**

**Step 1** Click the **Line [1] - Add a new DN** link in the Association Information panel.

**Step 2** Enter the parameters. Parameters that are marked with an asterisk (*) are optional; those not listed may be left to their default settings.

| Parameter | Setting |
|---|---|
| Directory Number | 5040 |
| Route Partition | RSMSimPhone |
| CTI Control | Yes |
| Voice Mail Profile | No voicemail |
| Calling Search Space | RSMSimPhone |
| Presence Group | Standard Presence group |
| User Hold MOH Audio Source * | 1-SampleAudioSource |
| Network Hold MOH Audio Source * | 1-SampleAudioSource |
| Line1 on Device <MAC ADDR><br>Monitoring Calling Search Space (CSS) | RSM SimPhone |

**Step 3** Click **Save**. Your first simphone and its associated line DN is now configured.

### *Use Simphone Bulk Administration Tool*

To use the Bulk Administration Tool , you must first import the comma-separated-values template (from either the RSM installation CD or installed instance of RSM), and then edit it, as applicable, in a spreadsheet application such as Microsoft Excel.

#### Procedure

**Step 1** Import the rsmsimphones.csv spreadsheet template file from the installed instance of RSM (located in the C:\CiscoRSM\Extras directory).

**Step 2** Open the file in a spreadsheet application, then add or remove rows in the file to match the number of simphone devices you need to create (default rows = 75).

**Step 3** If adding new rows, be sure to modify the data in the Device Name and Directory Number 1 columns to increment sequentially from the previous row in the list for the columns (for example, 00005E000001, 00005E000002, 00005E000003, and so on, for the simphone MAC addresses, and 5040, 5041, 5042, and soon, for the line DNs).

**Step 4** Verify that the Device Pool, Partition 1, Line CSS 1 and Monitoring Calling Search Space 1 settings are correct for your environment (refer to Tables 3-1 and 3-2, above).

**Note** No changes are required if you entered RSMSimPhone for the Simphone Device Pool, Partition, and CSS settings during your simphone configuration.

**Step 5** Navigate to **Bulk Administration** > **Upload/Download Files**.

**Step 6** Click **Add New**.

**Step 7** Click **Browse** and navigate to the rsmsimphones.csv file that you previously downloaded and modified.

**Step 8** Choose **Phones** from the Select the Target drop-down list.

**Step 9** Select **Insert Phones - All Details** from the **Select Transaction Type** drop-down list.

**Step 10** Click **Save**. The file is uploaded to the system.

**Step 11** Navigate to **Bulk Administration** > **Phones** > **Insert Phones**.

**Step 12** Select **Insert Phones-All Details**, and then select **rsmsimphones.csv** from the **File Name** drop-down list.

**Step 13** Enter **Insert RSMSimPhones** for the **Job Description**, and then select **Run Immediately**.

**Step 14** Click **Submit**.
The file is imported into the system.

**Step 15** Navigate to **Bulk Administration** > **Job Scheduler** to verify that the job status is either Processing or Completed.

**Step 16** When the job status is **Completed**, navigate to **Device** > **Phones** and review the phones that you have created.

**Step 17** Enter **SEP00005E** in the **Find Phone** text box, then click **Find**.
The simphone devices that you have created will appear in the returned results.

### Set Up Login Pool Simphone

The first five simphone devices that are created for each cluster are automatically assigned to the VLEngine login pool. The login pool performs a test login to CTI OS when a caller is authenticated by RSM, to support the VLEngine authentication mechanism.

Because CTI OS logins are performed on these simphone devices, they must be associated with the pguser account on each Unified Communications Manager cluster. They must also have Cisco Unified Intelligent Contact Management Enterprise device targets created for them, as described below.

**Note** Device target creation is required only for Unified CCE. You do not need to create device targets if you use Cisco Unified System Contact Center Enterprise (Unified SCCE) or if the Cisco Unified CCE PG type is IPCC.

Follow this procedure to associate a pguser.

#### Procedure

**Step 1** Navigate to **User Management** > **Application User**.
**Step 2** Click **Find** to display all application users. Locate then click the pguser account for your cluster.
**Step 3** Select the first five simphone devices in the **Device Information** > **Available Devices** list box.
**Step 4** Click the down arrow above the box to move the devices to the **Controlled Devices** list box. Click **Save**.

### Create RSM User Group

A RSM user group must be created for each cluster used by RSM. This provides the user with the necessary system permissions that would otherwise be available only to the Unified Communications Manager Super Administrator.

Follow this procedure to add an RSM user group to a cluster.

#### Procedure

**Step 1** Navigate to **User Management** > **User Settings** > **Access Control Group**.
**Step 2** Click **Add New**.
**Step 3** Enter **Remote Silent Monitoring** in the Name field, then click **Save**.
**Step 4** Navigate to **User Management** > **User Group**.
**Step 5** Click **Find** to display all user groups.
**Step 6** Click the icon in the Roles column for the Remote Silent Monitoring group.
**Step 7** Click **Assign Role to Group**. A new window appears.
**Step 8** Click **Find** to display all group roles.
**Step 9** Select the following roles:

- Standard CTI Allow Call Monitoring

- Standard CTI Allow Control of All Devices
- Standard CTI Enabled

**Step 10** Click **Add Selected**. The User Group Configuration page appears.

**Step 11** Click **Save**.

### Create RSM Application User

You must create an application user named rsmuser on each Unified Communications Manager cluster for RSM. This user derives its permissions from the user group that was previously created. The rsmuser must be associated with all simphones in the cluster (with the exception of simphones in the login pool). It must also be associated with all agent phones that RSM can monitor.

Simphones in the login pool (that is the first five simphone devices) must be associated with the cluster's pguser, while all other simphones not in the login pool are associated with the RSM application user.

**Note**

- For 4000 agent deployment with two PGs, create two Application Users, one for each of the agent PGs.
- Whenever a new non-login-pool simphone or agent device is created, it must be associated with the RSM user.

Follow this procedure to add an RSM application user to a cluster.

#### Procedure

**Step 1** Navigate to **User Management** > **Application User**.

**Step 2** Click **Add New** to create a new application user.

**Step 3** Enter rsmuser for the user ID.

**Step 4** Enter a password. Ensure that the password is alphanumeric and does not contain any special characters.

**Step 5** Associate the user with all simphone devices in the cluster (except for the login pool devices) by selecting those devices in the Available Devices section and moving them to the Controlled Devices section.

**Step 6** Associate all agent phone devices to be monitored through RSM.

**Step 7** From the Permissions Information window, click **Add to User Group**, and then add the user to the Remote Silent Monitoring group, as previously created.

**Step 8** Click **Save**.

### Set Up Agent Phone Device

To configure an agent phone device to be monitored by RSM, ensure the following:

- Edit the device using the Cisco Unified Communications Manager Administration interface and enable the Built-In Bridge setting
- Associate the device with the rsmuser, similar to the way it is associated with the pguser.

### Configure MediaSense


- Set Up Trunk , on page 745
- Set Up SIP Options, on page 746
- Set Up Route Pattern , on page 747
- Set up Recording Profile, on page 751
- Configuring Device, on page 751
- Disable iLBC, iSAC and g.722 for Recording Device , on page 751


# Base Configuration Parameters


- Base Configuration Parameters for 500 and 1000 Agent Deployment, on page 768
- Base Configuration Parameters for 4000 Agent Deployment, on page 775
- Base Configuration Parameters for Small Contact Center Agent Deployment, on page 780
- Base Configuration Parameters for 12000 Agent Deployment, on page 783


## Base Configuration Parameters for 500 and 1000 Agent Deployment

Following is the list of load base configuration parameters for 500 and 1000 agent deployment.


1 PG Explorer, on page 769
2 ICM Instance Explorer , on page 769
3 Network VRU Explorer, on page 769
4 System Information, on page 770
5 Expanded Call Variable List, on page 770
6 Network VRU Script List, on page 772
7 Agent Desk Settings List, on page 773
8 Application Instance List, on page 773
9 Media Class for Multi-Channel, on page 774
10 Media Routing Domain, on page 774
11 Network VRU Mapping, on page 774
12 Agent Targeting Rule , on page 774

13 Outbound Dialer, on page 775

## PG Explorer

| PG Explorer | Type of PIM | Routing Client Name |
|---|---|---|
| **Generic PG** | CUCM | CUCMPG1 |
| | VRU | CVPPG1A |
| | VRU | CVPPG1B |
| | VRU | CVPPG2A |
| | VRU | CVPPG2B |
| **MR PG** | MediaRouting | Multichannel |
| | MediaRouting | Outbound |

**Note**

- Select the option Enable Agent Reporting for CUCMPG1 Routing Client.
- Enter the Primary and Secondary CTI address and port information in the Unified Communications Manager PG for the Cisco Unified WIM and EIM feature.
- In **Agent Distribution** tab, add a site name for **Administration and Data Server** site name field.

## ICM Instance Explorer

- Go to the Instance and select the Network VRU to Type 10 Network VRU in the Customer definition tab.

## Network VRU Explorer

- **CVP_Network_VRU - Type10**

| Serial Number | Network VRU Label | Routing Client Name |
|---|---|---|
| 1 | 7777777777 | CVPPG1A |
| 2 | 7777777777 | CVPPG1B |
| 3 | 7777777777 | CVPPG2A |
| 4 | 7777777777 | CVPPG2B |
| 5 | 8881111000 | CUCMPG1 |
| 6 | 6661111000 | Outbound |

- **MR_Network_VRU - Type 2**

## System Information

- Expanded Call Context: Enabled
- Minimum Correlation number: 1001
- Maximum Correlation number: 9999
- Retain script versions:5

## 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.<br>**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 hangs up. |
| user.cim.activity.id | FALSE | FALSE | 30 | Needed for all types of WIM and EIM activities. |
| user.wim.customer.name | FALSE | FALSE | 30 | Needed for chat, callback, and delayed callback activities. |

| Name | Enabled | Persistent | Maximum Length | Description |
|---|---|---|---|---|
| user.cisco.cmb | FALSE | FALSE | 30 | Needed for callback, and delayed callback activities. |
| user.cisco.cmb.callclass | FALSE | FALSE | 30 | Needed for callback, and delayed callback activities. |
| user.media.id | FALSE | FALSE | 36 | A number identifying a call to the ICM 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. |

## Network VRU Script List

| Name | Network VRU | VRU Script Name | Time out (Sec) | Configuration Parameter | Customer | Interruptible | Override |
|---|---|---|---|---|---|---|---|
| VXML_Server | Select Type 10 CVP VRU | GS, Server, V | 180 | __ | hcs | Unchecked | Unchecked |
| VXML_Server_ Interruptible | Select Type 10 CVP VRU | GS, Server, V, interrupt | 9000 | __ | hcs | Checked | Unchecked |
| VXML_Server_ Noninterruptible | Select Type 10 CVP VRU | GS, Server, V , nointerrupt | 9000 | __ | hcs | Unchecked | Unchecked |
| AgentGreeting | Select Type 10 CVP VRU | PM, -a | 180 | none | hcs | Unchecked | Unchecked |

| Name | Network VRU | VRU Script Name | Time out (Sec) | Configuration Parameter | Customer | Interruptible | Override |
|---|---|---|---|---|---|---|---|
| GreetingMenu _1_to_9 | Select Type 10 CVP VRU | M, press _1_thru_9 _greeting, A | 180 | 1-9 | hcs | Checked | Unchecked |
| Greeting SubMenu | Select Type 10 CVP VRU | M, press1-press2-press3,A | 180 | 1-3 | hcs | Checked | Unchecked |
| Greeting _Not_Found | Select Type10 CVP VRU | PM, no _greeting _recorded, A | 180 | Y | hcs | Checked | Unchecked |
| GreetingReview | Select Type10 CVP VRU | PM,-a,A | 180 | Y | hcs | Checked | Unchecked |
| T10_GS_AUDIUM | Select Type 10 CVP VRU | GS,Server,V, FTP | 180 | ,,,,,,,,,Y | hcs | Checked | Unchecked |
| CIMExternal ApplicationScript | MR_network_VRU | CIMExternal ApplicationScript | 180 | - | hcs | Unchecked | Unchecked |

**Note** For 4000 Agent Deployment, map CIMExternalApplicationScript to MR_Network_VRU1.

## Agent Desk Settings List

Name: Default_Agent_Desk_Settings

## Application Instance List

| | Name | Application Type | Permission Level | Application Key |
|---|---|---|---|---|
| Application Instance Multichannel | MultiChannel | Other | Full read/write | cisco123 |
| Application Instance CCDM | CCDM | Cisco Voice | Full read/write | cisco123 |

## Media Class for Multi-Channel

- Media classes are created with following names:

  Name : CIM_BC

  Name : CIM_EIM

  Name: CIM_OUTBOUND

  Name: CIM_WIM

- Set the following values in task section:

  Life : 300

  Start Time out : 30

  Max duration : 28800

## Media Routing Domain

| | Interruptible | Calls in Queue (Max) | Max per call type | Max time in queue |
|---|---|---|---|---|
| Cisco_BC | Unchecked | 5000 | - | - |
| Cisco_EIM | Checked | 15000 | - | - |
| Cisco_EIM_OUTBOUND | Checked | 5000 | - | - |
| Cisco_WIM | Unchecked | 5000 | - | - |

**Note** Set the **Max Per Call Type** and **Max Time in Queue** values as per your requirement.

## Network VRU Mapping

- In the Advanced tab of PG explorer for Unified CVP Routing client - Map the **CVP_Network_VRU - Type10**
- In the Advanced tab of PG explorer for Multichannel and outbound routing clients - Map the **MR_Network_VRU - Type 2**

## Agent Targeting Rule

| Attribute | |
|---|---|
| Name | AgentExtensions |

| Attribute | |
|---|---|
| Peripheral | CUCM_PG_1 |
| Rule Type | Agent Extension |
| Routing Client | All routing clients |
| Extension Range | 000 - 999<br>0000 - 9999<br>00000 - 99999<br>000000 - 999999<br>0000000 - 9999999<br>00000000 - 99999999<br>000000000 - 999999999<br>0000000000 - 9999999999 |

### Outbound Dialer

| Dialer Name | Peripheral Name |
|---|---|
| Peripheral | CUCM_PG_1 |
| Dialer Name | SIP_DIALER |
| Enable | YES |
| ICM peripheral name | CUCM_PG_1 |
| Hangup Delay(1-10) | 1 Sec |
| Port Throttle | 10 |

# Base Configuration Parameters for 4000 Agent Deployment

Following is the list of load base configuration parameters for 4000 agent deployment.

1. PG Explorer, on page 776
2. ICM Instance Explorer, on page 777
3. Network VRU Explorer, on page 777
4. System Information, on page 778
5. Expanded Call Variable List, on page 778
6. Network VRU Script List, on page 778
7. Agent Desk Settings List, on page 778

## PG Explorer

PG Explorer

| PG | Type of PIM | Routing Client Name |
|---|---|---|
| Unified Communication Manager PG1 | CUCM | CUCMPG1 |
| Unified Communication Manager PG2 | CUCM | CUCMPG2 |
| Unified Voice Response (VRU) PG | VRU | CVPRC01 |
| | VRU | CVPRC02 |
| | VRU | CVPRC03 |
| | VRU | CVPRC04 |
| | VRU | CVPRC05 |
| | VRU | CVPRC06 |
| | VRU | CVPRC07 |
| | VRU | CVPRC08 |
| | VRU | CVPRC09 |
| | VRU | CVPRC10 |
| | VRU | CVPRC11 |
| | VRU | CVPRC12 |
| | VRU | CVPRC13 |
| | VRU | CVPRC14 |
| | VRU | CVPRC15 |
| | VRU | CVPRC16 |
| Media Routing (MR) PG 1 | MediaRouting | Multichannel |
| | MediaRouting | Outbound1 |
| Media Routing (MR) PG 2 | MediaRouting | Outbound2 |

**Note**

- Enter the Primary and Secondary CTI address and port information in the Unified Communications Manager PGs for the Cisco Unified WIM and EIM feature.
- In **Agent Distribution** tab, add **Administration and Data Server** site name.

## ICM Instance Explorer

- ICM Instance Explorer for 4000 agent deployment is similar to ICM Instance Explorer of 500 and 1000 agent deployment. See ICM Instance Explorer , on page 769.

## Network VRU Explorer

- CVP Network VRU - Type 10

| Serial Number | Network VRU Label | Routing Client Name |
|---|---|---|
| 1 | 7777777777 | CVPRC01 |
| 2 | 7777777777 | CVPRC02 |
| 3 | 7777777777 | CVPRC03 |
| 4 | 7777777777 | CVPRC04 |
| 5 | 7777777777 | CVPRC05 |
| 6 | 7777777777 | CVPRC06 |
| 7 | 7777777777 | CVPRC07 |
| 8 | 7777777777 | CVPRC08 |
| 9 | 7777777777 | CVPRC09 |
| 10 | 7777777777 | CVPRC10 |
| 11 | 7777777777 | CVPRC11 |
| 12 | 7777777777 | CVPRC12 |
| 13 | 7777777777 | CVPRC13 |
| 14 | 7777777777 | CVPRC14 |
| 15 | 7777777777 | CVPRC15 |
| 16 | 7777777777 | CVPRC16 |
| 17 | 8881111000 | CUCMPG1 |
| 18 | 8881111000 | CUCMPG2 |

| Serial Number | Network VRU Label | Routing Client Name |
|---|---|---|
| 19 | 6661111000 | Outbound1 |
| 20 | 6661111000 | Outbound2 |

- **MR_Network_VRU1 - Type 2**
- **MR_Network_VRU2 - Type 2**

## System Information

System Information for base configuration for 4000 agent deployment is similar to 500 and 1000 agent deployment. See System Information, on page 770.

## Expanded Call Variable List

Base configuration expanded call variable list for 4000 agent deployment is similar to 500 and 1000 agent deployment , See Expanded Call Variable List, on page 770 .

## Network VRU Script List

Network VRU base configuration for 4000 Agent is similar to 500 and 1000 Agent Base Configuration, See Network VRU Script List, on page 772.

## Agent Desk Settings List

Name: Default_Agent_Desk_Settings

## Application Instance List

Application instance list is similar to 500 and 1000 agent deployment. See Application Instance List, on page 773

## Media Class for Multi-Channel

- Media classes are created with following names
  - Name : CIM_BC
  - Name : CIM_EIM
  - Name: CIM_OUTBOUND
  - Name : CIM_WIM
- Set the following values in task section

- Life : 300
- Start Time out : 30
- Max duration : 28800

## Media Routing Domain

Media Routing Domain is similar to Media Routing Domain of 500 and 1000 agent deployment. See Media Routing Domain, on page 774.

## Network VRU Mapping

- In the **Advanced** tab of PG Explorer for Unified CVP Routing client - Map the **CVP_Network_VRU-Type10**.
- I In the **Advanced** tab of PG Explorer for multichannel and outbound routing clients - Map the **MR_Network_VRU-Type 2**.

## 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

| Dialer Name | Peripheral Name for PG1 | Peripheral Name for PG2 |
|---|---|---|
| Peripheral | CUCM_PG_1 | CUCM_PG_2 |
| Optional Filter | NONE | NONE |
| Dialer Name | SIP_DIALER1 | SIP_DIALER2 |
| Enable | YES | YES |
| ICM peripheral name | CUCM_PG_1 | CUCM_PG_2 |
| Hangup Delay(1-10) | 1 Sec | 1 Sec |
| Port Throttle | 10 | 10 |

# Base Configuration Parameters for Small Contact Center Agent Deployment

Following is the list of load base configuration parameters for small contact center agent deployment.



## PG Explorer

| PG | Type of PIM | Routing client Name |
|---|---|---|
| Unified Communication Manager PG1 | CUCM | CUCMPG1 |

| PG | Type of PIM | Routing client Name |
|---|---|---|
| Unified Voice Response (VRU) PG | VRU | CVPRC01 |
| | VRU | CVPRC02 |
| | VRU | CVPRC03 |
| | VRU | CVPRC04 |
| | VRU | CVPRC05 |
| | VRU | CVPRC06 |
| | VRU | CVPRC07 |
| | VRU | CVPRC08 |
| | VRU | CVPRC09 |
| | VRU | CVPRC10 |
| | VRU | CVPRC11 |
| | VRU | CVPRC12 |
| | VRU | CVPRC13 |
| | VRU | CVPRC14 |
| | VRU | CVPRC15 |
| | VRU | CVPRC16 |

**Note**

- Select **PG Explorer > Agent Distribution**, select **Enable Agent Reporting for CUCMPG Routing Client** option. Enter site name for **Administration and Data Server**
- Enter Primary and Secondary CTI address, port information in Unified Communications Manager PG for the Cisco Unified Email and Web Interface Management feature.

## ICM Instance Explorer

- ICM Instance is similar to ICM Instance Explorer of 500 and 1000 agent deployment. See ICM Instance Explorer , on page 769

## Network VRU Explorer

CVP Network VRU - Type 10

| Serial Number | Network VRU Label | Routing Client Name |
|---|---|---|
| 1 | 7777777777 | CVPRC01 |

| | | |
|---|---|---|
| 2 | 7777777777 | CVPRC02 |
| 3 | 7777777777 | CVPRC03 |
| 4 | 7777777777 | CVPRC04 |
| 5 | 7777777777 | CVPRC05 |
| 6 | 7777777777 | CVPRC06 |
| 7 | 7777777777 | CVPRC07 |
| 8 | 7777777777 | CVPRC08 |
| 9 | 7777777777 | CVPRC09 |
| 10 | 7777777777 | CVPRC10 |
| 11 | 7777777777 | CVPRC11 |
| 12 | 7777777777 | CVPRC12 |
| 13 | 7777777777 | CVPRC13 |
| 14 | 7777777777 | CVPRC14 |
| 15 | 7777777777 | CVPRC15 |
| 16 | 7777777777 | CVPRC16 |
| 17 | 8881111000 | CUCMPG1 |

- MR_Network_VRU - Type 2

## System Information

System Information for base configuration is similar to 500 and 1000 agent deployment. See System Information, on page 770.

## Expanded Call Variable List

Base configuration expanded call variable list is similar to 500 and 1000 agent deployment , See Expanded Call Variable List, on page 770 .

## Network VRU Script List

Network VRU base configuration is similar to 500 and 1000 agent base configuration, See Network VRU Script List, on page 772.

## Agent Desk Settings List

Name: Default_Agent_Desk_Settings

## Application Instance List

| | Name | Application Type | Permission Level | Application Key |
|---|---|---|---|---|
| Application Instance Multichannel | MultiChannel | Other | Full read/write | cisco123 |
| Application Instance CCDM | CCDM | Cisco Voice | Full read/write | cisco123 |

## Network VRU Mapping

In the **Advanced** tab of PG Explorer for Unified CVP Routing client - Map the **CVP_Network_VRU-Type10**.

# Base Configuration Parameters for 12000 Agent Deployment

Following is the list of load base configuration parameters for 12000 agent deployment contact center agent deployment.



## PG Explorer

| PG | Type of PIM | Routing Client Names |
|---|---|---|
| Unified CommunicationManager PG1 | CUCM | CUCMPG1 |

| PG | Type of PIM | Routing Client Names |
|---|---|---|
| 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, CVPRC02 … CVPRC16 |
| Unified Voice Response (VRU) PG2 | VRU | CVPRC17, CVPRC18 … CVPRC32 |
| Unified Voice Response (VRU) PG3 | VRU | CVPRC33, CVPRC34 … CVPRC48 |
| Media Routing (MR) PG 1 | MediaRouting | Multichannel |
| | MediaRouting | Outbound1 |
| Media Routing (MR) PG 2 | MediaRouting | Outbound2 |
| Media Routing (MR) PG 3 | MediaRouting | Outbound3 |
| Media Routing (MR) PG 4 | MediaRouting | Outbound4 |
| Media Routing (MR) PG 5 | MediaRouting | Outbound5 |
| Media Routing (MR) PG 6 | MediaRouting | Outbound6 |

**Note**

- Enter the Primary and Secondary CTI address and port information in the Unified Communications Manager PGs for the Cisco Unified WIM and EIM feature.
- In **Agent Distribution** tab, add **Administration and Data Server** site name.

## ICM Instance Explorer

- ICM Instance is similar to ICM Instance Explorer of 500 and 1000 agent deployment. See ICM Instance Explorer , on page 769

## Network VRU Explorer

- CVP Network VRU - Type 10

| Serial Number | Network VRU Label | Routing Client Name |
|---|---|---|
| 1 | 7777777777 | CVPRC01, CVPRC02 … CVPRC48 |
| 2 | 8881111000 | CUCMPG1,CUCMPG2 … CUCMPG6 |
| 3 | 6661111000 | Outbound |

- MR_Network_VRU1 - Type 2
- MR_Network_VRU2 - Type 2

## System Information

System Information for base configuration is similar to 500 and 1000 agent deployment. See System Information, on page 770.

## Expanded Call Variable List

Base configuration expanded call variable list is similar to 500 and 1000 agent deployment , See Expanded Call Variable List, on page 770 .

## Network VRU Script List

Network VRU base configuration is similar to 500 and 1000 agent base configuration, See Network VRU Script List, on page 772.

## Agent Desk Settings List

Name: Default_Agent_Desk_Settings

## Application Instance List

Application instance list is similar to 500 and 1000 agent deployment. See Application Instance List, on page 773

## Media Class for Multi-Channel

Media Class for Multi-Channel is similar to 500 and 1000 agent deployment model. See,Media Class for Multi-Channel, on page 774

## Media Routing Domain

Media Routing Domain is similar to Media Routing Domain of 500 and 1000 agent deployment. See Media Routing Domain, on page 774.

## Network VRU Mapping

- In the **Advanced** tab of PG Explorer for Unified CVP Routing client - Map the **CVP_Network_VRU-Type10**.
- I In the **Advanced** tab of PG Explorer for multichannel and outbound routing clients - Map the **MR_Network_VRU-Type 2**.

## 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 |
| Extension Range | 000 - 999<br>0000 - 9999<br>00000 - 99999<br>000000 - 999999<br>0000000 - 9999999<br>00000000 - 99999999<br>000000000 - 999999999<br>0000000000 - 9999999999 |

## Outbound Dialer

| Dialer Name | Peripheral Name for PG |
|---|---|
| Peripheral | CUCM_PG_1, CUCM_PG_2 … CUCM_PG_6 |
| Optional Filter | NONE |
| Dialer Name | SIP_DIALER1, SIP_DAILER2 … SIP_DAILER6 |
| Enable | YES |

| Dialer Name | Peripheral Name for PG |
|---|---|
| ICM peripheral name | CUCM_PG_1, CUCM_PG_2 … CUCM_PG_6 |
| Hangup Delay(1-10) | 1 Sec |
| Port Throttle | 10 |

# 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 and Unmount ISO Files

**Upload ISO image to data store:**

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

**Mount the ISO image:**

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

**Unmount the ISO image:**

1. Right-click the VM in the vSphere client and select **Edit virtual machine settings**.
2. Click **Hardware** and select **CD|DVD Drive 1**.
3. Uncheck **Connect at power on** (Device status panel, upper right).

# 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

# Automation Tool Spreadsheet

To complete the automation spreadsheet for import, use the information provided in the table below. The import automation script requires this information to import the virtual machines to the customer ESXi host.The table describes the values of each virtual server and associated properties.

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

***Table 81: Complete Automation Spreadsheet Columns for Import***

| Column | Description | Example |
|---|---|---|
| CREATEVM | Select **YES** to create a VM.<br>Select **NO** to ignore. | YES |
| OPERATION | Leave Blank. | Leave Blank |
| CUSTOMIZATION | Select **YES** to apply values in the spreadsheet to the imported server.<br>Select **NO** if you do not have the values at the time you complete the spreadsheet.<br>If you do have the values but set to **NO**, the values will not be applied. | YES |
| SOURCE_HOST_IP | The IP address or fully qualified name of the ESXi host where Template is created | xx.xx.xx.xx |
| SOURCE_DATASTORE_NAME | The name of Datastore where Template is created. | datastore2(1) |
| SOURCE_VMNAME | Leave blank. | Leave blank. |
| GOLDEN_TEMPLATE_NAME | Enter the name for the golden template. | GTCS-1A |

| Column | Description | Example |
|---|---|---|
| NEW_VM_NAME | The name for the new VM. Should not contain spaces or special characters. Maximum of 32 characters. | CallServerSideA |
| DEST_HOST_IP | The IP address or fully qualified name of the ESXi Host for the new VM. | xx.xx.xxx.xxx |
| DEST_DATASTORE_NAME | The name of the Datastore for the new VM. | datastore2(1) |
| PRODUCT_VERSION | Currently this field is applicable only for Cisco Unified Communications Manager. | ?? 10.0(x)? |
| COMPUTER_NAME | The NET BIOS name for the new computer. Maximum 15-characters. Do not use special characters. | Demo-CallSrvA |
| WORK_GROUP | Dropdown:<br>**YES** adds the VM to a WorkGroup and enables WORK_GROUP_NAME.<br>**NO** adds the VM to a domain and enables DOMAIN_NAME,<br>DOMAIN_USER, and DOMAIN_PASSWORD. | NO |
| WORK_GROUP_NAME | Enter the Workgroup name. Used only if WORK_GROUP is set to **YES**. | NA |
| DOMAIN_NAME | Enter the Domain name. Used only if WORK_GROUP is set to **NO** | |
| TIME_ZONE_LINUX_AREA | Drop-down selection of the timezone area to be set Unified CM. For the United States of America, select *America*. | America |
| TIME_ZONE_LINUX_LOCATION | Drop-down selection of the timezone location to be set for Unified CM, CUIC, or Finesse. | Eastern |
| TIME_ZONE_WINDOWS | Drop-down selection of the timezone to be set for the Unified CVP and Unified CCE VMs. | (GMT-05:00) Eastern Time (US & Canada) |

| Column | Description | Example |
|---|---|---|
| DOMAIN_USER | The user name for a domain user with privileges to add the new computer to the domain. Enabled only if WORK_GROUP is set to **NO**. | DOMAIN\Username |
| DOMAIN_PASSWORD | The password for the package123 domain user. Enabled only if WORK_GROUP is set to **NO**. | package123 |
| PRODUCT_KEY | The valid Windows OS product key in the format xxxxx-xxxxx-xxxxx-xxxxx-xxxxx. | ZZZM2-Y330L-HH123-99Y1B-GJ20B |
| OWNER_NAME | The full name of the owner.<br>*Administrator* and *Guest* are not allowable names.<br>This is a mandatory field for OS_TYPE Windows 2012. | LabAdmin |
| ORGANIZATION_NAME | The Organization Name to be set for Unified CM, CUIC, or Finesse. | MyName |
| ORGANIZATION_UNIT | The Organization Unit to be set for Unified CM, CUIC, or Finesse. | MyUnit |
| ORGANIZATION_LOCATION | The Organization Location to be set for Unified CM, CUIC, or Finesse. | MyCity |
| ORGANIZATION_STATE | The Organization State to be set for Unified CM, CUIC, or Finesse. | MyState |
| ORGANIZATION_COUNTRY | Drop-down selection of the Organization Country to be set for Unified CM, CUIC, or Finesse. | United States of America |
| NTP_SERVER | The IP Address of the NTP server. | xx.xx.xxx.xxx |
| NIC_NUM | Values in the field are pre-populated based on VM_TYPE field and are protected. Values are “1” or “2”. | 2 |
| SUB_NET_MASK_NIC1 | A valid subnet mask (IPv4 address) for NIC 1. | xx.xx.xxx.xxx |
| IP_ADDRESS_NIC1 | A valid IPv4 address for NIC 1. | xx.xx.xxx.xxx |

| Column | Description | Example |
|---|---|---|
| DNS_ALTERNATE_NIC1 | A valid IPv4 address for the alternate DNS for NIC1. | xx.xx.xxx.xxx |
| DEFAULT_GATEWAY_NIC1 | A valid Default gateway (IPv4 address) for NIC1. | xx.xx.xxx.xxx |
| DNS_IP_NIC1 | A valid IPv4 address for the primary DNS for NIC1. | xx.xx.xxx.xxx |
| IP_ADDRESS_NIC2 | A valid IPv4 address for NIC 2.<br>Valid only if the value in the NIC_NUM fields is 2. | xx.xx.xxx.xxx |
| SUB_NET_MASK_NIC2 | A valid subnet mask (IPv4 address) for NIC 2. For Unified CCE VMs only. | 255.255.255.255 |
| DNS_IP_NIC2 | A valid IPv4 address for the primary DNS for NIC2. For Unified CCE VMs only. | xx.xx.xxx.xxx |
| DNS_ALTERNATE_NIC2 | A valid IPv4 address for the alternate DNS for NIC2. For Unified CCE VMs only. Must differ from the address of the primary DNS for NIC2. (Optional) | xx.xx.xxx.xxx |
| VM_NETWORK | Leave Blank | Leave Blank |

# 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**.

# Glossary

**CoW**

Clustering over the WAN

**CTI OS**

CTI Object Server

**DNS**

Domain Name System

**ESXi**

VMware server virtualization software (includes the hypervisor)

**HA**

High Availability

**HCS**

Hosted Collaboration Solution

**HDS**

Historical Data Server

**IIS**

Internet Information Services

**IVR**

Interactive Voice Response

**JTAPI**

Java Telephony Application Programming Interface

**NTP**

Network Time Protocol

**NTFS**

New Technology File System

**OAMP**

Operations Administration Maintenance Provisioning

**OVA**

Open Virtual Archive

**OVF**

Open Virtualization Format

**PG**

Peripheral Gateway

**PIM**

Peripheral Interface Manager

**PSTN**

Public Switched Telephone Network

**RAID**

Redundant Array of Independent Disks

**SAN**

Storage Area Network

**SIP**

Session Initiation Protocol

**TDM**

Time Division Multiplexing

**UC**

Unified Communications

**VM**

Virtual Machine

**VOS**

Voice Operating System

**VRU**

Voice Response Unit

# INDEX

## N



## P



## R



## S



## T



## U



## V



## W