Solution Design Guide for Cisco Unified Contact Center Express, Release 12.5(1) SU2

First Published: 2022-04-11

Last Modified: 2023-06-26

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

CONTENTS

PREFACE

Preface ix

Change History ix

About This Guide ix

Audience ix

Conventions x

Related Documents xi

Documentation and Support xii

Documentation Feedback xii

CHAPTER 1

Cisco Unified Contact Center Solutions 1

Unified Contact Center Express Solution 1

CHAPTER 2

Unified CCX Reference Designs 3

Introduction to the Unified CCX Solution Reference Designs 3

Unified CCX General Rules for Design 5

Reference Designs 6

Single-Server Non-High Availability Reference Design 6

Two-Server High Availability Reference Design 6

Other Design Considerations 6

Mobile and Remote Access 8

Multiple Cisco Unified CCX Clusters Integrated with a Single Cisco Unified Communications Manager Cluster 8

CHAPTER 3

Contact Center Express Solutions Overview 11

Overview 11

Unified CCX Components 11

Unified CCX Licensing 12
Features 17
Agent Interfaces 17
Cisco Finesse Agent Desktop Features 18
Cisco Finesse IP Phone Agent Features 20
Cisco Finesse Supervisor Desktop Features 21
Agent Device Selection 22
Inbound Voice 22
IVR Ports 24
Inbound Voice Packaged Components 24
Unified CCX Outbound Dialer 31
High Level Components 31
Functional Description 32
Direct Preview Outbound 33
Outbound Progressive and Predictive Dialer 34
Outbound IVR and Agent 35
Scalability 36
Call Flow Description 36
Deployment Guidelines 39
Unified CCX Chat 40
Deployment Scenario 1: Customer Web Site in Demilitarized Zone (DMZ) 40
Deployment Scenario 2: Customer Web Site in Public Cloud or Domain 41
Unified CCX Chat Features 41
Group Chat 43
Unified CCX Web Chat 43
Facebook Messenger Integration 44
Unified CCX Agent Email 45
Agent Email Features 46
Reporting 48
Unified Intelligence Center 48
Finesse Reports 52
Wallboards 53
Recording 53
Webex Quality Management and Compliance Recording 54

Workforce Management 55
Home Agent with Extend and Connect 56
Deployment Guidelines 59
Remote Agent Over Broadband 59
VPN-less Access to Finesse Desktop 60
Supported Reverse-Proxy Deployment Models 60
Security Guidelines for Reverse-Proxy Deployment 63
Expressway Support 67
Reporting 67
Configuration APIs 67
Remote Expert Mobile 67
Post Call Treatment 67
Caller ID Support 67
E.164 Support 68
Single Sign-On 69
SAML 2.0 Authentication 69
Elements Used in SAML 2.0 69
Cisco Identity Service (IdS) 70
Authentication and Authorization Flow 70
Accessibility 71

CHAPTER 4 **Unified CCX Solution Design Considerations** 77
Core Components Design Considerations 77
General Solution Requirements 77
Principal Design Considerations for Call Center Sizing 77
Preliminary Information Requirements 78
Terminology 79
Effect of Performance Criteria on Unified CCX Server 80
Impact of Performance Criteria on the Unified CM Servers 80
Cisco Finesse Design Considerations 81
Cisco Finesse 81
Cisco Finesse IP Phone Agent 84
Desktop Chat 85
Cisco Unified Intelligence Center Design Considerations 87

Unified Intelligence Center Deployments 87
Standalone Cisco Unified Intelligence Center 88

CHAPTER 5 High Availability and Network Design 89
Unified CCX High Availability over LAN 89
Unified CCX High Availability over WAN 90
Network Requirements 90
Delay 90
Bandwidth 91
Quality of Service 93
Deployment Considerations 93
Engine Redundancy 94
When the Master Engine is Down 94
Automatic Call Distribution (ACD) 95
Interactive Voice Response 95
Unified CCX Outbound Dialer 95
WAN Link Failure Between Sites—Island Mode 96
WAN Link and Single Engine Failure 96
Chat and Email 97
Cisco Finesse High Availability Considerations 97
Finesse IP Phone Agent Failure Behavior 100
Cisco Unified Intelligence Center High Availability Considerations 100
Customer Collaboration Platform High Availability Considerations 101
ASR TTS High Availability Considerations 101
Cisco IM&P High Availability Considerations 101

CHAPTER 6 Solution Security 103
Security 103
Transport Layer Security 104
Cross-Origin Resource Sharing (CORS) 105
Gadget Source Allowed List 105
Secure Real-Time Protocol (Secure RTP or SRTP) 105
SRTP Considerations 105
Federal Information Processing Standards 140-2 Level 1 106

FIPS 140-2 Level 1 Considerations 106
FIPS 140-2 Mode Restrictions 107
Supported Ciphers 108

CHAPTER 7 Design Considerations for Integrated Features 111
Single Sign-On (SSO) Considerations 111
SSO Message Flow 112
Single Sign-On High Availability Considerations 112
Single Sign-On Design Impacts 113
Qualified Identity Providers 114
IdP Metadata Schema 114
SAML Request Attributes 114
Expectations from SAML Response 115

CHAPTER 8 Bandwidth, Latency, and QoS Considerations 117
Bandwidth, Latency, and QoS for Core Components 117
Estimating Bandwidth Consumption 117
Unified CCX Bandwidth Calculator 117
Remote Agent Traffic Profile 118
External System Interactions 119
IP Call Bandwidth Usage 119
Bandwidth Available for Monitoring and Recording 120
Web Chat Feature 122
Agent Email Feature 123
QoS and Call Admission Control 126
CAC and RSVP 127
Bandwidth, Latency, and QoS for Cisco Finesse 129
Cisco Finesse Desktop Latency 129
QoS for Cisco Finesse 130
Bandwidth, Latency, and QoS for Unified Intelligence Center 130
Reporting Scaling Considerations 130

CHAPTER 9 Sizing Operating Conditions for Reference Design 131
Contact Center Basic Traffic Terminology 131

Server Capacities and Limits 133
Operating Considerations for Reference Design Compliant Solutions 138
Time Synchronization 138
IPv6 Support 139
SIP Support 139

CHAPTER 10 Cisco Webex Experience Management 141
Overview 141
Post-Call Voice Survey Call Flow 142
SMS or Email Post-Call Survey Call Flow 143

Preface

- Change History, on page ix
- About This Guide, on page ix
- Audience, on page ix
- Conventions, on page x
- Related Documents, on page xi
- Documentation and Support, on page xii
- Documentation Feedback, on page xii

Change History

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

Change	See	Date
Initial Release of Document for Release 12.5(1) SU2		
Added information about the availability of VPN-less Finesse desktop for agents and supervisors	Contact Center Express Solutions Overview > Features > VPN-Less Access to Finesse Desktop	**April 2022**

About This Guide

This guide provides design considerations and guidelines for deploying Cisco Unified Contact Center Express (Unified CCX). This guide assumes that you are familiar with basic contact center terms and concepts.

Audience

This guide is primarily for contact center designers and system administrators.

Conventions

This manual uses the following conventions.

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit** > **Find** • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • An argument for which you must supply values. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco Unified Contact Center Express Installation Guide*.

`window` font	Window font, such as Courier, is used for the following:
	• Text as it appears in code or information that the system displays. Example:
	`<html><title> Cisco Systems,Inc. </title></html>`
	• File names. Example: `tserver.properties`.
	• Directory paths. Example:
	`C:\Program Files\Adobe`

string	Nonquoted sets of characters (strings) appear in regular font. Do not use quotation marks around a string or the string will include the quotation marks.
[ ]	Optional elements appear in square brackets.

Convention	Description
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
< >	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.
^	The key labeled Control is represented in screen displays by the symbol ^. For example, the screen instruction to hold down the Control key while you press the D key appears as ^D.

Related Documents

Document or Resource	Link
Cisco Unified Contact Center Express Documentation Guide	https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_documentation_roadmaps_list.html
Cisco Unified CCX documentation	https://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html
Cisco Unified Intelligence Center documentation	https://www.cisco.com/en/US/products/ps9755/tsd_products_support_series_home.html
Cisco Finesse documentation	https://www.cisco.com/en/US/products/ps11324/tsd_products_support_series_home.html
Cisco Customer Collaboration Platform documentation **Note** From Unified CCX Release 12.5(1), CCP documents are available in the Cisco Unified CCX documentation folder.	https://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html
Cisco Unified CCX Virtualization Information	https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-contact-center-express.html

Document or Resource	Link
Cisco Unified CCX Compatibility Information	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html

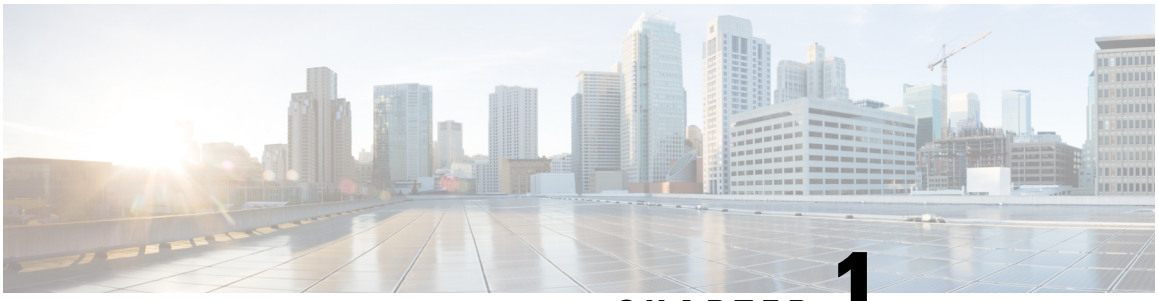
Documentation and Support

To download documentation, submit a service request, and find additional information, see *What's New in Cisco Product Documentation* at https://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Documentation Feedback

To provide your feedback for this document, send an email to:

contactcenterproducts_docfeedback@cisco.com



CHAPTER 1

Cisco Unified Contact Center Solutions

• Unified Contact Center Express Solution, on page 1

Unified Contact Center Express Solution

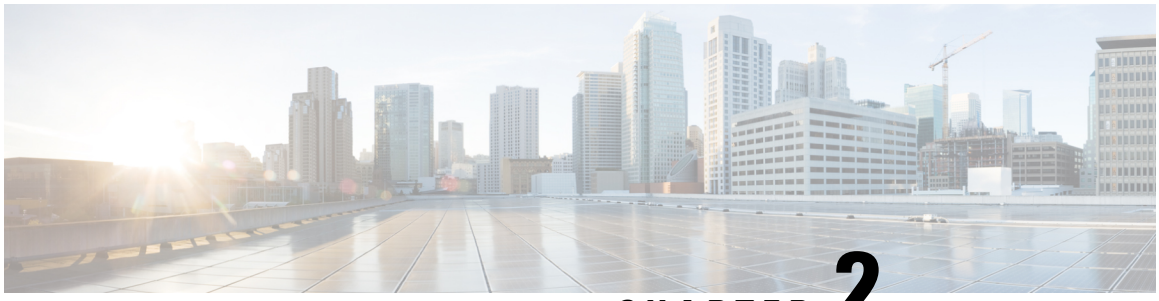
Cisco Unified Contact Center Express (Unified CCX) meets the contact center needs of departmental, enterprise branch, or small to medium-sized companies. Unified CCX offers easy-to-deploy, easy-to-use, highly available, and sophisticated customer interaction management for up to 400 agents. Unified CCX enhances the efficiency, availability, and security of customer contact interaction management in a virtual contact center. It offers integrated self-service applications across multiple sites.

Unified CCX provides reduced business costs and improved customer response by providing a single-server, contact-center-in-a-box deployment with the following:

- A sophisticated and distributed automatic call distributor (ACD)
- Computer telephony integration (CTI)
- Agent and desktop services

You can add the Cisco Workforce Optimization suite to provide quality management and work force management tools to improve workforce productivity.

Unified CCX is available in Enhanced and Premium versions to better match product functions with your business requirements. All Unified CCX solutions are tightly integrated with Unified CM.



CHAPTER 2

Unified CCX Reference Designs

- Introduction to the Unified CCX Solution Reference Designs, on page 3
- Unified CCX General Rules for Design, on page 5
- Reference Designs, on page 6
- Other Design Considerations , on page 6

Introduction to the Unified CCX Solution Reference Designs

This chapter discusses the reference designs that are available for Unified CCX. Use the Cisco Collaboration Sizing Tool to help you determine the number and types of servers required for any supported deployment model and call processing requirements. Before using that tool, it is necessary to have an understanding of what deployment model you desire.

Cisco Unified Intelligence Center, Cisco Finesse, and Cloud Connect are deployed on the same Virtual Machine (VM) with Unified CCX and support all the Unified CCX reference designs.

The following table depicts the reference designs that are supported in Unified CCX. These models have no bearing on which specific server model is used. The Cisco Collaboration Sizing Tool identifies the minimum server model required. This chapter provides general rules for design and considerations and limitations for each of these reference designs. This information allows a Unified CCX system planner or designer to understand what other similar reference designs are supported. This also helps to understand how to determine the best solution for a given set of requirements.

Table 1: Unified CCX Reference Designs

Unified CCX Reference Design	Unified CCX Components on Server 1	Unified CCX Components on Server 2
Single-Server Non-High Availability Deployment Model—Unified Communication Manager Integration	Engine, Database, Monitoring, Reporting, Desktop, Cisco Identity Service components, Cloud Connect components.	—
Two-Server High Availability Deployment Model—Unified Communication Manager Integration	Engine, Database, Monitoring, Reporting, Desktop, Cisco Identity Service components, Cloud Connect components.	Engine, Database, Monitoring, Reporting, Desktop, Cisco Identity Service components, Cloud Connect components.

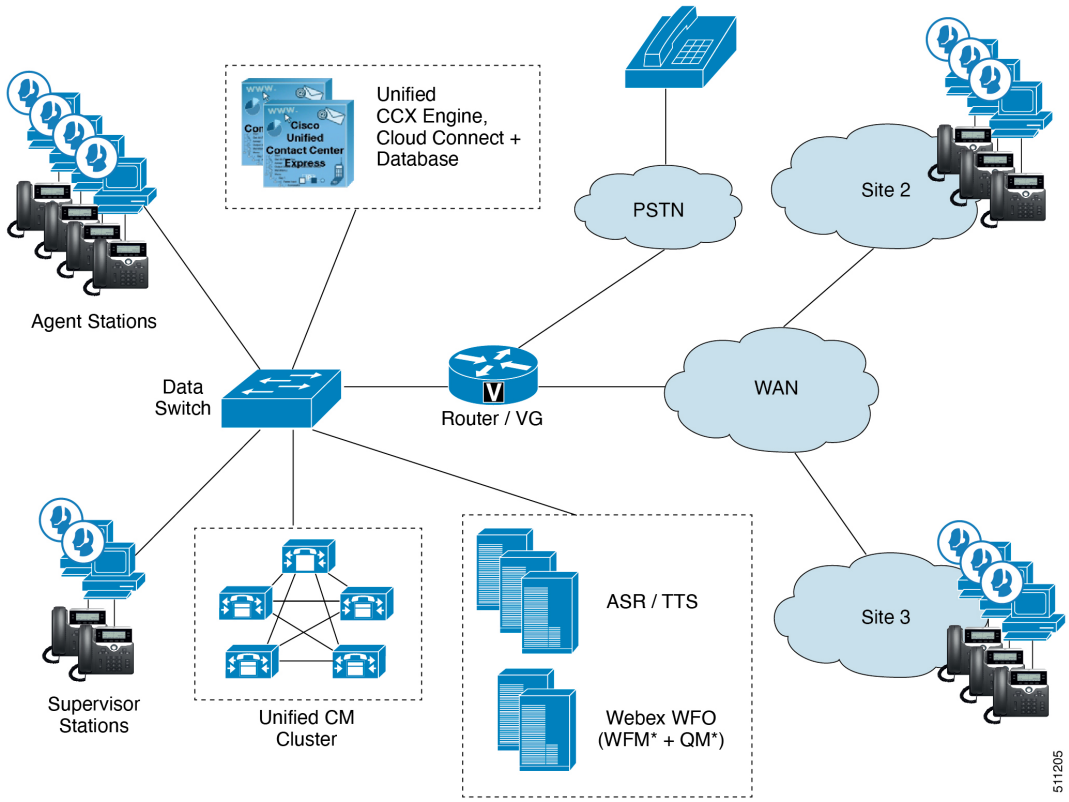
Note Unified CCX deployment model integrated with Unified CME is not supported in 9.0(1) and higher versions.

For hardware requirements, see *Cisco Unified CCX Virtualization Information* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-contact-center-express.html.

The following figure depicts the deployment when integrating Unified CCX with Unified Communications Manager. In this deployment, optional Unified CCX components shown with an asterisk (*) can be added. These components are:

- Cisco Unified Work Force Management and Quality Manager.

Figure 1: Deployment Model of Unified CCX Integrated with Unified Communication Manager



Note ASR and TTS can be added in Unified CCX integrated with Unified Communication Manager. ASR and TTS software is not provided by Cisco. This software must be purchased from other vendors. These vendors can provide design and server sizing requirements for their software.

Unified CCX General Rules for Design

The following rules apply when designing a Unified CCX deployment:

- When deploying for high availability (HA), the Unified CCX servers can be located in the same campus LAN to provide server redundancy. The Cisco Unified CCX servers can also be located in different sites separated by WAN to provide spatial redundancy.

Note For HA over LAN deployment, heartbeats are sent every one second and failover occurs if three consecutive heartbeats are missed. For HA over WAN deployment, heartbeats are sent every second and failover occurs if ten consecutive heartbeats are missed. These values are not configurable.

- You can locate the Unified Communications Manager servers that run CTI Managers with which Unified CCX communicates in the same campus LAN. In Unified CCX servers that are deployed over WAN, for better site redundancy, deploy local Unified Communications Manager server at both sites.
- The Recording component must be redundant, if recording is used in a high availability deployment.
- All agents for a Unified CCX deployment must be using phones that register to the same Unified CM cluster. Calls can be received from devices and callers on another Unified CM cluster (using intercluster trunks).
- Unified CCX software versions must be the same for both the master and standby nodes in a high availability deployment.
- Unified CCX solution works with a combination of software and hardware components, providing an open and flexible environment for customers to run complex scripts, custom codes, documents, and so on. Overloading any of the software and hardware components such as virtual memory and CPU could impact the solution performance. Review and optimize the scripts, custom codes, and documents before they are loaded to the production setup. Also constantly monitor the system component and hardware attributes like disk space and CPU utilization.

When deploying Quality Management and Workforce Management with Unified CCX, consider the following guidelines:

- Unified CCX does not support the use of third-party applications (for example, using TAPI) to control its devices.
- For more deployment information about Workforce Management and Quality Management, refer to the *Cisco Webex WFO User Guide for Cloud Deployments* available at here:

  https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/workforce_optimization/Webex_WFO/webex-wfo-user-guide.pdf.

Note Existing Unified CCX customers with WFO licenses will have to remain on classic licensing as WFO licenses are not supported in Smart Licensing. However, you can move Unified CCX licenses to Smart Licensing and existing Cisco WFO licenses to Cisco SolutionsPlus. For more information, contact Cisco Support.

Reference Designs

The following sections describe the Unified CCX Reference Designs.

Single-Server Non-High Availability Reference Design

Unified CM integration with Unified CCX on a single-server nonhigh availability is for small deployments. This reference design places a single instance of all the Unified CCX software components on the same server and uses Informix Dynamic Server as the database server.

This reference design allows the Unified CCX Engine to fail over to a backup CTI Manager if the primary CTI Manager fails. CTI ports and CTI route points should be grouped into device pools that have the same primary and secondary server list as those used for JTAPI communications with the CTI Managers.

Two-Server High Availability Reference Design

This reference design can support silent monitoring and recording for agents at any WAN-connected site by using desktop monitoring. (See the Unified CCX Compatibility related information located at: http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html for a list of phones that support desktop monitoring.) It can also support SPAN port monitoring for agents on the VLAN segment local to Unified CCX server. This reference design provides redundancy for both recording and silent monitoring for all agents using desktop monitoring (regardless of location) or agents on the local VLAN using SPAN port monitoring. Silent monitoring and recording are not possible for agents who are using the Cisco Finesse IP Phone Agent at remote sites. Similarly, silent monitoring and recording are not possible for agents at remote sites who are using phones that do not support desktop monitoring.

This reference design allows either Unified CCX Engine component to fail over to a backup CTI Manager if the primary server fails. CTI Ports and CTI Route Points should be grouped into device pools that have the same primary and secondary server list as that used for JTAPI communications to the CTI Managers.

Note In HA deployments, historical data comes from the database located in the standby engine node. A higher number of historical reporting sessions during operating hours is supported for HA deployments.

Other Design Considerations

Consider the following when designing your Unified CCX system:

- High availability requires additional disk space, so historical call reporting capacity may be reduced. Historical call reporting capacity also depends upon BHCC, hours of operation per day, and days of operation per week.
- G.711 call recording requires about 1 MB per minute. G.729 call recording requires about 256 KB per minute.
- The following categories of data use hard disk space:

  - Operating system files, Unified CCX software, and Informix Database Management software
  - Unified CCX logs
  - The Unified CCX database (comprised of 4 data stores)

- The Unified CM sizing tools assume devices are evenly distributed across all servers. CTI route points are configured as part of a device pool in the Cisco Unified Communications Manager Server as the primary CTI Manager being used; it may be required to run the Cisco Unified Communications Manager sizing tool on a per-location or per-server basis.
- The Unified CM QSIG (Q Signaling) path replacement feature is not supported for Unified CCX calls.
- Unified CM Forced Authorization Codes and Client Matter Codes should be turned off for all route patterns in the Unified CM cluster that are used by Unified CCX. Enabling these features for route patterns that are not used by Unified CCX does not affect Unified CCX.
- For a list of unsupported features in Unified CM with Unified CCX, refer to the current release notes for Unified CCX.
- Unified CCX supports different sets of Finesse IP Phones as agent devices on the Unified CM and Unified CM platform; not all agent devices can be used as Finesse IP Phone Agent. For a complete list of supported agent devices, see the Unified CCX Compatibility related information located at: http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.
- Finesse allows each agent to choose and set a language from the language selector drop-down list on the sign-in page.
- An agent using Cisco Finesse Agent Desktop can log in using Extension Mobility but the agent phone must be in the Unified CM cluster that is used by Unified CCX.
- Sometimes new releases of Unified CM will not support Unified CCX immediately at Unified CM first customer ship (FCS) time. Some organizations may be early adopters of new Unified CM releases and may be delayed from migrating to new Unified CM releases and using new Unified CM features if Unified CCX is installed with that same Unified CM cluster. Therefore, in some situations, it makes sense to have a separate Unified CM cluster for Unified CCX.
- Cisco Jabber runs in two modes: Deskphone Mode and Softphone Mode. Unified CCX only supports Cisco Jabber as an agent device in Softphone Mode.
- Video is now supported if you are using Cisco Jabber as an agent phone. The agent desktop where Jabber is used for video should comply to the Cisco Jabber hardware requirements listed in the *Release Notes for Cisco Jabber for Windows* , located at: http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-release-notes-list.html and *Release Notes for Cisco Jabber for Mac* located at: http://www.cisco.com/c/en/us/support/unified-communications/jabber-mac/products-release-notes-list.html
- The following features are not supported if you are using Cisco Jabber as an agent phone:
  - Extension Mobility

Mobile and Remote Access

The Cisco Collaboration Edge architecture includes Unified Communications Mobile and Remote Access (MRA) to enable access by devices that are not in the enterprise network. MRA uses Cisco Expressway to provide secure firewall traversal and support for Unified CM registrations. Unified CM can then provide supported devices with call control, provisioning, messaging, and presence services.

For details on Collaboration Edge, see the documentation at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/tsd-products-support-series-home.html. For details on Cisco Expressway deployment and configuration, see the documentation at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html. See the *Compatability Matrix* for your solution for details of device support for MRA.

If Unified CCX uses MRA, consider these points:

- The connection between the Cisco Finesse client and server is over a VPN, not over the MRA connection.
- If you have VPN split-tunneling configured, you can use Jabber with MRA and the Finesse desktop on the same client machine. See https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html for Cisco AnyConnect Mobility Client Split-Tunneling configuration.
- If VPN split-tunneling is not available, you can run after splitting them onto two clients.
  - A remote agent who runs Jabber with MRA on one client machine and the Finesse desktop with a VPN connection on a second client machine.
  - A remote agent who runs a Jabber softphone on a laptop that is connected over MRA and runs the Finesse desktop as a Xenapp thin client.
- Certain phones do not support Extension Mobility over MRA.
- Unified CCX video deployments do not support MRA.
- Certain Contact center features like Agent Greeting and Unified CM-based Silent Monitoring that rely on a phone's BiB are not supported over MRA.

Multiple Cisco Unified CCX Clusters Integrated with a Single Cisco Unified Communications Manager Cluster

You can integrate multiple Unified CCX clusters with a single Cisco Unified Communications Manager cluster.

Note There is no limit to the number of Unified CCX clusters supported with a single Unified CM cluster as long as the combined agent phones, CTI ports, and CTI route points that are utilized by all Unified CCX clusters are used to size Unified CM.

- To determine if you need more than one CTI Manager, refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

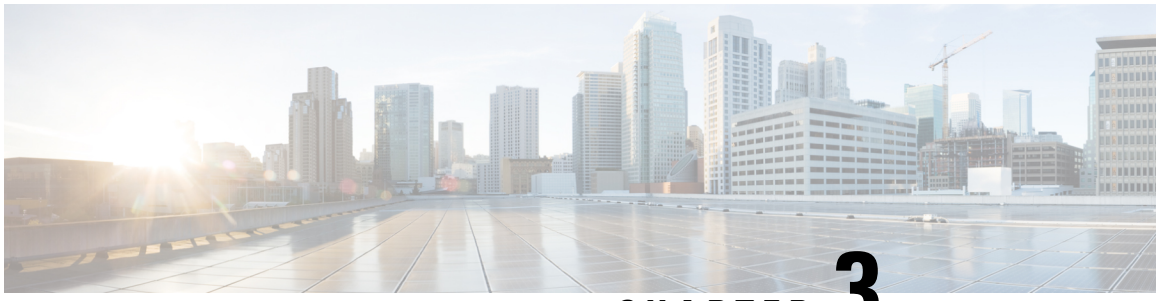
If your deployment requires more than one CTI Manager, you load-balance the Unified CCX and other CTI applications across various CTI Managers in the cluster to provide maximum resilience, performance, and redundancy.

For additional information on CTI Manager, refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

- If more than one Unified CM primary subscriber is required to support your configuration, distribute all agents equally among the Unified CM subscriber nodes. This configuration assumes that the busy-hour call attempts (BHCA) is uniform across all agents.
- Each Unified CCX cluster is standalone and independent from other Unified CCX clusters. There is no communication or synchronization between the Unified CCX clusters. Agents should operate using only one Unified CCX cluster.

  Unified CM Telephony Triggers (CTI Route Points) and CTI ports should be different across Unified CCX clusters.
- In the list of Resources in Unified CCX Administration, each Unified CCX cluster displays all the agents in the Cisco Unified Communications Manager cluster, even though the agents can operate and log in to another Unified CCX cluster.

  This situation requires that the Unified CCX Administrator be aware of which resources are associated with each cluster. The Unified CCX Administrator can mitigate this situation by having a unique naming convention for resources associated with a particular Unified CCX cluster.
- This deployment is not intended to provide Unified CCX redundancy across different Unified CCX clusters. If a Unified CCX cluster fails, the agents that operate in this cluster cannot operate in other Unified CCX clusters. If another Unified CCX cluster is configured to accept the calls that were originally sent to the Unified CCX cluster that failed, there will be no report integration between the Unified CCX clusters.
- This deployment does not change the characteristics and design considerations of each individual Unified CCX cluster. For example, within a Unified CCX cluster, high availability is still supported.
- If more than one Unified CCX cluster is integrated with the same Unified CM cluster, all agents belonging to all the Unified CCX clusters are visible to administrators of all the Unified CCX clusters. The administrator must be aware of the agents belonging to the Unified CCX cluster that the administrator manages and configures.



CHAPTER 3

Contact Center Express Solutions Overview

- Overview, on page 11
- Unified CCX Components, on page 11
- Unified CCX Licensing, on page 12
- Features, on page 17

Overview

Cisco Unified Contact Center Express provides a secure, highly available, and easy to deploy customer interaction management solution for up to 400 agents. This integrated “contact center in a box” is intended for both formal and informal contact centers.

Unified CCX provides options to address multiple contact center functional areas such as:

- Inbound voice
- Outbound campaign
- Agent email
- Web chat

Other components included are:

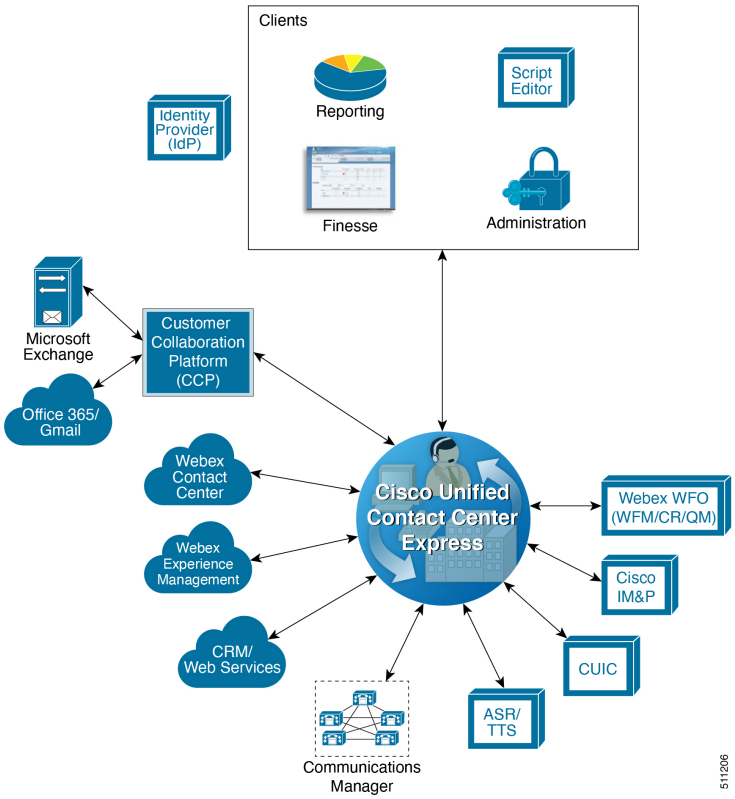
- Historical and Real Time Reporting.
- Browser-based Cisco Finesse Desktops

You can deploy these options on Cisco Unified Computing Systems (UCSs) or any other equivalent specification-based third-party virtual servers with the supported reference designs. For more information, see the Unified CCX Virtualization related information located at: http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-contact-center-express.html

Unified CCX Components

The following diagram depicts the components of Unified CCX:

Figure 2: Unified CCX Components



Unified CCX Licensing

Unified CCX is available in the following different packages: Enhanced, and Premium. The different packages provide varying levels of customer interaction management channel options and capability within a contact channel. For more detailed information, refer to product data sheets, feature guides, and end-user documentation for each type of Unified CCX customer contact interaction management at the following URL:

http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1846/index.html

Note Standard license is not supported from release 12.0(1).

Unified CCX is now part of Flex licensing. For more details refer to the following link:

https://www.cisco.com/c/en/us/products/collateral/unified-communications/cisco-collaboration-flex-plan/datasheet-c78-741220.html

Unified CCX deployments must have all product components and optional features of the same package type. Mixing components or options from different license packages is not supported.

Licensing for Cisco Unified Contact Center Express

The feature availability is based on the type of license for Cisco Unified Contact Center Express. Unified CCX Licenses are concurrent and the Workforce Management licenses are named-user licenses.

Concurrent licenses apply to logged in users. Different individuals may share a concurrent license as long as only one of them is logged in. For example, Company A has 300 unique users that work in 3 shifts. Each shift has 100 logged in users. Company A needs to purchase only 100 concurrent user licenses.

Named licenses apply to unique individual users regardless of their logged in status. Company B has 300 unique users that work in 3 shifts and each needs access to the licensed option. Each shift has 100 logged in users. Company B must purchase 300 named licenses.

Note Existing Unified CCX customers with Named licenses have to remain on Classic Licensing as Named Licenses are not supported in Smart Licensing. However, you can move Unified CCX licenses to Smart Licensing and existing Cisco Named licenses to Cisco SolutionsPlus. For more information, contact Cisco Support.

Unified CCX gives an option to either remain on Classic Licensing or move to Smart Licensing. This option is available ONLY for the existing Unified CCX customers on older version and upgrading to version 12.5.

Unified CCX has enabled Smart Licensing that helps you to procure, deploy, and manage licenses easily, and report license consumption. It pools the license entitlements in a single account and allows you to move licenses freely across virtual accounts. Smart Licensing is enabled across Cisco products and is managed by Cisco Smart Software Manager (Cisco SSM). Smart Licensing registers the product instance, reports license usage, and obtains the necessary authorization from Cisco SSM. For more information, see *Cisco Unified Contact Center Express Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-feature-guides-list.html.

Smart Licensing allows you to use more licenses than you have purchased. However, if you want to limit the license usage to the purchased quantity or less, use **License Control**. With **License Control**, you can disable **Overage Allowance** option to restrict the number of agents and ports that can be used in Unified CCX. For different license types, appropriate fields will be displayed for you to restrict the usage of licenses and ports. For more information about license restrictions in different license types, see the *Overview* section of *Smart Licensing* chapter in *Cisco Unified Contact Center Express Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-feature-guides-list.html.

Note When you over-consume the licenses, the product instance will be moved to out-of-compliance and later to enforcement mode, which eventually enforce you to buy more licenses.

License Control is not available with **Not For Resale (NFR)** and **Non Production Systems (NPS)** licenses.

Overage Allowance is enabled by default. It can be edited while registering and re-registering the product instance, and when the product instance is in registered state.

Specific License Reservation is a feature that is used in highly secure networks. It provides a method to deploy a software license on a system (product instance - Unified CCX), which does not share the license utilization data with Cisco SSM regularly due to organization policies. You can reserve licenses (including add-on licenses) for your product instance on Cisco SSM.

Specific License Reservation is available by default in the smart account. To enable Specific License Reservation, you must use Unified CCX CLI.

For more information about Specific License Reservation, see the *Specific License Reservation* section in *Cisco Unified Contact Center Express Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-feature-guides-list.html.

Note When Specific License Reservation is enabled, **License Control** option is not available.

Specific License Reservation is not available with **HCS-Flex**, **Not For Resale (NFR)**, and **Non Production Systems (NPS)** licenses.

The following table lists the Cisco Unified CCX licenses and the available features.

Note Perpetual licenses have reached End of Sale and cannot be ordered. Only Flex licenses are available.

Table 2: Cisco Unified Contact Center Express Perpetual and Flex Licensing

Feature	Perpetual Premium	Perpetual Enhanced	Flex Premium	Flex Standard	Optional
Inbound Voice	Yes	Yes	Yes	Yes	No
Blended Preview Outbound Dialer	Yes	No	Yes	Yes	No
Predictive and Progressive Outbound Dialer	Yes	No	Yes	No	Yes
Outbound IVR	Yes	No	Yes	Yes	Yes
Outbound Voice	Yes	No	Yes	Yes	No
Agent E-Mail	Yes	No	Yes	No	No
Web Chat	Yes	No	Yes	No	No
Inbound Voice High-Availability Option	Yes	Yes	Yes	Yes	Yes
Database Integration	Yes	No	Yes	No	No
Webex WFO: Call Recording	Yes	Yes	Yes	Yes	Yes
Webex WFO: Quality Management	Yes	Yes	Yes	Yes	Yes

Feature	Perpetual Premium	Perpetual Enhanced	Flex Premium	Flex Standard	Optional
Webex WFO: Workforce Management	Yes	Yes	Yes	Yes	Yes
Webex WFO: Analytics	NA	NA	Yes	Yes	Yes
Cisco WFO: On Demand Call Recording	EOL	EOL			
Cisco WFO: Quality Management Option	EOL	EOL			
Cisco WFO: Advanced Quality Management Option	EOL	EOL			
Cisco WFO: Workforce Management Option	EOL	EOL			
Finesse Agent and Supervisor Desktop	Yes	Yes	Yes	Yes	No
Finesse IP Phone Agent	Yes	Yes	Yes	Yes	No
Standalone CUIC	Yes	No	Yes	No	No
Cisco Customer Collaboration Platform	Yes	No	Yes	No	No
Post Call Surveys	Yes	Yes	Yes	Yes	Yes
Single Sign-on	Yes	Yes	Yes	Yes	Yes
Chrome Browser Support	Yes	Yes	Yes	Yes	Yes
Chromium Edge Support	Yes	Yes	Yes	Yes	Yes
IE Browser Support	EOL	EOL	EOL	EOL	EOL

Feature	Perpetual Premium	Perpetual Enhanced	Flex Premium	Flex Standard	Optional
Firefox ESR Browser Support	Yes	Yes	Yes	Yes	Yes
Edge Browser Support	Yes	Yes	Yes	Yes	Yes
REST APIs for Configuration	Yes	Yes [1]	Yes	Yes	Yes
Supervisor Access to Historical Reports	Yes	Yes	Yes	Yes	Yes
TLS 1.2 Support	Yes	Yes	Yes	Yes	Yes
Calendar Management (Business Hours and Holidays)	Yes	Yes	Yes	Yes	Yes
Advanced Supervisor Capabilities	Yes	Yes	Yes	Yes	Yes
Workflow for Digital Channels	Yes	No	Yes	No	Yes
Smart Licensing Support [2]	Yes	Yes	Yes	Yes	No
Specific License Reservation (SLR) [2]	Yes	Yes	Yes	Yes	Yes
Overage Allowance [2]	Yes	Yes	Yes	Yes	Yes
Remote Agent: Agent Device Selection	Yes	Yes	Yes	Yes	Yes
OAuth 2.0 Support: Gmail	Yes	No	Yes	No	Yes
Webex Experience Management Post Call Survey: IVR	Yes	Yes	Yes	Yes	Yes

Feature	Perpetual Premium	Perpetual Enhanced	Flex Premium	Flex Standard	Optional
Webex Experience Management Post Call Survey: SMS, Email	Yes	Yes	Yes	Yes	Yes
64 Alpha-numeric Characters Agent ID Support	Yes	Yes	Yes	Yes	Yes
VPN-less support for Finesse Desktop	Yes	Yes	Yes	Yes	Yes
Support for Case Insensitive Login to Finesse and appadmin	Yes	Yes	Yes	Yes	Yes
ECDSA and RSA 4K Certificate Support	Yes	Yes	Yes	Yes	Yes
Conversational IVR Support	Yes	Yes	Yes	Yes	Yes

[1] For more information on APIs, refer to the *Cisco Unified Contact Center Express Developer Guide*, available at https://developer.cisco.com/docs/contact-center-express/#!configuration-api-dev-guide.

[2] Not applicable for Webex WFO and Cisco WFO

Features

Agent Interfaces

Cisco Finesse provides the following agent interfaces:

- Cisco Finesse agent desktop and IP Phone Agent (IPPA) for agent use.
- Cisco Finesse supervisor desktop for supervisor use.
- Cisco Finesse administrator console for administrator use.

The following Cisco Finesse agent interface services are available with Unified CCX:

Agent Interfaces
Cisco Finesse Agent and Supervisor desktops
Cisco Finesse IP Phone Agent

Agent Interfaces
Cisco Finesse administrator console

Cisco Finesse Agent Desktop Features

Cisco Finesse provides Cisco Finesse agent desktop and IP Phone Agent (IPPA) for agent use. The following table describes the Cisco Finesse Agent Desktop features that are available in Unified CCX.

Table 3: Cisco Finesse Agent Desktop Features Available in Unified CCX

Feature
Agent State Control. From the agent desktop, agents log in, log out, and make themselves ready and not ready.
Call Control. From the agent desktop, agents can answer, release, hold, retrieve, conference, consult, and direct transfer the calls.
Dynamic Regrouping. Change of agent association with a resource group is applied immediately.
Live Data Gadgets. Agents have access to Live Data Gadgets for themselves and their associated queues. For example, from the Cisco Finesse Gadgets, agents can see how many calls they have handled today and how many calls are currently in the queue for their CSQ.
Reason. Agents can choose the reason for Not Ready and Logout that are configured by the administrator.
Basic CTI. The agent desktop supports one variable in the header of the call control gadget and up to a total of 20 variables in two columns below the header. Each column can have up to 10 variables. You can use call variables, Extended Call Context (ECC) variables, or the following Outbound Option ECC variables: • BACampaign • BAAccountNumber • BAResponse • BAStatus • BADialedListID • BATimeZone • BABuddyName

Feature
Telephony Support. You can deploy Cisco Finesse with certain Cisco IP Phones, as described in the Unified CCX Compatibility related information located at: http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html. However, there are different features available on different phones. Unified CCX monitors and reports on the activities of the first four configured lines on a phone, including non-ACD lines. Agents are associated with a specific Cisco Communications Manager extension (directory number). Agents' primary and secondary extensions can be shared with multiple devices. When an extension is shared with multiple devices, agents must ensure that they use the device that was selected while logging on to Finesse desktop (active device). When an agent is busy on the secondary Non-ACD line, the agent state changes to Not Ready, if configured by the Administrator. Agents can also place calls in the Ready state.
Hot Desking. Hot desking allows agents to log in using Finesse and any Cisco Unified IP Phone that is registered with the same Cisco Unified Communications Manager cluster. This capability allows multiple agents to use the same phone, one at a time. For example, different agents on different shifts may use the same workstation and phone. Extension Mobility brings a user-specific phone profile (including its configured extensions) to the phone the agent is logged into. After logging in to Cisco Unified Communications Manager with Extension Mobility, agents can log in to Unified CCX using Cisco Finesse.
Desktop Workflows. The workflows allows you to automate common repetitive agent tasks. The workflow has a unique name and a helpful description. Use the Manage Workflows and Manage Workflow Actions gadgets in Cisco Finesse to view, add, edit, or delete workflows and workflow actions. All workflows are team-level workflows. You cannot create a global workflow. If you need a global workflow, create a team workflow and assign it to all teams.
Application Integration - HTTP. You can configure Cisco Finesse with desktop workflows to allow the passing of call data to other desktop applications (for example, CRM applications) for an application window. You can pass data to other applications through HTTP put or get commands that are then associated with specific call activities such as call ringing. A screen pop does not require any programming. You can also perform application integration on call release to pop open a wrap-up application on the agent workstation.
Workflow-Initiated Call Recording. You can configure Cisco Finesse to automatically start recording calls. The calls must meet the conditions that are defined in the application script and voice contact workflow.
Automatic Failover. When the active Unified CCX server fails, Cisco Finesse automatically logs the agents back in. The agents are then logged in back to the same state (Ready or Not Ready) that they were in before the failover. However, if the agent was in an active call, they are logged back into the Not Ready State and the call continues uninterrupted. The failover may affect the call duration and other information that are associated with the call in the historical reporting database. If you generate historical reports for time periods in which a failover occurred, the report will have missing or incorrect data.
Wrap-Up Reasons. The Wrap-Up Reason selection is available to the agent.
Agent Email. Queues and routes email messages to staffed and skilled agents and helps the agent to respond easily. The Agent Email also provides a collection of historical reports that help measure email performance accurately.

Feature
Web Chat . The web chat with premium provides the facility for customers to initiate a chat session with the agent.
Workforce Optimization. Webex Workforce Optimization (WFO) for Unified CCX is a full-featured solution for optimizing performance and quality. WFO is an integral component of the Cisco Unified Communications System. The Webex WFO suite provides two solutions: Workforce Management (WFM) and Call Recording and Quality Management (QM). **Note** Existing Unified CCX customers with WFO licenses have to remain on classic licensing as Smart Licensing does not support WFO licenses. However, you can move Unified CCX licenses to Smart Licensing and existing Cisco WFO licenses to Cisco SolutionsPlus. For more information, contact Cisco Support.
Outbound Preview Dialer. Cisco Finesse includes buttons to control an agent response to an outbound contact offering by the system. If the agent clicks the Accept button, the system places the outbound call to the customer from the agent phone.
Desktop Chat. Agents can initiate a chat session with other users in the contact center using the Desktop Chat gadget. You need a Cisco Instant Messaging and Presence (IM&P) server to use this feature. Users must log in to the Desktop Chat gadget. They can then initiate a chat with any user logged in to the IM&P either from the Desktop Chat gadget or from a desktop client like Jabber. Cisco Finesse Desktop Chat gadget does not support Single Sign-On. The minimum supported version of Cisco IM&P and Unified CM for Desktop Chat is 12.5.
Team Message. Teams can view the messages that are sent by their respective supervisors and take necessary action.

Cisco Finesse IP Phone Agent Features

The following table describes the Finesse IP Phone Agent (FIPPA) features that are available in Cisco Unified CCX.

Table 4: FIPPA Features Available in Cisco Unified CCX

Feature
Agent State Control. From the FIPPA XML application, agents log in, log out, and make themselves ready or not ready.
Call Control. The Cisco Unified IP Phone provides call control.
Queue Statistics. Agents can view the number of calls waiting in the queue and the longest call waiting in the queue.
Dynamic Regrouping. Change of agent association with a resource group is applied immediately.
Reason. Agents can be configured to select reasons for Not Ready and Logout.
Basic CTI. FIPPA allows for call data to be popped onto the IP Phone display upon call ringing.

Feature
Telephony Support. Finesse can be deployed with select Cisco Included Unified IP Phone models, as described in the Unified CCX Compatibility related information located at: http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.
Hot Desking. Hot desking allows agents to log in using any Cisco Unified IP Phone that is registered with the same Cisco Unified Communications Manager cluster. Agents using Cisco IP Communicator can also use Extension Mobility. This capability allows multiple agents to use the same phone, but only one at a time. For example, different agents on different shifts may use the same workstation and phone. Extension Mobility brings a user-specific phone profile (including configured extensions for that user) to the phone being logged in from. After logging in to Cisco Unified Communications Manager with Extension Mobility, agents can log in to Cisco Unified CCX using Finesse.

Note Finesse IP Phone Agent (FIPPA) is not supported for Blended (inbound and outbound) users and users configured for Outbound only.

Cisco Finesse Supervisor Desktop Features

The following table lists the Cisco Finesse Supervisor Desktop features that are available in Cisco Unified CCX.

Table 5: Cisco Finesse Supervisor Desktop Features Available in Cisco Unified CCX

Feature
View / Change Agent State. Supervisors can view the current state of all agents that are part of their team. The supervisor desktop allows the supervisors to change an agent state to Ready, Not Ready, or Logout.
Live Data Gadgets. Supervisors can view statistics of all agents and queues that are associated with their team.
Silent Monitoring. Supervisors can silently monitor agent calls and manual outbound calls made by the agent. Supervisor can only monitor one agent at a time. To monitor another agent, supervisor must end the silent monitoring call, and then select a new agent who is in Talking state. When an agent makes a manual outbound call from Not Ready state on the ACD line, the silent monitoring button on the team performance gadget will show enabled on the supervisor desktop. Supervisor can silent monitor the agent's call, however, the supervisor cannot change the state of the agent to Ready or Not Ready.
Barge-in. Supervisors can barge in on an agent call that they are silently monitoring. The Barge-in feature brings the supervisor, the agent, and the caller into a three-way conference. The agent is aware when the supervisor barges in. Barge-in is supported with Finesse using supported phones, or FIPPA.
Intercept. Supervisors can intercept an agent call. The intercept feature transfers the call to the supervisor and the agent is available to take another call. Intercept is supported with Finesse using supported phones, or FIPPA.

Feature
Automatic Failover and Re-login. Upon Cisco Unified CCX Engine failover, Finesse automatically fails over to the secondary Unified CCX Engine. The supervisor is logged in again and set to “Not Ready” state, but the call will continue to progress.
Advanced Capabilities. Supervisors who have been assigned advanced capabilities can manage queues, prompts, applications, calendars, and outbound campaigns.
Desktop Chat. Supervisors can initiate a chat session with other users in the contact center using the Desktop Chat gadget. A Cisco Instant Messaging and Presence (IM&P) server must be deployed for this fetaure. Users must login to the Desktop Chat gadget and can initiate a chat with any user logged in to the IM&P either from the Desktop Chat gadget or from a desktop client like Jabber. The Single Sign-On is not supported with the Finesse Desktop Chat gadget. The minimum supported version of Cisco IM&P and Unified CM for Desktop Chat is 12.5.
Team Message. Supervisors can broadcast messages to their teams.

Agent Device Selection

Administrators can enable or disable the **Agent Device Selection** feature. This feature allows agents to select a preferred device while logging on to Finesse desktop.

Agents' primary and secondary extensions can be shared with multiple devices. When an extension is shared with multiple devices, agents must ensure that they use the device that was selected while logging on to Finesse desktop (active device).

If the call is answered from non-active device, subsequent third party call control such as consult call, consult transfer, conference, and so on will not work properly.

Auto Answer

Administrators can configure Auto Answer for a team. For all the agents for whom this feature is configured, a call to their IPCC extension is Auto Answered, if they are in Ready state in the Finesse desktop. The calls to non-IPCC extensions are not Auto Answered by Unified CCX. If agents' IPCC extensions are shared across multiple devices, it is recommended not to use Unified CM Auto Answer, instead use Unified CCX Auto Answer.

Inbound Voice

Cisco Unified CCX Enhanced and Premium provide varying levels of inbound voice ACD, IVR, CTI, agent and supervisor desktops, desktop administration, real-time and historical reporting, and web-based administration features.

Each user license is for a concurrent user. For example, a contact center with three shifts of 100 agents and supervisors requires 100 concurrent user licenses. Each shift of 100 users would reuse these licenses during their shifts.

The following table lists the inbound voice licensed features:

Table 6: Inbound Voice Licensed Features

Feature
Concurrent inbound voice seat with FIPPA Each concurrent inbound voice user (agent or supervisor) requires a concurrent seat license. Each quantity of one seat license provides one quantity of Cisco Finesse IP Phone Agent (FIPPA).
Concurrent inbound voice seat with Finesse Desktop Each concurrent inbound voice user (agent or supervisor) requires a concurrent seat license.
Basic Prompt and Collect IVR port
Advanced IVR port
High Availability (HA) option HA provides licensing for mirrored, warm standby server software.

The following table lists the inbound voice features:

Table 7: Inbound Voice Features

Feature
System Features
Inbound voice redundancy support
Maximum number of ACD lines per agent is one (1).
Maximum number of secondary lines with Finesse is three (3).
Call conferencing
Agent inter-dialing support
Direct-outward-dialing (DOD) support
Inbound Voice Seats
Maximum number of configurable inbound agents supported is 2000.
Maximum number of active inbound agents supported (including supervisor seats) is 400.
Maximum number of inbound supervisor positions supported is 42.
Inbound seat license type is Concurrent user type.
Integrated ACD Features with Server Software
Custom scripting with Cisco Unified Contact Center Express Drag and Drop Editor
Maximum number of agent groups supported is 150.

Feature
Maximum number of agents per team is 50.
Automatic Number Identification (ANI) support
Dialed Number Identification Service (DNIS) support
Route on Skill
Route on Skill competency
Conditional routing (time of day, day of week, and custom variables)
Custom routing based on data from database access (for example, data-directed priority routing)
Dynamic priority queuing
Maximum number of definable skill groups is 150.
Maximum number of skills per agent is 50.
Recording
Workflow-based recording with Cisco Finesse is available with Webex WFO license.

IVR Ports

IVR ports are packaged as either Basic or Advanced IVR ports.

- Basic IVR ports licensing—Basic IVR ports are not licensed. You must use the Cisco Collaboration Sizing Tool to determine the maximum number of Basic IVR ports that are supported on a per-configuration basis.
- Advanced IVR ports licensing—Advanced IVR ports are licensed on a per-inbound voice seat basis and are available only with the Premium package. Each inbound voice seat provides two Advanced IVR port licenses. For example, a 100-seat inbound voice deployment provides 200 Advanced IVR port licenses. Advanced IVR port licenses counts are checked at run-time. In the example given here, the 201st simultaneously active request for an Advanced IVR port to handle an incoming call would be denied. Deployments that require additional advanced IVR ports need to purchase add-on Unified CCX Premium seats. Each Premium seat provides two advanced IVR ports.

Inbound Voice Packaged Components

The following sections describe the primary components that are provided with inbound voice. These sections provide high-level descriptions of the features and functions provided for these components. For more specific information, see the Cisco Unified CCX user documentation.

Automatic Call Distribution

The following table describes the Automatic Call Distribution (ACD) features that are available in a Unified CCX package.

Table 8: ACD Features Available in a Unified CCX Package

Feature
Conditional Routing. Unified CCX supports routing based on caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialed number, and processing of data from XML text files.
Agent Selection. Unified CCX supports the longest available, linear, most handled contacts, the shortest average handle time, and circular agent selection algorithms. With Basic ACD functionality, agents are associated with one resource group only.
Customizable Queuing Announcements. Unified CCX supports the playing of customizable queuing announcements based on the skill group that the call is being queued to, including announcements related to position in queue and expected delay.
Re-route on Ring No Answer. If the selected agent does not answer within the allowed time limit, the caller retains the position in queue. Any screen pop data is also preserved.
Data driven routing for HTML and XML data sources. The ability to use data obtained from HTML or XML documents to make routing decisions. XML document processing can also be used as a data store to access system-wide static data, such as a list of holidays, hours of operation, or a short list of hot customer accounts.
Agent Skill and Competency-Based Routing. Agents can be configured with specific number of skills, each with up to 10 different competency levels. Contact Service Queues (also known as skill groups) can be configured as requiring up to specific number of skills, each with up to 10 minimum skill competency levels. The Unified CCX routing logic then matches the caller and contact requirements with agent skills to find the optimum match using one of the following agent selection criteria: • Longest available, most handled contacts, or shortest average handle time • Most skilled, most skilled by weight, or most skilled by order • Least skilled, least skilled by weight, or least skilled by order
High Availability Failover. With HA failure of the active server can be detected and the ACD subsystem can automatically fail over from the active to the standby server.
Dynamic Re-skilling by Administrator or Supervisor. Changes to CSQ skills and competencies and agent skills and competencies are applied immediately.
Prioritized Queuing. Up to 10 levels of customer contacts can be prioritized based on call or customer data, and calls may be moved within or among queues under workflow control using priority information.
Agent Routing. Unified CCX routing applications can select a specific agent if that agent is in Ready state. (Queuing on a per agent basis is not supported.)
Data-driven routing based on JDBC database sources via SQL. The ability to use data obtained from a JDBC compatible database via a SQL query to make routing decisions.
Wrap-Up and Work Modes. After call completion, an agent can be configured to be automatically placed into Work state, on a per CSQ basis. The agent can also choose to enter work state if that option is provided by the agent desktop administrator. A wrap-up timer is also configurable on a per CSQ basis.
Wrap-Up Reasons. Agents may select Wrap-Up Reasons configured by the administrator.

Interactive Voice Response

The following table describes the Interactive Voice Response (IVR) features that are available in each Unified CCX package.

Table 9: IVR Features Available in Each Unified CCX Package

Feature	Premium	Enhanced	IVR License
Basic Prompt and Collect IVR. Basic IVR ports provide a queue point, custom messaging and prompting, caller input collection, and processing via DTMF decoding. Decoded DTMF input may be used for both routing and screen pop purposes. Basic call controls such as terminate, transfer, and place call are also supported as part of the basic IVR functionality. **Note** Basic IVR port and Advanced IVR port cannot be mixed in the same configuration. Advanced IVR port includes all features available in Basic IVR port.	Included as a part of advanced IVR port	Included	Included
High Availability Failover. With HA, failure of the active server can be detected and the IVR subsystem can automatically fail over from the active to the standby server. All IVR functions will be restored on the standby server. **Note** All calls in queue and calls receiving IVR call treatment will be lost. Calls already transferred to the agent will be preserved.	Optional with HA license	Optional with HA license	Optional with HA license

Feature	Premium	Enhanced	IVR License
Advanced IVR Port Database Integration. The Unified CCX server can interoperate with any JDBC-compliant database. Databases tested and supported by Cisco are listed in *Cisco Unified CCX Software and Hardware Compatibility Guide*, which is available at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html. Data retrieved from databases can be used with the conditional routing capabilities to provide customer profile-based routing and queuing. Database integration also provides the ability to offer complete self-service applications to callers. Database views are not supported using the Unified CCX Editor database steps, but database views can be accessed using Voice XML or Java logic modules.	Included	Not available	Included
Advanced IVR Ports HTTP Triggers (the web analog to Unified CM Telephony) to invoke and run a workflow. HTTP triggers enable a Unified CCX to receive a customer contact request through an HTTP request. This approach allows web users to be offered service through a "click to talk to an agent" button. Information collected using the web (a customer call back number, account number, shopping cart content, and so on) can be passed to the Unified CCX script to allow customer profile-based routing and a data-rich window. These contacts can be prioritized and routed using the same methods available to general inbound voice callers.	Included	Not available	Included
Advanced IVR Port SMTP outbound mail subsystem that may be used at run time under workflow control to send an email message. Third-party paging or fax products that accept an incoming email message to invoke a page or fax service may use this subsystem to provide real-time paging and fax responses in addition to email responses.	Included	Not available	Included

Feature	Premium	Enhanced	IVR License
Advanced IVR Port VoiceXML 2.0 Support Unified CCX supports executing application logic developed with the VoiceXML (VXML) standard. VXML is required for certain complex grammar ASR and TTS interactions and is optional for a DTMF or simple ASR or TTS voice interaction service. VXML allows organizations to reuse application logic from other applications, such as a transaction server to a mainframe database. For the complete list of supported VXML tags and attributes, see *Cisco Unified Contact Center Express Getting Started with Scripts*. **Note** Unified CCX uses MRCP v1 and MRCP v2 for communicating with third-party ASR-TTS servers. For information on compatible versions of the ASR-TTS see, *Compatibility Matrix for Unified CCX* at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.	Included	Not available	Included
Advanced IVR Port Java Support. The Unified CCX server can support the defined logic using Java. Java support allows the reuse of logic from the existing web and Java applications.	Included	Not available	Included
Advanced IVR Port Automatic Speech Recognition via MRCP. ASR provides the ability to use natural human speech to replace DTMF keypad presses as a way to interact with IVR applications.	Optional with purchase of compatible ASR product	Not available	Optional with purchase of compatible ASR product
Advanced IVR Port Text to Speech via MRCP. TTS provides the ability to use flat text files as input to a computer-generated speech engine. TTS can replace prerecorded human speech in IVR applications.	Optional with purchase of compatible TTS product	Not available	Optional with purchase of compatible TTS product
General IVR Features			
Play messages to callers: Music on hold	Included through Cisco Unified Communications Manager Music on Hold server or .wav file	Included through Cisco Unified Communications Manager Music on Hold server or .wav file	Included through Cisco Unified Communications Manager Music on Hold server or .wav file

Feature	Premium	Enhanced	IVR License
Play messages to callers: Prompts	Included through .wav file	Included through .wav file	Included through .wav file
Play messages to callers: Combine prompts, music, and messages	Included and fully customizable	Included and fully customizable	Included and fully customizable
Capture and process caller DTMF input	Included	Included	Included
Automated-Attendant support	Included and fully customizable	Included and fully customizable	Included
Database integration	Included	Not available	Included
Automatic Speech Recognition (ASR)	Optional through Media Resource Control Protocol (MRCP)	Not available	Through Media Resource Control Protocol (MRCP)
Text to Speech (TTS)	Optional through MRCP	Not available	Optional through MRCP
Real-time notification services (email; support for paging and fax)	Included (paging and fax require integration with third-party services)	Not available	Included (paging and fax require integration with third-party services)
VoiceXML for ASR, TTS, and DTMF	Included	Not available	Included
Read data from HTTP/S and XML pages	Included	Included	Included
Run workflows through HTTP/S request	Included	Not available	Included
Integrated self-service application support	Included	Not available	Included
Retrieve XML data using HTTP/S mechanism	Included	Not available	Included
Retrieve XML/JSON based data using generic REST API call	Included	Not available	Included

The following table describes the Outbound IVR features that are available with a premium package and separate Outbound IVR license which provides both predective and progressive.

Table 10: Outbound IVR Features Available with a Premium Package

Feature	Premium
System Features	

Feature	Premium
Hardware configuration	IVR Outbound Dialer is deployed co-loaded on the same virtual machine (VM) as the inbound voice server. CPA is performed on the compatible external voice gateway.
Outbound IVR Ports	
Maximum number of Outbound IVR ports supported	150
Outbound IVR Port license type	Concurrent
Outbound IVR Features	
Maximum number of active outbound campaigns	15
Maximum number of active contacts per outbound campaign **Note** Import contacts in chunks of 10,000 at a time.	100 thousand
Ability to automatically detect voice answer, answering machine, fax/modem, busy and invalid numbers	Included
Administration	
Ability for administrator to create and configure campaigns	Included
Ability for administrator to create non-North American area code to time-zone mappings	Included

The summary overview of system maximums for inbound and outbound voice in the tables are for reference only.

Multiline Support

Unified CCX supports the use of multiple lines on agent phones. You can configure one or more secondary lines on an agent phone. Unified CCX monitors first four configured lines. The agent's ACD line must be in button positions 1 - 4. Any calls on the observed lines are reported in the historical reports. Agent going Off-hook on the Non-ACD line will make the agent to Not Ready State if it is configured by the Administrator.

For example, if Agent A uses his non-ACD line to call Agent B (on Agent B's primary/ACD extension), the agent A is moved to Not Ready State and the call does not appear on Agent A's desktop. The call appears on Agent B's desktop because Agent B received the call on the primary/ACD extension.

Direct Transfer Across Line (DTAL) and Join Across Line (JAL) are not supported.

Codec Support

Unified CCX supports the following codecs:

- G.711 a-law and μ-law
- G.729

Unified CCX Outbound Dialer

Unified CCX supports the following outbound dialers with Cisco Agent Desktop:

- Unified CCX Outbound Preview Dialer
- Unified CCX Outbound IVR Dialer

Unified CCX Outbound Preview Dialer allows Outbound agents to participate in outbound campaigns in addition to handling inbound calls. This feature selects those agents who are not busy with inbound calls to handle outbound calls, which maintains a high level of agent productivity.

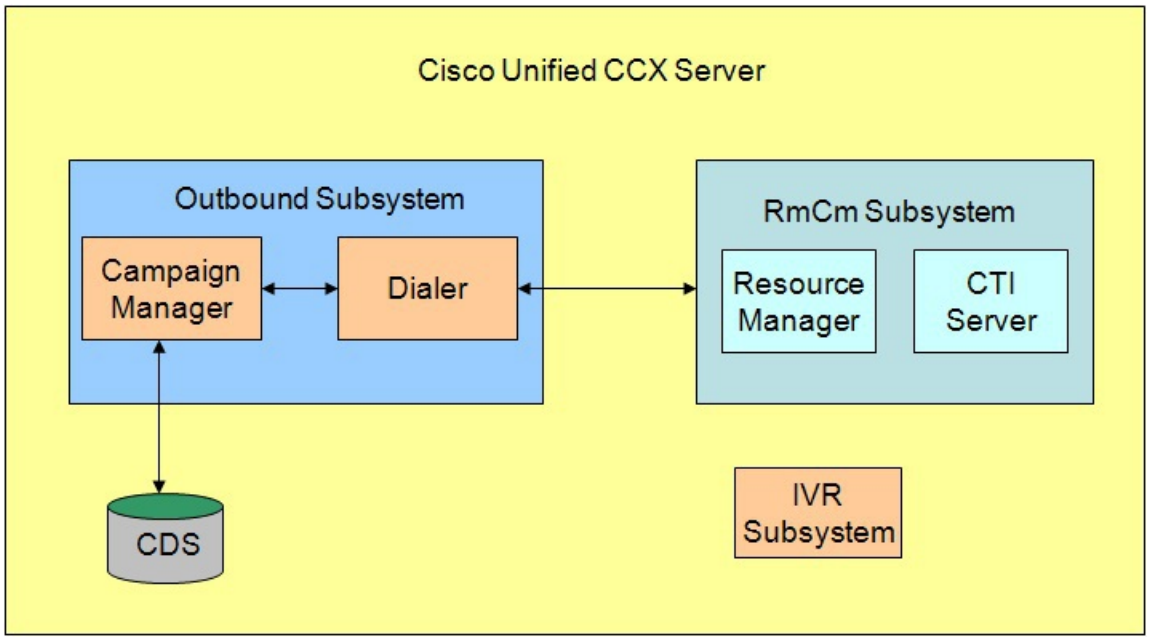
Unified CCX Outbound IVR Dialer allows for Outbound calls to be placed to contacts in a campaign and subsequently for live contacts to be serviced by an IVR application. Call Progress Analysis (CPA) capabilities of the SIP Voice gateway are used to filter non-live contacts (which could be fax and no answer). Live calls that are answered by a customer and answering machine contact are transferred to a CTI route point to be serviced by an associated IVR application. An Outbound IVR call that is answered by a customer contact but cannot be serviced due to unavailability of an IVR port is said to be abandoned.

Note Outbound dialer is not available with Cisco Finesse.

High Level Components

This figure and the following table describe the components deployed in Cisco Unified CCX for Outbound:

Figure 3: Cisco Unified Outbound Components



Campaign Manager	Responsible for starting and stopping each campaign and retrieving and updating contact records from and to the database.

Dialer	Receives contacts from the Campaign Manager and initiates the outbound calls. Notifies the Campaign Manager of the call status and call result after the call is answered. The dialer software is IP based and does not require any telephony cards for making outbound calls. In Outbound Preview, the dialer uses the Finesse agent IP phone to place outbound calls through a voice gateway configured in Unified CM. In Outbound IVR, the dialer uses the SIP protocol to place outbound calls through the SIP gateway configured for the Outbound IVR feature.
Resource Manager	Monitors agent states, reserves agents and receives instructions from the Dialer to place the outbound call. This component is used for Outbound Preview, Agent Predictive, and Agent Progressive features.
CTI Server	Handles requests and responses from and to the Finesse and passes the customer data to the Finesse for screen pop. This component is used for Outbound Preview, Agent Predictive, and Agent Progressive features.
IVR Subsystem	Responsible for execution of the IVR application associated with the campaign when a live contact has been detected by the SIP gateway and transferred to the configured CTI Route Point on the Unified CM. This component is used only in the Outbound IVR feature.
Config Datastore (CDS)	Contains the customer contacts information.

All of these components run as part of the Unified CCX Engine and cannot be installed separately.

Functional Description

There are typically four types of dialing modes in outbound ACDs: preview, direct preview, progressive, and predictive.

Outbound Preview

The Outbound Preview feature supports only the direct preview dialing mode. It uses a 3-stage process for making an outbound call. The first stage is to find an available agent and retrieve the customer information for making the outbound call. The second stage is the reservation call, and its purpose is to reserve an agent and send customer data to the agent desktop. During this stage, the agent is reserved and the data appears on the desktop so that the agent can review the data and decide whether to accept the call by pressing the corresponding button on the agent desktop. If the agent does not accept the call, the call is handled by other outbound agents or closed for the campaign. If the agent does accept the call, Outbound Preview kicks in the last stage where Unified CM is instructed to place the outbound call using the agent's phone. When the outbound call is answered, Outbound Preview updates the customer contact in the database with the call status and call result.

When the outbound call connects with the customer, the agent can perform all call control operations that are usually supported on inbound calls (transfer, conference, hold, retrieve, and so on). Ensure that the agent transfers or conferences the outbound call, only if the call is answered by a person but not through other media such as an answering machine or a fax machine.

Note CUBE is supported with the Outbound Predictive and Progressive dialers for agent and IVR with CPA (Call Progress Analysis).

Direct Preview Outbound

The Direct Preview Outbound Dialer provides campaign-based outbound preview dialer support. Each inbound Premium seat provides one outbound seat. If you have 100 agent licenses, you can have up to 100 agents logged in and up to 100 agents handling inbound and outbound calls at the same time.

The following table describes the Outbound Preview Dialer features that are available in premium Unified CCX package:

Note For the Outbound feature, the maximum number of campaigns supported is 15 and the maximum number of supervisor positions supported is 42.

Table 11: Direct Outbound Preview Features Available for Unified CCX Premium Package

Feature
System Features **Note** These features are the same as for inbound voice with the exception of redundancy.
Hardware configuration Deploys and runs co-loaded on the same virtual machine as the inbound voice server.
Outbound Voice Seats
Maximum number of active outbound agents supported: 150
Outbound license type: Concurrent user
Outbound Preview Dialer Features
Maximum number of active outbound campaigns: 15
Integrated CTI and Screen Pop Features with Cisco Unified Contact Center Express Seat License
Populates customer's name, account number, and phone number dialed
Cisco Finesse Features for Agent with Cisco Unified Contact Center Express Seat License
Workflow-based recording
Ability for supervisor to use Silent Monitor, Barge-In, and Intercept
Ability for agent to accept or reject outbound contact. Agent can reclassify call to anyone of many call results, such as busy, fax, and answering machine.
Cisco Finesse Features for Supervisor with Cisco Unified Contact Center Express Seat License
Live Data Gadgets Silent Monitor: Listen in on an agent's call
Barge-In: Join in on an agent's conversation
Intercept: Take a call from an agent

Record: Optional with Webex WFO, or WFO Solutions Plus
Integrated Historical Reporting with Cisco Unified Contact Center Express Seat License
Administration
Campaign Management: Administrators can create and configure campaigns. They can specify a daily time range during which outbound calls are made and a set of CSQ to specify whose agents make the outbound calls, They can also specify and import a list of customer contacts to be called.
Area Code Management: Administrators can add mappings from area-code to time zone for non-North American locations. This information is used to determine the customer contact current time before placing an outbound call.

Outbound Progressive and Predictive Dialer

The Unified CCX Outbound Progressive and Predictive Dialer provides campaign-based agent outbound progressive and predictive dialer support. The number of agent seats depends on the number of outbound licenses available. If you have 10 outbound licenses, you can have up to 10 concurrent agent seats to handle outbound calls and 10 concurrent outbound IVR calls.

The following table describes the Outbound Progressive and Predictive features that are available for the Outbound License with the premium package.

Note For the Outbound feature, the maximum number of campaigns supported is 15 and the maximum number of supervisor positions supported is 42.

Table 12: Outbound Progressive and Predictive Dialer Availability with Premium Package and an Additional Outbound License

Feature
System Features **Note** These features are the same as for inbound voice with the exception of redundancy.
Hardware configuration Deploys and runs co-loaded on the same virtual machine as the inbound voice server.
Outbound Voice Seats
Maximum number of active concurrent agents supported: 150
Outbound license type: Concurrent user
Outbound Progressive and Predictive Dialer Features
Maximum number of CSQs per outbound campaign: 10
Cisco Finesse Features with Cisco Unified Contact Center Express Seat License
Workflow-based recording

View agent activity in real time
Cisco Finesse Features for Supervisor with Cisco Unified Contact Center Express Seat License
Silent Monitor: Listen in on an agent's call
Barge-In: Join in on an agent's call
Intercept: Take a call from an agent
Integrated Historical Reporting with Cisco Unified Contact Center Express Seat License See the Cisco Unified Contact Center Express Reporting Guide at: http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list
Integrated Live Data Reporting with Cisco Unified Contact Center Express Seat License See the Cisco Unified Contact Center Express Reporting Guide at: http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list
Administration
Campaign Management: Administrators can create and configure campaigns using Unified CCX Administration we interface and REST APIs

Outbound IVR and Agent

The Outbound IVR feature supports two types of dialing modes namely progressive and predictive. Each dialer dials an appropriate number of contacts to make efficient use on the available system resources (IVR Ports). Both algorithms use a ratio called lines per port (LPP) to determine the number of outbound calls to place per available IVR port.

Progressive algorithm uses an LPP value configured by the administrator through Unified CCX Administration.

Predictive algorithm dynamically varies the LPP to ensure that the abandon rate does not exceed the threshold configured through Unified CCX Administration (abandon rate is the percentage of live calls that had to be dropped due to the unavailability of an IVR port).

Outbound IVR uses the Call Progress Analysis (CPA) capability of the SIP gateway to place and filter outbound calls. The SIP gateway filters out non-live contacts such as fax, invalid number, and no answer and forwards only the live calls answered by a customer contact and answering machine to a CTI Route Point on the Unified CM. This operation in turn triggers execution of an IVR application associated with the campaign at Unified CCX.

Note You can use the IVR campaign only with service providers that work with TDM, because such gateways support CPA capability, which is an IVR feature. Gateways using SIP or H323 trunks does not support CPA; the IVR campaign does not work with these service providers.

The following table describes the Outbound IVR features that are available with a premium package and separate Outbound IVR license which provides both predictive and progressive.

Scalability

Outbound Preview supports different capacities and limits when compared to inbound agents.

For outbound IVR, the number of active outbound IVR ports is limited by the maximum number of outbound IVR ports that are supported for a given platform. In addition, the sum of the active IVR ports in use for inbound and outbound cannot exceed the maximum number of IVR ports that are supported for the platform.

Because IVR for inbound and outbound contend for the same set of IVR ports, the actual number of active IVR ports in use for inbound and outbound depends on multiple parameters:

- Number of licensed inbound ports
- Number of licensed outbound ports
- Sum of the number of ports dedicated across outbound IVR campaigns

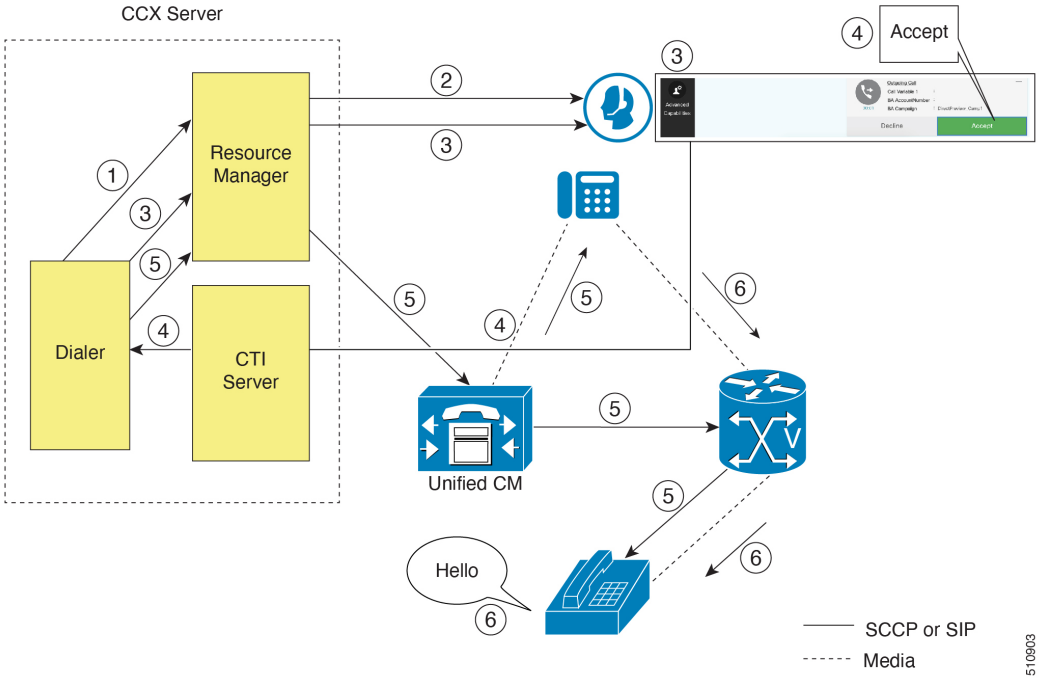
Refer to the "Configuring Unified CCX Dialer" chapter of the *Unified CCX Administration Guide* for details on how the numbers of active IVR ports for inbound and outbound are determined by the above parameters.

Call Flow Description

Direct Preview Mode

In the direct preview mode, the agent hears the ring-out on the agent phone. The direct preview call flow proceeds as illustrated in this figure and the description that follows:

Figure 4: Call Flow for Direct Preview Mode



1. An agent in Ready state is available and the Dialer has retrieved contact records from the Campaign Manager. The Dialer requests the Resource Manager to reserve the agent.

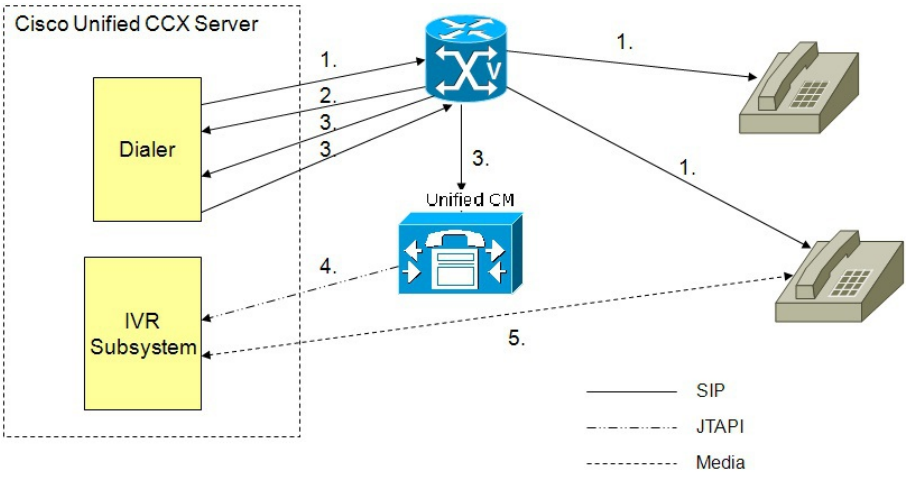
2. The Resource Manager reserves the agent by moving the agent to Reserved state.
3. The Dialer sends a reservation call to the agent desktop and, at the same time, a screen pops that contains the customer information and is presented to the agent. The agent reviews the customer data and decides whether to take the call.
4. The agent can choose to accept, skip, or cancel this reservation call. If the agent chooses to accept it, the agent clicks the Accept button on the desktop.
5. The Dialer instructs the Resource Manager to place an outbound call from the agent phone through Unified CM out to the voice gateway. Because this call is a direct preview call, the agent immediately hears the ringback of the customer phone.
6. As soon as the call is answered, the Dialer closes the contact, classifies it as a voice call and sends the result to the Campaign Manager. If an answering machine answers the call, the number is invalid, or the customer requests a callback, and the agent can reclassify the call from the desktop accordingly. If the customer requests a callback and the agent reclassifies the call, the customer is called back using the same number, an alternate number, or a callback number specified by the customer.

Note A CTI Port is not required to place the outbound call.

IVR Mode

The call flow description for Outbound IVR is illustrated in this figure and the description that follows.

Figure 5: Call Flow for IVR Mode



1. Outbound IVR dialer determines the number of contacts to dial per the configured algorithm (progressive or predictive) and places outbound calls using SIP through the voice gateway.
2. Voice gateway detects non-live contact through its CPA capabilities and sends status of non-live contact to the dialer. The dialer uses this to update contact status information in the configuration database.
3. Voice gateway detects live contact through its CPA capabilities and sends status of live contact to the dialer. The dialer uses this to update contact status information in the configuration database and also

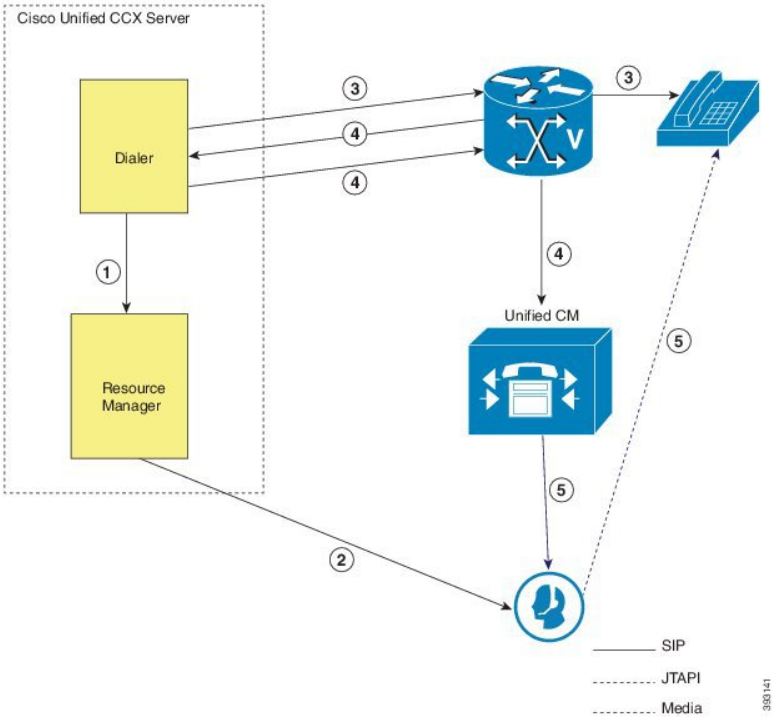
sends a SIP refer message to the SIP gateway which in turn transfers the call to the configured CTI Route Point on Cisco Unified CM.

4. Cisco Unified CM transfers the call to a IVR port on Cisco Unified CCX server.
5. The IVR subsystem then associates the call with the IVR application associated with the campaign. The engine starts execution of the application and an IVR session takes place between the IVR application for the campaign on Cisco Unified CCX and the customer contact.

Agent Mode

The call flow description for Agent Outbound is illustrated in this figure and the description that follows.

Figure 6: Call Flow for Agent Mode



1. The dialer requests the Resource Manager to reserve the agent.
2. The Resource Manager reserves the agent by moving the agent to Reserved state.
3. Outbound dialer determines the number of contacts to dial as per the configured algorithm (progressive or predictive) and places outbound calls using SIP through the voice gateway.
4. The voice gateway detects live contact through its CPA capabilities and sends status of live contact to the dialer. The dialer uses this information to update contact status information in the configuration database and also sends a SIP refer message to the SIP gateway, which then transfers the call to the Cisco Unified CM.
5. Cisco Unified CM transfers the call to the reserved agent on Cisco Unified CCX server. The Outbound subsystem then associates the call to the reserved agent.

Deployment Guidelines

The following guidelines should be followed when deploying outbound:

- Outbound supports a maximum of 15 active campaigns and a maximum of 100 thousand active outbound records for each campaign.
- Outbound does not come preinstalled with any Do Not Call lists. The system administrator should manually filter the contact list against the Do Not Call list prior to importing contacts.

The following guidelines are specific to outbound:

- Outbound supports a maximum of 10 CSQs for each campaign.
- Finesse IPPA agents are not supported.
- Direct preview outbound cannot detect an answering machine, fax, or modem. The agent should manually reclassify the call to “answer machine” or “fax” from the desktop. The contact will be called again using the same number (in the case of “answer machine”) or using an alternate number (in the case of “fax”).
- For direct preview outbound, agents should not transfer or conference the outbound call if the call is answered by the media other than a person, such as an answering machine or fax machine.
- For progressive and predictive outbound, the SIP gateway performs call progressive analysis which determines whether the outcome of a call is an answering machine, live voice, fax, or beep tone and presents only the live voice calls to the agents. The contact will be called again using the same number in case of no answer and busy tone or using an alternate number in case of a fax, modem or an invalid number.
- When Phone 1 of a contact is dialed and the CPA marks it as Busy or Unanswered the same number is retried based on the retry count and delay configured in the campaign. When the retry count reaches the maximum value, the contact is marked as closed. The other phone number for a given contact is dialed only when the called number is classified as Modem, Fax or Invalid.

The following guidelines are specific to IVR and agent-based progressive and predictive outbound:

- It is possible to only have a single instance of the SIP gateway in the deployment.
- Install the SIP gateway on the same site (that is, the same campus LAN) as the Unified CCX primary engine. The SIP gateway can be installed across the LAN or WAN. The maximum delay over the WAN should not exceed 80 milliseconds.

Note The primary engine is always the first node that was installed in the Unified CCX cluster and cannot be changed.

- No voice gateway based redundancy of the SIP gateway is supported.
- The protocol supported between the SIP Gateway and Unified CM for transferring the outbound call to an IVR application or to an available agent includes SIP and H323.
- It is possible to use the same gateway for both inbound and outbound voice.

Unified CCX Chat

The different types of chat media channels available in Unified CCX are:

- **Web Chat**

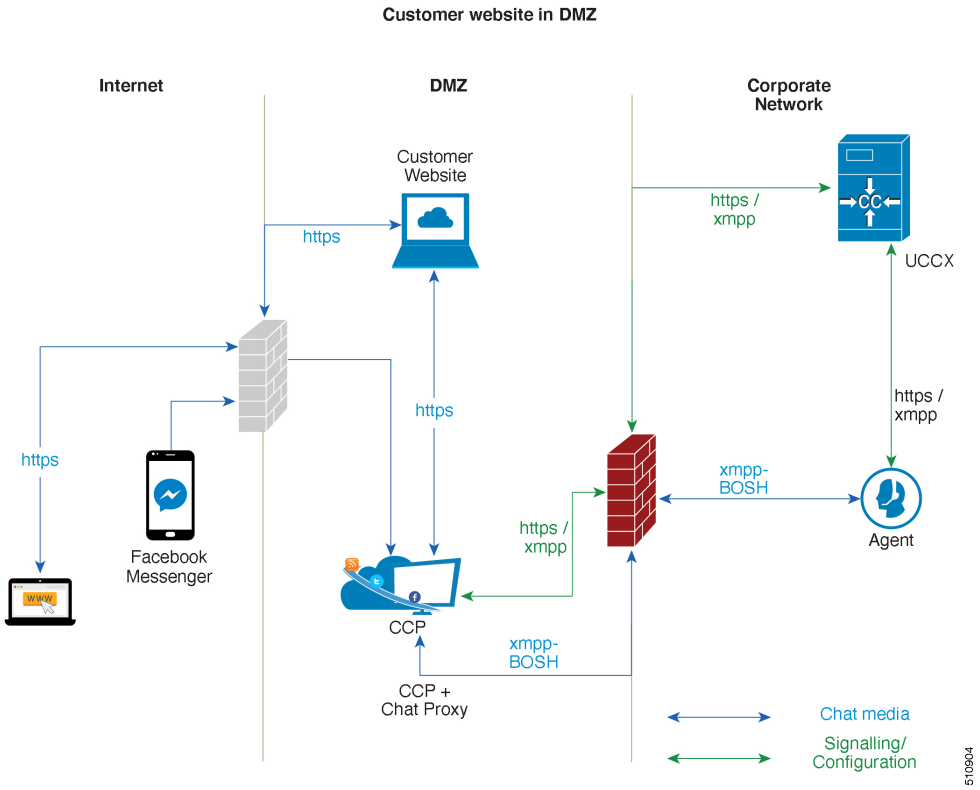
  Unified CCX agents can service customer chat requests using the Web Chat gadget in Cisco Finesse. Customers can initiate a chat session from the organization website. The chat web form is hosted on the organization website that enables the customers to initiate a chat.

- **Chat - Facebook Messenger Integration**

  Unified CCX agents can service Facebook Messenger chat requests from Facebook users. Customers can initiate a chat session from their Facebook account through Messenger. The business entity must have a Facebook page of its own with Messenger enabled. For more details on configuration see, Cisco Unified Contact Center Express Administration and Operations Guide.

Deployment Scenario 1: Customer Web Site in Demilitarized Zone (DMZ)

Figure 7: Customer Web Site in DMZ



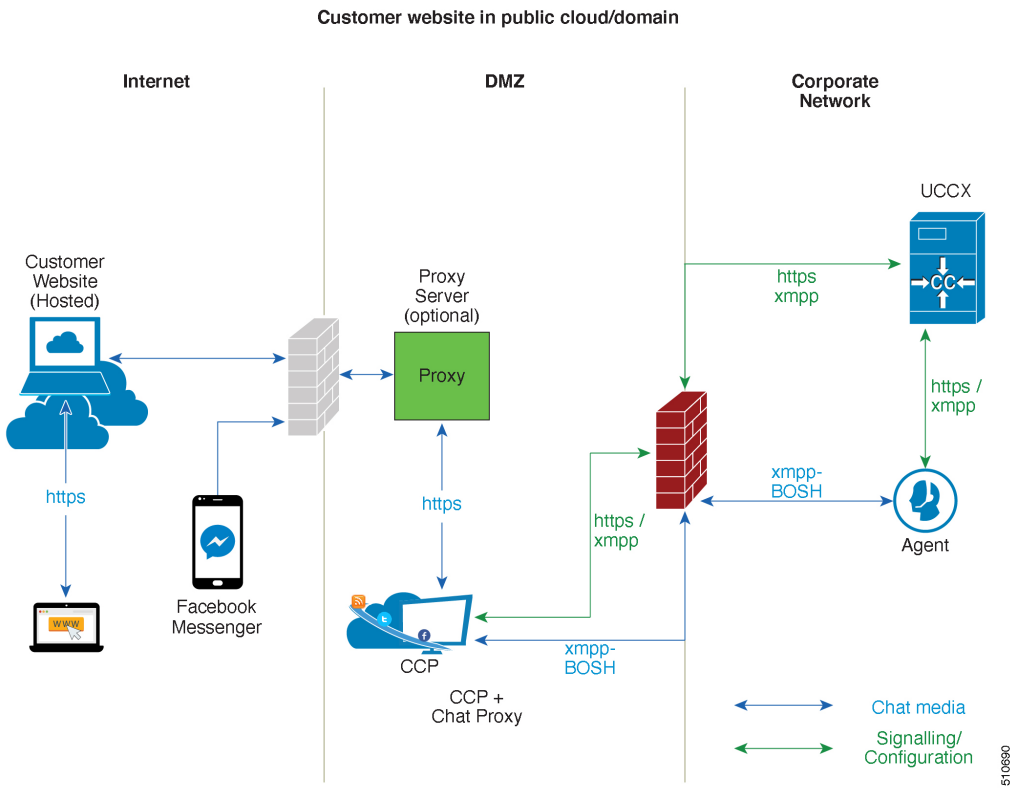
The Cisco Unified CCX is deployed inside the enterprise firewall and Customer Collaboration Platform is deployed inside company premises in the DMZ along with the customer website. The DMZ is open to all HTTPS traffic from the Internet. For Unified CCX Web Chat deployment to work, allow bidirectional HTTPS traffic between End User and Customer Collaboration Platform. Upload Customer Collaboration Platform certificate to the Unified CCX Tomcat trust store. Allow bidirectional HTTPS and XMPP traffic between Customer Collaboration Platform in the DMZ and Unified CCX on ports HTTPS (443) and XMPP (5222).

Allow bidirectional BOSH traffic between CCP and the agent on port BOSH (7443). Allow unidirectional HTTPS traffic inward from Internet to Customer Collaboration Platform Chat Gateway webhook interface (10443). For more information on the ports utilized, see the *Port Utilization in Customer Collaboration Platform* section in the Port Utilization Guide for Cisco Unified Contact Center Express Solutions.

The Unified CCX is shielded from all outside traffic except the traffic coming from the DMZ zone. All web chat communications occur over HTTPS and BOSH ports irrespective of where Customer Collaboration Platform is deployed.

Deployment Scenario 2: Customer Web Site in Public Cloud or Domain

Figure 8: Customer Web Site in Public Cloud or Domain



One variation of the preceding scenario can be an addition of a proxy server that can intercept and relay all interactions going to Customer Collaboration Platform.

Note Customer Collaboration Platform should only need to access a proxy server if it sits behind a corporate network firewall and has to use an http or https proxy server for accessing an outside network. Configuration of private NAT address is not supported between Customer Collaboration Platform and Unified CCX.

Unified CCX Chat Features

The following table describes the chat features that are available in premium package.

Table 13: Chat Features Available in Premium Package

Feature
Auto chat reject. If no agent is available, the chat request is rejected.
Chat Timeouts. Session timeouts for chat inactivity and maximum wait period.
Toaster Notification. When the Cisco Finesse Desktop session is inactive, the agent receives a toaster notification for a new chat.
Multiple Chat Sessions. Administrators can configure up to a maximum of five concurrent chat sessions per agent.
Predefined Responses. Administrator can configure up to 500 Predefined Responses across chat and email. These Predefined Responses can be tagged Global or with up to 10 CSQ tags.
Multiple skills per chat agent. Multiple skills can be assigned to agents handling chat.
Blended voice, chat, and email agents. Agents can be configured for blended voice, chat, and email.
Offer voice calls when on chat. Agents can be offered voice calls when on voice chat.
Offer chat when on voice calls. Agents can be offered chat when on voice calls.
Wrap-Up Reasons. Agent can apply a maximum of five (5) Wrap-Up Reasons to the chats.
Group Chat. Agent can involve another agent in an ongoing chat session to support the customer.
Dedicated chat agents. Agents can be configured to handle only chat.
Separate voice and non-voice state model . Ability to set the Agent State for Voice, Email and Chat.
Chat Routing. Supports Agent skill and competency-based routing. • Longest available • Most skilled • Agent skill based routing
Dynamic reskilling. Changes to CSQ skills and competencies and agent skills and competencies are applied immediately.
Conditional routing. Chat is queued to the appropriate CSQ based on the problem statement selected by the customer.
Rerouting the chats that were not accepted. If the allocated agent does not accept chat within the allowed time limit, the contact is presented to another agent.
Customizable queuing messages. Customizable messages.
High Availability (HA) failover. With Unified CCX in HA, failure of the active server can be detected and the nonvoice subsystem can automatically fail over from the active to the standby server. However, Customer Collaboration Platform is not supported in HA.

Feature
Plain text. Only plaintext chat and predefined responses are supported.
Live Data and Historical Reports. See the Cisco Unified Contact Center Express Reporting Guide available at: http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html
Supervisor Reports. Team report for CSQ and agents. Agent statistics and CSQ statistics for chat.

Group Chat

The group chat feature is used when the agent would like to involve another agent in an ongoing chat session to support the customer. This can be used for seeking further information or support for the ongoing chat. A group chat enables an agent to:

- Send a chat invite to an available agent of the selected CSQ.
- Enter the summary of the ongoing chat for the other agent. This helps the agent to understand the background of the ongoing chat.
- Accept or decline the incoming group chat invitation.

Few reporting considerations for the Group Chat feature are:

- The Historical reports, **Chat Agent Details Report** and **Chat Agent Summary Report** reflect the chat session information handled by the agents only after the contact is ended.
- In Chat Agent Details Historical report (in the case of group chat):
  - **Chat Routed CSQ** column will show the name of the csq to which the chat contact was initially injected to the agents.
  - **Chat Type** column will show as 'group chat' for the agents whoever is involved in a group chat.
- Contacts Abandoned count will now also include the Group Chat contacts which the customer ends while it is being offered to the second Agent.

Unified CCX Web Chat

As part of the Premium license, Unified CCX agents can service customer chat requests using the Agent Web Chat gadget in Cisco Finesse.

This feature requires a Customer Collaboration Platform deployment to accept and relay the contact requests from a customer website. One Customer Collaboration Platform deployment can serve only one Unified CCX deployment (single node or high availability deployment). Customer Collaboration Platform does not support redundancy.

Note The Chat Web Form that is generated uses JavaScript. The web page where this is loaded must be accessed using a JavaScript enabled browser. The default Chat Web Form displays a message to the user if JavaScript is not enabled on the browser where it is loaded.

An audio alert is played when the agent receives a new chat request or when there is a new message on an inactive chat session tab. With multiple chat session tabs, the selected chat session tab is considered as active. All other chat session tabs are considered as inactive.

Web Chat Features

The following table describes the web chat features in addition to the chat features that are available in premium package.

Table 14: Web Chat Features Available in Premium Package

Feature
Agent Alias. During a chat session, the customer sees the alias that has been configured for the agent by the administrator. The Agent Alias now supports the character, Space.
Typing Indicator. The agent or customer can see when the customer or agent is typing a message.
Chat Transcript. Chat transcripts can be downloaded by the customer after the chat session. Administrators can login to Customer Collaboration Platform to retrieve chat transcripts.
Visual Customization of the Chat Form. A customizable customer chat form.
Post Chat Rating The customers can rate the chat experience after chat is ended.

Facebook Messenger Integration

This feature integrates Facebook Messenger as a customer-side channel with Unified CCX Web Chat feature (using Cisco Customer Collaboration Platform) as an out-of-box feature. Facebook users can now contact the customer care of a business entity on Facebook page of the business entity.

To integrate Facebook Messenger with Unified CCX, you must ensure that the following conditions are met:

- Business entity must have a public Facebook page for their business.
- The endpoints like, Cisco Customer Collaboration Platform or a reverse proxy must have valid Certificate Authority signed SSL certificates as they are exposed publicly to the Internet.
- A new Facebook App is created on the Messenger platform. For more details on creation of the Facebook app and Messenger setup see https://developers.facebook.com/docs/messenger-platform.
- A new unidirectional HTTPS 10443 port must be able to accept incoming HTTPS connections from Facebook.

Note Customer Collaboration Platform Chat Gateway supports only TLS 1.2 version.

- A valid CA signed certificate must be uploaded to the Tomcat certificate store of Cisco Customer Collaboration Platform or publicly exposed host.

Chat - Facebook Messenger Features

The following table describes the Facebook Messenger chat features in addition to the chat features that are available in premium package.

Table 15: Facebook Messenger Chat Features Available in Premium Package

Feature
Typing Indicator. The customer can see when the agent is typing a message. However, the agent can't see when the customer is typing a message.
Group Chat. Agent can involve another agent in an ongoing chat session to support the customer. However, the user using Facebook Messenger cannot distinguish individual agents in a group chat.
Post Chat Rating The customers can rate the chat experience on a scale of 1 (worst) to 5 (best) after the chat is ended.

Unified CCX Agent Email

As part of the Unified CCX Premium license, Unified CCX supports agent email with Finesse.

Administrators should edit the Cisco Finesse Desktop Layout to enable the gadgets to appear on the agent desktop.

As part of the Premium license, Unified CCX agents can service customer email requests using the Agent Email gadget in Cisco Finesse

For more information, see “Cisco Finesse” section in the *Cisco Unified Contact Center Express Administration and Operations Guide* at :

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

The Agent Email feature requires the deployment of Cisco Customer Collaboration Platform to handle the email and relay the contact requests from a mail server. One Customer Collaboration Platform deployment can serve only one Unified CCX deployment (single-node or high-availability deployment), and vice versa.

The Agent Email feature requires the use of an external mail server (Microsoft Exchange 2013, 2016, 2019, Office 365, and Gmail are supported). This mail server is not provided, installed, or configured as part of the Unified CCX installation. To communicate with the Exchange Server, Customer Collaboration Platform uses secure IMAPS (for message retrieval) and secure SMTP (for message sending). On the Exchange Server, enable IMAPS (SMTP is enabled by default).

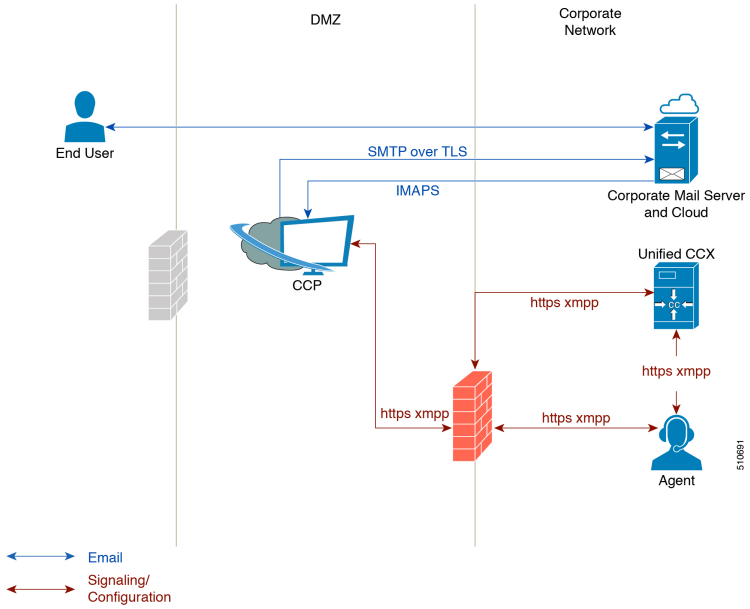
For more information about enabling IMAPS, see section “Mail Server Configuration” in *Cisco Unified Contact Center Express Administration and Operations Guide* at:

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

For details on the integration of Unified CCX with Customer Collaboration Platform for Agent Email see, https://www.cisco.com/c/en/us/support/docs/customer-collaboration/socialminer/200892-Integrate-UCCX-with-SocialMiner-for-Agen.html.

For details on the unsupported configurations in integration of Unified CCX with Customer Collaboration Platform see, https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/211530-Unsupported-configurations-for-UCCX-and.html.

Figure 9: Customer Web Site in DMZ



Unified CCX allows email contacts to be routed to agents based on the email addresses to which they are sent by the customers. Cisco Finesse Agent Email feature uses skill-based routing and last-agent email routing.

Separate CSQs are required for Email. You must associate each Email CSQ with a separate email account on the mail server. This account must be dedicated to the Email CSQ feature and must not be used for other purposes. Agent association with Email CSQs is configured in the same manner as Voice CSQs by assigning skills and competency levels to the CSQ.

Cisco Finesse provides a common chat and email state, separate from voice state. Blending ensures that agents can handle voice, email, and chat contacts from the same desktop.

When an agent replies to a customer's email, the reply email is always in HTML format. The email address depends on the information in the customer's email. If the customer's email contains the Reply-to header field, the agent's reply email is sent to the email address in the Reply-to header. If the Reply-to header is missing in the customer's email, the agent's reply email is sent to the From address in the customer's email. The sender address of agent's email is the email account associated with the Email CSQ from which the reply is being sent. Upon requeue, Unified CCX ensures that the response is sent with the email address of the requeued CSQ as the From address.

Agent Email Features

The following table describes the email features that are available with the premium package.

Finesse Email is available with Microsoft Exchange, Office 365, and Gmail with a Cisco Customer Collaboration Platform configured within Unified CCX.

Table 16: Agent Email Features Available with Premium Package

Feature
Fully integrated with Cisco Finesse agent desktop.

Feature
Visible alert. Email alert along with pending email count.
Toaster Notification. Toaster Notification. Agent receives a notification when a new email is received when the Cisco Finesse Desktop is not active.
Auto accept email. Incoming emails are automatically presented to the agent without any explicit accept (button click).
Email contact handling Agents can be configured to handle up to five email contacts.
Requeue email. Agent can re-queue an email to another CSQ.
Reply To Header. If the Reply To header is present, the agent's response is sent to that address. Otherwise, it uses the From address of that email to respond.
Reply To, Reply All, Cc, Bcc, Forward Agent can respond to the from email address, edit the **To** field, can add email addresses in the **Cc** and **Bcc** fields to mark copy or blind copy to other contacts, do a **Reply All** to all the email addresses existing in the email, and **Forward** the email to any other email address.
Save drafts. The system periodically saves the email drafts.
Discard email. Discards email from the agent desktop, but mails are not deleted from the server.
Rich Text. Rich text is available for the email body, predefined response and email signature.
Predefined Responses. Administrator can configure up to 500 Predefined Responses across chat and email. These Predefined Responses can be tagged Global or with up to 10 CSQ tags.
Email Signatures Administrator can configure email signatures for the Global CSQs and Multiple CSQs. The email signatures can be tagged Global or Custom to upto 10 CSQs.
Wrap-Up Reasons. Agents can select Wrap-Up Reasons for the emails handled by them. A maximum number of five (5) Wrap-Up Reasons can be selected. Wrap-Up Reasons are available only after the Administrator has configured the same for the CSQs.
Attachments. Supported. **Attachment size limit** The total attachment file size limit in an agent's reply is 20MB. The size limit of a single file attachment is 10 MB. The total size limit of attachments in the incoming email from the customer is 20 MB. **Note** The email attachment size limit must be configured on the mail server.
Historical Reports. See the *Cisco Unified CCX Reporting Guide* for more details on the reports at, http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html.
Email Live Data Reports. See the *Cisco Unified CCX Reporting Guide* for more details on the reports at, http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html.

Feature
Microsoft Exchange. Supported email service. This must be purchased separately by customer.
Dedicated or Blended email agents. Agents can be configured to handle emails only or both, email and chat.
Email Routing. • Last Agent Email Routing where an attempt is made to route an email to the last agent who handled the email last. • Skill and competency based routing that applies to new emails or when Last Agent Email Routing expires. • The longest available or most skilled agent selection algorithm.
Dynamic reskilling. Changes to CSQ skills and competencies and agent skills and competencies (either through Admin interface or Advanced Supervisor Capabilities in Finesse) are applied immediately. Emails that are currently being worked by the agents are not affected.
High Availability (HA) failover. HA is supported in Unified CCX. Upon Unified CCX failover, all emails in the system are automatically requeued and rerouted. Emails are presented to the agents after the failover.
Keyboard shortcuts. Use the keyboard shortcuts for easy access to the Cisco Finesse agent and supervisor desktop features. The keyboard shortcuts are available for both agent and supervisor.

Reporting

Cisco Unified Intelligence Center is the web-based reporting platform for Cisco Unified CCX. Cisco Unified Intelligence Center is available with Unified CCX packages. To use Cisco Unified Intelligence as standalone reporting, use the Cisco Unified Intelligence Premium license.

Unified Intelligence Center

Unified Intelligence Center is the reporting solution for Unified CCX that provides access to Historical reports and Live Data reports.

Note

- Historical Reporting Client (HRC) is no longer available with Unified CCX.
- Co-resident CUIC on Unified CCX provides the capability to customize reports or to restrict value list collections by implementing custom report definitions.
- Standalone CUIC on premise server doesn't provide the access to view Live Data Reports.
- During a manual or nightly Unified CCX synchronization with Unified Intelligence Center, the collections that are manually added to the default stock value lists (UCCX_AgentID, UCCX_AgentName, UCCX_TeamNames, UCCX_CSQ Names, UCCX_Voice_CSQ, UCCX_Email_CSQ, UCCX_Chat_CSQ_List) are deleted.

Unified Intelligence Center Historical Reports

The following table presents the Historical reports that are available for each license package:

Historical reports	Premium	Enhanced	IP-IVR
Inbound reports			
Abandoned Call Detail Activity Report	Yes	Yes	Yes
Aborted Rejected Call Detail Report	Yes	Yes	Yes
Agent Call Summary Report	Yes	Yes	No
Agent Detail Report	Yes	Yes	No
Agent Login Logout Activity Report	Yes	Yes	No
Agent Not Ready Reason Code Summary Report	Yes	Yes	No
Agent State Detail Report	Yes	Yes	No
Agent State Summary by Agent Report	Yes	Yes	No
Agent State Summary by Interval Report	Yes	Yes	No
Agent Summary Report	Yes	Yes	No
Agent Wrap-up Data Summary Report	Yes	Yes	No
Agent Wrap-up Data Detail Report	Yes	Yes	No
Call Custom Variables Report	Yes	Yes	Yes
Called Number Summary Activity Report	Yes	Yes	Yes
Common Skill CSQ Activity report	Yes	Yes	No
Contact Service Queue Activity by CSQ Report	Yes	Yes	No
Contact Service Queue Activity by Window Duration	yes	Yes	No
Contact Service Queue Activity Report	Yes	Yes	No
Contact Service Queue Activity Report by Interval	Yes	Yes	No
Contact Service Queue Call Distribution Summary	Yes	Yes	No
Contact Service Queue Priority Summary	Yes	Yes	No
Contact Service Queue Service Level Priority Summary Report	Yes	Yes	No
CSQ Agent Summary Report	Yes	Yes	No
Detailed Call by Call CCDR Report	Yes	Yes	Yes
Detailed Call CSQ Agent Report	Yes	Yes	No

Historical reports	Premium	Enhanced	IP-IVR
Priority Summary Activity Report	Yes	Yes	No
Traffic Analysis Report	Yes	Yes	Yes
Agent All Fields Report	Yes	Yes	No
Contact Service Queue Activity by Window Duration	Yes	Yes	No
CSQ All Fields Report	Yes	Yes	No
Reason Code Report by Agent Grouping	Yes	Yes	No
Reason Code Report by Reason Code Grouping	Yes	Yes	No
Chat reports			
Chat Agent Detail Report	Yes	No	No
Chat Agent Summary Report	Yes	No	No
Chat CSQ Activity Report	Yes	No	No
Chat CSQ Agent Summary Report	Yes	No	No
Chat Traffic Analysis Report	Yes	No	No
Email reports			
Email Agent Activity Report	Yes	No	No
Email Contact Detail Report	Yes	No	No
Email CSQ Activity Report	Yes	No	No
Email Traffic Analysis Report	Yes	No	No
Outbound reports [1]			
IVR Outbound Campaign Summary Report	Yes	Yes	Yes
IVR Outbound CCDR Report	Yes	Yes	Yes
IVR Outbound Half Hourly Report	Yes	Yes	Yes
Preview Outbound Agent Detail Performance Report	Yes	Yes	Yes
Preview Outbound Campaign Summary Report	Yes	Yes	Yes
System reports			
Application Performance Analysis Report	Yes	Yes	Yes
Application Summary Report	Yes	Yes	Yes
License Consumption Report	Yes	Yes	Yes

[1] Obtain IVR-Outbound license that is optional with the Premium license to access IVR-Outbound reports.

Unified Intelligence Center Live Data Reports

The following table presents the Live Data reports that are available for each license package:

Live Data Reports	Premium	Enhanced	IP-IVR
Agent reports			
Agent CSQ Statistics Report	Yes	Yes	No
Recent State History	Yes	Yes	No
Recent Call History	Yes	Yes	No
Agent Statistics Report	Yes	Yes	No
Agent Team Summary Report	Yes	Yes	No
Supervisor reports			
Team State Report	Yes	Yes	No
Team Summary Report	Yes	Yes	No
Voice CSQ Agent Detail Report	Yes	Yes	No
Voice CSQ Summary Report	Yes	Yes	No
Email Agent Statistics Report	Yes	No	No
Email CSQ Summary Report	Yes	No	No

Note

- The team that accesses Live Data reports has a maximum limit of 20 logged in agents at any particular time.
- A maximum number of 42 users are supported to run Live-Data Reports concurrently on Cisco Unified Intelligence Center.
- All the Live Data reports are available as gadgets. For more information to configure gadgets, see the *Cisco Unified Contact Center Express Administration and Operations Guide* located at http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html.
- Live Data counters in the Unified Intelligence Center reports and the Cisco Finesse gadgets are reset in the following scenarios:
  - Manual reset—Administrator resets the real-time report counters from the Application Administration interface.
  - Automatic reset—Daily purge resets the real-time report counters at midnight (in the local Unified CCX server time zone). The reset of report counters has an impact on the reports of all the agents. However, the impact is prominent in the reports of the agents who are not in server time zone. For example, In the Team State Report, the Login Duration of an agent is calculated since midnight. After the reset, the report has a major impact for agents who are not in server time zone.

  If there are active calls at the time of reset, the Contact Service Queue (CSQ) reports display data for the calls, and the agent report counters are set to zero.
- Unified CCX Engine updates the changed records every three seconds. The unchanged records are updated every 15 seconds so that the sliding window fields (such as, **Average Talk Time-Long Term**, **Average Talk Time-Short Term** in Team Summary report) have the updated data.

  A sliding window is a time period that stretches back in time from the present. For example, the **Average Talk Time-Long Term** field with a sliding window of 30 minutes indicates the average time that an agent spent in Talking state in the last 30 minutes.
- In Live Data reports, the time in the auto increment fields (such as **Login Duration** in Team Summary report, **Total Talk Time** in Agent Statistics report) is incremented every second. When there is an update from Unified CCX Engine, there may be fluctuations in these fields. The time may advance by few seconds and revert to the actual time published by Unified CCX Engine.
- Live Data reports are not updated dynamically if configuration changes are made to CSQ, team, or agents. Refresh the report to see the latest changes.
- Live Data reports do not support team names and CSQ names that have multi-byte characters. Such team names and CSQ names are not synced from Unified CCX to Unified Intelligence Center, but user names are synced.

Finesse Reports

Agents and supervisors can access Live Data reports that are configured to be displayed as gadgets in the desktops. The following are the default reports that are configured:

Agent desktop

- Home tab
  - Agent CSQ Statistics Report
  - Agent Team Summary Report
- My Statistics tab
  - Agent Statistics Report
  - Recent Call History

Supervisor desktop

- Team Data tab
  - Team Summary Report—Short and Long Term Average
  - Team Summary Report—Since Midnight
- Queue Data tab
  - Voice CSQ Agent Detail Report
  - Voice CSQ Summary Report

Note To add or modify the report gadgets, contact your administrator. For more information, see available here:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Wallboards

Unified CCX supports wallboard reporting. Obtain the wallboard from a Cisco-approved vendor from Cisco Marketplace:

https://marketplace.cisco.com

Recording

The following recording options are available:

- Cisco Finesse workflow-based recording using Webex WFO (Workforce Optimization).

Note While using the Webex WFO recording option, you must have the Compliance Recording/Quality Management licenses.

The following table details the various recording features that are supported based on the type of recording options available:

Feature	Recording using Webex WFO	Recording using WFO Solutions Plus applications
Audio Recording	Supported	Supported
Video Recording	Not Supported	Supported
On Demand Recording	Supported	Supported
Quality Management	Supported	Supported

Note The licenses required for the recording options mentioned in the above table are:

- For recording using Webex WFO, Webex WFO licenses are required.
- For recording using WFO Solutions Plus applications, licenses on Unified CCX for Workflow based recording and Solutions Plus WFO licenses are required.

Webex Quality Management and Compliance Recording

Each user license is for a named (not concurrent) user. For example, a contact center with three shifts of 100 agents and supervisors needs 300 named user licenses. Each person in a shift of 100 users uses the license associated with them during their shift.

Quality Management is licensed on a per named user basis and provides all the server software required with the exception of the Windows operating system and database software for the Webex QM server, which must be purchased off the shelf.

The following table lists the license types and features available:

Table 17: License and Features

Feature	Compliance Recording	Webex Quality Management
Compliance Recording	Included	Included
Endpoint Recording	Included	Included
Server Based Recording (via SPAN port)	Included	Included
Network Based Recording	Included	Included
Cisco CUBE Recording (via SIP)	Included	Included
Network Recording (Built In Bridge)	Included	Included
Gateway Recording	Included	Included
Role-based Scoping	Included	Included

Feature	Compliance Recording	Webex Quality Management
Users Synchronized with UCCX	Included	Included
Finesse Recording Controls - (Pause, Resume, Delete)	Included	Included
Attach Custom Metadata	Included	Included
Role Based Dashboards	Included	Included
Exporting of Recordings	Included	Included
Monitoring and Notification Service	Included	Included
Recording Monitoring Dashboard	Included	Included
Reporting	Included	Included
Live Audio Monitoring	Included	Included
Quality Evaluation	Not available	Included
Evaluator Comments	Not available	Included
Screen Recording	Not available	Included
Live Screen Monitoring	Not available	Included

Workforce Management

Cisco Workforce Management allows supervisors and contact center managers to develop schedules for their agents and manage key performance indicators and real-time adherence. Managers can create and manage schedules for an unlimited number of sites, manage scheduling for offices spread out in different time zones, and schedule alternative media sources seamlessly, including email. Cisco Workforce Management also allows agents to view their schedules and performance metrics and request exceptions to those schedules, such as schedule offers and trades and requesting time off. Cisco Workforce Management is available with Unified CCX Enhanced and Premium licenses.

Each user license is for a configured (not concurrent) user. For example, a contact center with three shifts of 100 agents and supervisors needs 300 configured user licenses. Each person in a shift of 100 users uses the license associated with them during their shift.

The following Workforce Management features are available in each Cisco Unified CCX package:

- Forecasting
- Multimedia Scheduling
- Intraday Management
- KPIs and Reporting
- Alerts

- Reporting
- Web Interface
- Desktop Integration

Home Agent with Extend and Connect

Definitions

- CTI Remote Device — New device type that represents the user's off-cluster phones, which the users plan to use with Cisco Unified Communications applications. The device type is configured with one or more lines (for example, Directory Numbers) and one or more remote destinations.
- Remote Destinations — A numerical address that represents the user's other phones (for example, home office line and other PBX phone). The phone can be any off-cluster device such as DVO-R (Dial-via-Office-Reverse).

Introduction

The Extend and Connect feature can be configured for agents and supervisors on remote devices. This feature works with Cisco Jabber for Windows in Extended mode and the new CTI Remote Device type and enables applications to have limited call control capability over third-party devices of an user. Configure all third-party devices or end points of an user as remote destinations on a virtual CTI Remote Device. You can configure third-party devices or end points of an user from Cisco Unified Communications Manager administration console.

If there is an active remote destination set for a remote device, a call to that device is placed only to the active remote destination.

Note You cannot perform silent monitoring on Home Agents using this feature.

Feature Availability by License Package

The following table lists the availability of Extend and Connect feature in the Unified CCX packages.

Feature	Unified CCX Premium	Unified CCX Enhanced	Unified IP IVR
Extend and Connect	Available	Available	Not available

Persistent Connection Call

Persistent connection allows an agent to maintain a dedicated connection with an active remote destination. Persistent connection is supported from Cisco Unified Communications Manager. This connection saves connection establishment time for each call.

A persistent connection call is made to the active remote destination during agent login. The agent answers the persistent connection call only from a configured remote destination. ICD calls are placed over persistent connection. The agent moves to Ready state after answering the persistent connection call. Unified CCX plays

an announcement upon answering persistent connection call provided that announcement is configured with the identifier as “UCCX Persistent Connection Prompt”.

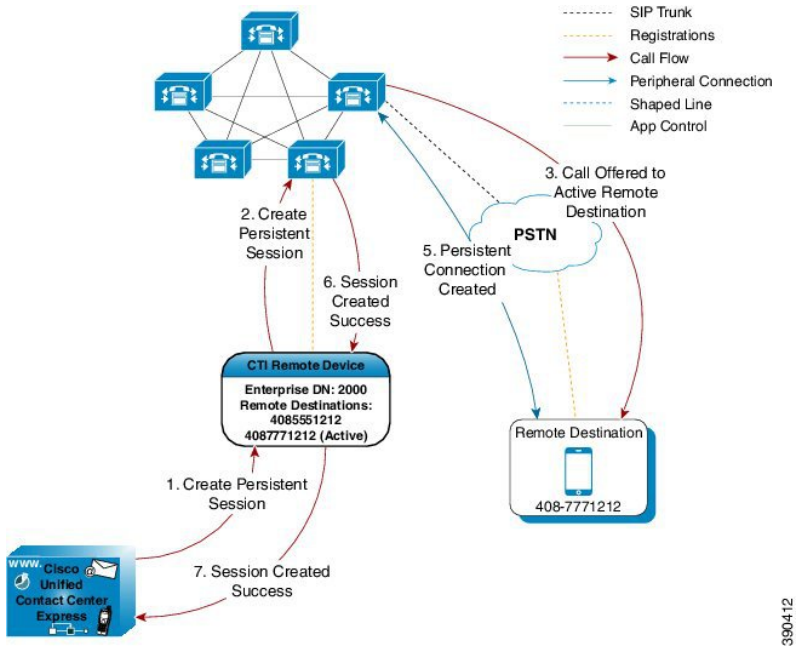
After the persistent connection is established for incoming calls, Unified CCX plays an announcement on persistent connection provided that announcement is configured with identifier as "UCCX Customer Call Prompt". The agent’s remote device displays the caller ID during the ICD call provided that the remote device has a provision to display caller information. The caller ID name is displayed as **EC Mode**. The caller information remains displayed until the next call is placed on the persistent connection call. By default, Unified CCX makes a maximum of three attempts to establish a persistent connection call.

The default call duration for a persistent connection is 12 hours. You can change the persistent connection duration using the **Maximum Call Duration Timer** field in Cisco Unified Communications Manager.

When a persistent connection call is not answered, the agent is moved to Not Ready state and is not allowed to move to Ready state until the persistent connection call is established. The persistent connection call is dropped after the agent logs out.

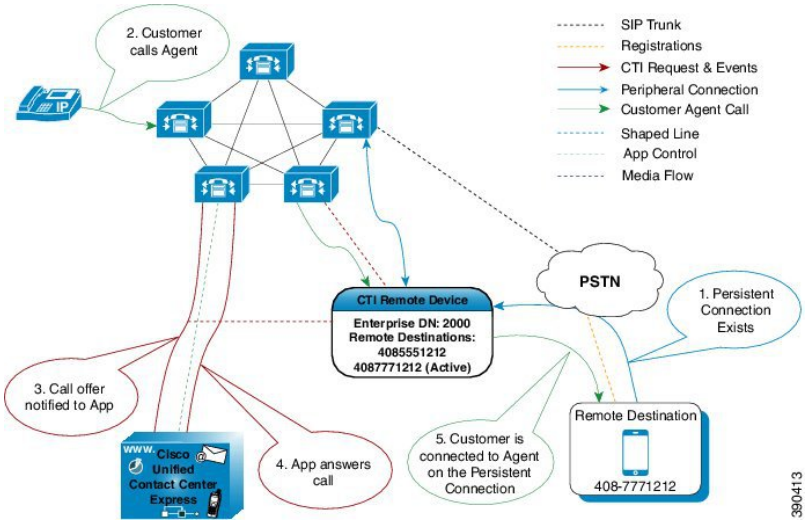
The following figure shows the persistent connection call flow:

Figure 10: Persistent Connection Call Flow



The following figure shows a persistent connection incoming call:

Figure 11: Persistent Connection Incoming Call

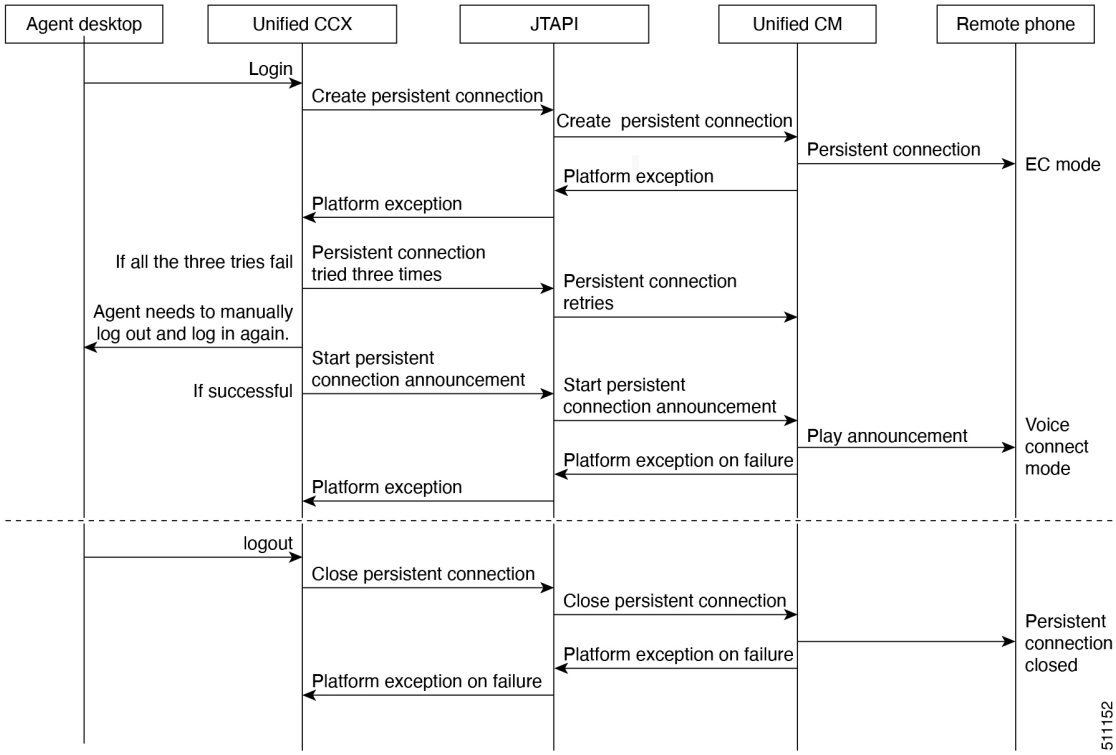


For remote phones that have persistent connection, the following features are not supported:

- Call Hold/Resume is not supported for a persistent connection call.
- Intercept/Barge-In is not supported for persistent connection with Cisco Finesse.
- Live Data and Historical reports do not distinguish the remote agents from the enterprise agents.
- The maximum number of supported remote agents is 100.
- Extend and Connect is not supported on shared lines.
- Call-by-call setup is not supported

Signaling Flow

The following figure shows the signaling flow chart:



Agent and Device Configuration

To use this feature, perform the following configuration:

1. Configure CTI Remote Device, CSF for Cisco Jabber, and Remote Destinations in Cisco Unified Communications Manager.
2. Configure ICT between Cisco Unified Communications Manager and Cisco Unified Presence server.

Deployment Guidelines

In case of fresh deployments of Cisco Unified Communications Manager and Unified CCX, ensure that the DNS is configured for all the components.

Remote Agent Over Broadband

Unified CCX supports remote agents (for example, at-home agents) using Cisco Unified IP Phone over a broadband internet connection.

The Cisco VPN Client feature available in select Cisco Unified IP Phones provides another option for remote agents to connect their IP Phones to the enterprise.

The enterprise will need to deploy and set up an appliance which supports SSL VPN connectivity. Connectivity between the remote agent and enterprise must be over broadband/SSL VPN.

The VPN feature needs to be configured on the Cisco Unified Communication Manager as per the *Cisco Unified Communications Manager Security Guide*.

The Cisco Unified IP Phone should then be configured within the enterprise as detailed in the *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*.

After the IP Phone has been configured in the enterprise, the agent can then take it home and connect it to a regular broadband router to obtain VPN connectivity to the enterprise. The agent will then be able to use the configured extension for receiving and placing calls from home.

VPN-less Access to Finesse Desktop

Agents and supervisors can acess the Finesse desktop from anywhere through the Internet without requiring VPN connectivity to the data center. To enable this feature, a reverse-proxy pair must be deployed in the DMZ.

Cisco Unified CCX supports Historical and Real Time report gadgets in agent and supervisor desktops in VPN-less deployments. The reverse-proxy configuration enables authentication of all requests at the proxy, along with other security enhancements as detailed in the *Reverse-Proxy Selection and Configurations* section of the *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

When deployed with VPN-less reverse-proxy, Customer Collaboration Platform can be deployed within the DMZ or can be moved within the enterprise.

Media access remains unchanged in reverse-proxy deployments. To connect to the media, agents and supervisors can use Cisco Jabber or Webex over Mobile and Remote Access solution (MRA). They can also enable the Extend and Connect feature in this deployment.

Supported Reverse-Proxy Deployment Models

Reverse-proxy deployment allows agents to concurrently access the Finesse desktop from both LAN and via reverse-proxy. Unified CCX supports the following deployment models:

- One Unified CCX cluster connects to one HA pair of reverse-proxy.
- Multiple Unified CCX clusters connect to one HA pair of reverse-proxy.

Features Available in VPN-less Finesse

- Supported Features
  - Finesse supervisor capabilities are supported via reverse-proxy.

    Cisco Unified IC RealTime and Historical reports are now supported via Finesse gadgets in a proxied environment.

    Authentication for all requests and communications require Lua support.
    - All Unified CCX and Customer Collaboration Platform requests are authenticated at the proxy before being allowed to enter the datacenter.
    - Websocket and Live data socketIO connections are also restricted and allowed only from clients that have successfully made a secured request to Finesse.
    - Brute force attack sensing and logging at the proxy, which can be used with Fail2Ban to block malicious IP addresses.

  - Security for reverse-proxy configuration requires Lua support.

- Mutual Transport Layer Security (TLS) authentication between reverse-proxy and the components.
- SeLinux settings.
- Enable mutual Secure Sockets Layer (SSL) trust verification for proxy and component server requests.

- Enhanced security for the proxy configuration to prevent Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks require Lua support.
  - Enhanced reverse-proxy (OpenResty Nginx) request rate limits for various parts of the system.
  - Rate limits for IP Tables.
  - Verification of static resource requests before requesting the upstream component server.
  - Lighter and cacheable unauthenticated pages which do not hit the upstream component server.

- Miscellaneous other features require Lua support.
  - Auto sensing Cross-Origin Resource Sharing (CORS) responses provided from the proxy to aid automatic configuration and to improve the performance.

Requirements for VPN-less Configurations

- Any reverse-proxy supporting the required criteria (as mentioned in the *Reverse-Proxy Configuration* section in the *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html) can be used, such as OpenResty Nginx installation with Lua support.
- Certificate Requirements
  - Unified CCX and Customer Collaboration Platform require the reverse-proxy host certificate to be added to the Tomcat trust store and the system to be restarted. This enables the reverse-proxy configuration to successfully connect to the component servers.
  - Unified CCX and Customer Collaboration Platform upstream server certificates need to be configured in the reverse-proxy server.

Authentication

Unified CCX supports authentication at the edge for the reverse-proxy.

Authentication is supported for both SSO and Non-SSO deployments. For all requests and protocols that are accepted at the proxy, authentication is enforced before they are forwarded to the respective Unified CCX servers. Finesse servers also enforce authentication locally. Authentications that are made at the proxy use the Finesse login credentials, irrespective of the component server to which the requests are made.

Persistent connections such as WebSockets that rely on post connection application protocols (such as XMPP) for authentication, are authenticated at the proxy by verifying the peer IP address of the connection. The peer IP address must correspond to a system that has successfully authenticated an API request prior to establishing the socket connection.

Requests that do not require authentication, such as static files and images, are configured to be served by the reverse-proxy from its cache.

Non-SSO

The list of valid users is cached at the proxy locally (updated every 15 minutes), which is used to validate the user in a request. User credentials are validated by forwarding the request to the configured Finesse URI and thereafter the credential hash is cached locally (every 15 minutes) to authenticate new requests locally. Any change in the username or password will take effect only after 15 minutes.

SSO Authentication

SSO authentication requires that the administrator configures the IdS token encryption key at the reverse-proxy server within the configuration file. The IdS token encryption key can be obtained from the IdS server with the `show ids secret` CLI command. For the SSO authentication to work, the key has to be configured as part of one of the must-change replacements that the administrator has to perform in the scripts.

After SSO authentication is configured, a valid pair of tokens can be used to access any of the endpoints in the system. The proxy configuration validates the credentials by intercepting the token retrieval requests made to IdS or by decrypting valid tokens and thereafter caching them locally for further validations.

Authenticate WebSocket Connections

WebSocket connections do not have a standard authentication mechanism. Therefore, applications rely on postconnection application level protocol payloads for validating the established connection. However, this mechanism is used to establish unauthenticated connections at scale, mounting DoS or DDoS attacks on the servers.

To mitigate this possibility, the provided reverse-proxy configuration performs specific checks before allowing WebSocket connections. The WebSocket connections are accepted only from those IP addresses that have successfully made an authenticated REST request. The REST request must be authenticated before establishing the WebSocket connection.

Reverse-Proxy deployments that use L7 intermediaries, such as Content Delivery Network (CDN), often redirect traffic through interim servers before the traffic reaches the reverse-proxy. In such deployments, ensure that the **X-Forwarded-For** headers are correctly relayed to identify the client IP address. The **X-Forwarded-For** headers are used to authenticate the WebSocket connection by matching it with the previously authenticated REST request.

Note The clients that attempt to create WebSocket connections before issuing any REST requests, an **Authorization Failed** error message is displayed.

Host Mapping File for Network Translation

Reverse-proxy deployment requires a invalid mapping file to configure the list of externally visible hostname/port combinations and their mapping to the actual server names and ports that are used by the Unified CCX servers and Cisco Collaboration Platform server. This mapping file which is configured on internal servers is the key configuration that allows the clients connected over the Internet to be redirected to the required hosts and ports that are used on the Internet.

The mapping file has to be deployed on a web server accessible to the component servers and its URI must be configured using a dedicated web server available within the LAN. If such a server is not available, the reverse-proxy can be used instead, which requires that the proxy is accessible from within the LAN. Using

the reverse-proxy presents a risk of exposing the information to external systems which can make unauthorized connection to the DMZ.

For all the requests that come through the reverse-proxy, the Unified CCX servers and Cisco Collaboration Platform server check the host mapping file, to translate the internal hostnames and ports that are used on the LAN. They are translated to the publicly resolvable hostnames and ports that have to be used on the Internet. This mapping file, referred to as the Proxy-config map file, is the key configuration that allows the clients connected over the reverse-proxy to be redirected to the required hosts and ports that are used on the internet.

The Proxy-config map file can be configured by using CLI available on Finesse, IdS, and CUIC servers. For details on the mapping file format and the data configured, refer to the *Populate Network Translation Data* section. For details on the CLI used to configure the file, refer to *Configure Proxy Mapping by Using CLI*.

The Proxy-config map file can be configured by using CLI available on Unified CCX servers and Cisco Collaboration Platform servers. For details on the mapping file format and the data configured, refer to the *Populate Network Translation Data* section in *Cisco Unified Contact Center Express Administration and Operations Guide*. For details on the CLI used to configure the file, refer to the *Configure Proxy Mapping by Using CLI* section in *Cisco Unified Contact Center Express Administration and Operations Guide* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

DNS Configuration

Each Unified CCX and Customer Collaboration Platform servers corresponding to a host that needs Internet access must be addressable from the Internet. This calls for a hostname and associated port which is resolvable from the Internet to be mapped to the public port and matching IP of the reverse-proxy so that the traffic is directed to the respective component servers.

DNS registration of the publicly resolvable hostnames and the corresponding IP addresses is mandatory before the requests reach the reverse-proxy.

SSL Certificates

For the hostnames that are configured, corresponding to each unique hostname that is used by the internet client, the respective TLS certificates must be acquired and configured on the reverse-proxy. Even though self-signed certificates are supported, they are risky because the users access directly from the internet. The clients can be more secure by using CA-signed TLS certificates. The best practice is to get CA certificates for proxy servers and third-party-gadget servers.

Security Guidelines for Reverse-Proxy Deployment

To allow VPN-less access, reverse-proxy hosts are deployed in the DMZ and they are directly accessible from the internet. Therefore, security is crucial in a reverse-proxy deployment. This section provides a set of guidelines to secure a reverse-proxy deployment.

Note The guidelines and recommendations provided are intended to be used as a minimum required guidance for administrators to secure the deployment. The deployment, configuration, and security of reverse-proxy and the network is the Contact Center's responsibility.

Reverse-Proxy

The reverse-proxy is the first application-level landing point for all requests that come into the Cisco Contact Center network from the internet. The reverse-proxy must have a high level of security to withstand attacks. The following are the guidelines to secure a reverse-proxy deployment:

- Configure TLS 1.2 and turn off other TLS protocols.
- Allow only secure HTTP/1.1 based access.
- Turn off default access and default rules for your proxy to avoid unplanned access to the proxy.
- Ensure that the reverse-proxy and the host systems are up to date with security patches to prevent potential breaches.
- Ensure that the reverse-proxy is not allowed to establish direct outbound connections to the internet.
- Harden your proxy host to ensure its safety when exposed to the Internet. For best practices, refer to https://www.cisecurity.org/cis-benchmarks/.
- Conduct regular security audits on reverse-proxy hosts to ensure that their security has not been compromised.
- For security reasons, ensure that API paths other than those explicitly exposed are not available through the configured rules. If OpenResty Nginx reverse-proxy is being deployed, refer to the OpenResty Nginx rules to find the paths which are explicitly opened for each Unified CCX and Customer Collaboration Platform servers.

  The OpenResty Nginx rules are available in the *Reverse-Proxy Configuration* chapter in *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.
- Caching is important from a security perspective because most of the static resources are unsecured. Simple DoS attacks can be prevented by caching these resources on the Finesse server. However, the resources have to be validated periodically with the Unified CCX and Customer Collaboration Platform servers to ensure that the resources are the latest.
- Validate the HOST headers to ensure that only the intended domains are accessed by the client.
- Regulate the WebSocket connections of Unified CCX and Customer Collaboration Platform servers for each domain corresponding to the expected number of clients.
- It is a best practice to maintain security hardened golden images of the reverse-proxy with updated patches and configuration changes. Installing from these golden images ensure that all the reverse-proxy instances are consistent and are as secure as possible.

Note For OpenResty Nginx-based reverse-proxy rules, installation, configuration, and security hardening instructions, see the *Reverse-Proxy Configuration* chapter in *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html. You can use any reverse-proxy meeting the required criteria (mentioned in the *Reverse-Proxy Selection Criteria* section of *Cisco Unified Contact Center Express Administration and Operations Guide*) instead of OpenResty Nginx for this feature.

Demilitarized Zone Security

Without an ongoing process and related efforts to ensure that the security of the network and the hosts are updated, a reverse-proxy deployment cannot maintain its security posture. The following are the important points to ensure that the DMZ is secure:

- Consider using dual firewalls (instead of a single firewall with multiple interfaces) to separate the DMZ from the internal network.
- Configure rules in the internal firewall to ensure that the requests originating from the DMZ do not reach hosts other than the ones configured in the reverse-proxy.
- Ensure that the DMZ is separated from the internal network with isolated routing and security policies.
- Install software updates and patches whenever they are available to ensure your reverse-proxy deployment remains secure.

Rate Limit

Unified CCX and Customer Collaboration Platform rely on host-level firewall rules for protection from DoS attacks. When reverse-proxy hosts are configured in front of these components, they exempt the configured reverse-proxy host from all host-level rate limiting rules. This is to support the required throughput for the proxy which is serving multiple clients that are connected to it. Therefore, packet rate limits and reverse-proxy-based rate-limiting rules should be enforced to ensure that the traffic routed to the hosts through the reverse-proxy are regulated for each individual IP. This ensures higher availability of the reverse-proxy and the hosts.

Note Consider imposing general network packet rate limits on ISP routers that connect your network to the DMZ. Implementing rate limits on the perimeter router is not effective against DoS attacks that are aimed at saturating the ISP links.

IP-table-based rate limiting and proxy-rule-based rate limiting is mandatory to prevent DoS attacks. The OpenResty Nginx proxy configurations provided with Unified CCX contain IP tables and Nginx-rule-based rate limits for a sample 400 deployment.

For more information on calculating the rate limits, see the *Determine Scale and Hardware for Proxy* section and for OpenResty Nginx specific information, see the *Reverse-Proxy Configuration* chapter in the *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

Network Security Devices

Network security devices that incorporate Intrusion Prevention System (IPS) functionality must be deployed to offer additional security to the traffic that enters the DMZ. These are devices that can prevent entire class of attacks that a proxy or firewall is not equipped to detect or prevent effectively. While deploying IPS devices, deploy devices that can detect Distributed Denial of Service (DDoS) signatures to guard against DDoS attacks.

Web Application Firewalls

Web Application Firewall (WAF) provides a higher layer of security for reverse-proxy deployments. The WAF devices extend the security checks into the application layer. This is achieved by inspecting the web application traffic for scripts, headers, cookies, HTTP methods, and so on to find known vulnerabilities and loopholes to block malicious traffic. This prevents diversified cyber-attacks that exploit vulnerabilities that

are specific to web applications. You can have devices that integrate IPS and WAF functionalities or use cloud services that provide all the above-mentioned capabilities.

DDoS Protection

Sophisticated attacks that get past the rate limits by using multiple clients to initiate DoS attacks are referred to as DDoS attacks. Individual systems are often unable to detect or react properly to DDoS attacks. To avoid such attacks, ensure that the traffic is regulated by applying proper rate limits.

One of the most effective ways to handle DDoS attacks is to employ Content Distribution Networks (CDN) that provide a high level of protection against most attacks and can absorb the brunt of these brute force attacks. Incorporating IPS devices, routers, or a firewall that can detect DDoS signatures can also help in preventing such attacks.

Reverse-Proxy Security Configuration

Reverse-proxy configuration is one of the areas that produces the biggest potential security flaws when configuring a proxy. The rules configured should be compared against known vulnerabilities and must be created to protect the applications that are being configured, such that, only the desired end points are exposed. The proxy, being the initial ingress point, plays a significant role in enhancing the security posture of the deployment. The following are the additional security enhancements included with the reverse-proxyconfiguration:

- Brute Force Attack Prevention
- Mutual TLS Verification
- SELinux Rules

Brute Force Attack Prevention

The authentication scripts (reverse-proxy scripts) provided with Unified CCX and above prevent brute force attacks which can be used to derive the user credentials. The scripts block the IP addresses corresponding to the failed authentication requests. The time period and number of failed attempts are configurable in the default configuration provided. The details of blocked IPs can also be accessed from the reverse-proxy logs. For more information on brute force, see the *Reverse-Proxy Configuration* chapter in the *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

Mutual TLS Verification

For enhanced security, Unified CCX adds mutual TLS verification. Mutual TLS verification uses the locally available pre-configured server certificate to verify the certificate presented during the TLS handshake. This enables participating servers to verify their peer's identity. Therefore, the server certificates of all component servers exposed by the proxy needs to be uploaded at the proxy. For the proxy to be able to connect to the component server (Unified CCX and Customer Collaboration Platform) too, the proxy certificate has to be uploaded to the component server.

SELinux Rules

OpenResty Nginx specific SELinux rules that work with the default configurations are available with the Unified CCX 12.5(1) SU2 proxy configuration. Enabling and configuring SELinux at the proxy is highly recommended to enhance the security posture of the deployment.

For more information, see the SELinux section in the *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

Expressway Support

Unified CCX supports Cisco Expressway as an endpoint for remote agents from 11.5(1) release onward. The agent phones must be registered with the Unified CM. The agents must be logged into Cisco Finesse desktop that is connected over the VPN or the Enterprise must have enabled access to Cisco Finesse over the internet (by enabling NAT). For any caveats and release specific information in Cisco Expressway see, http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-release-notes-list.html.

Reporting

Configuration APIs

The Cisco Unified Contact Center Express Application Programming Interface (UCCXAPI) provides a platform to integrate provisioning applications similar to what is provided by the Unified CCX Application Administration interface. Cisco Unified CCX exposes sophisticated control of the contact center application management with its Configuration REST APIs. For more information on supported APIs, see *Cisco Unified Contact Center Express Developer Guide* available here:

https://developer.cisco.com/site/collaboration/contact-center/uccxapi/overview/

Remote Expert Mobile

For all information about the Remote Expert Mobile deployment, see the *Cisco Contact Center Solutions and Unified Communications Manager Solution Configuration Guide for Remote Expert Mobile*, available at http://www.cisco.com/c/en/us/support/customer-collaboration/remote-expert-mobile/tsd-products-support-series-home.html.

Post Call Treatment

Post Call Treatment allows Unified CCX to provide treatment to an ICD call once the agent ends the call from the Finesse desktop. The Unified CCX administrator has an option to configure the Post Call Treatment via the Cisco Unified CCX Script Editor. This functionality will not be available if the agent ends the call from the phone or when the customer ends the call before the agent.

Caller ID Support

Caller ID feature displays the caller's number instead of the CTI port number on the agent's IP phone. Caller ID (CLID) is disabled by default. To enable CLID using a CLI command, see the *Cisco Unified Contact Center Express Operations Guide*, located at http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_maintenance_guides_list.html.

Note

- CLID is not supported with Jabber.
- When the CLID screen pops up on the phone screen, the **Answer** key is hidden below the CLID screen. You see two soft keys: **Update** and **Exit**. Press **Exit** to see the **Answer** key.

E.164 Support

Unified CCX supports E.164 numbering plan for route point directory numbers, and Finesse agent and supervisor extensions. E.164 is supported for the following components:

- Cisco Finesse
- Trigger directory numbers
- Agent extensions
- Display of Incoming calls
- Phonebook and keypad
- Route points
- Configuration APIs for route points
- Script editor

Note E.164 is not supported for outbound, Cisco Agent Desktop, and the directory numbers for a Call Control Group configuration.

Note For CTI port directory numbers:

- Unified CCX doesn't completely support E.164 numbering plan for CTI route point directory numbers (DN).
- This limitation is because of the Unified CM limit on device name length set as 15 characters. The system automatically adds "_" between the device name prefix and the DN. So a maximum of 13 characters in the DN is supported as device name prefix (which includes the "+" sign) is mandatory and hence at least one character is needed there. For example, (Device name prefix) + '_' + (length of DN) = 15 ==> [(1 + '_' + 13) = 15]

For Finesse Agent and Supervisor extensions:

- Unified CCX E.164 numbers support a total of 15 characters. When using the plus sign (+) dialing, the plus sign (+) is followed by up to 14 characters that consist of numerals and the special characters—alphabet X, hash(#), square brackets ([ ]), hyphen (-), and asterisk (*).

Single Sign-On

Single sign-on (SSO) is an authentication process that allows users to sign in to one application and then securely access other authorized applications without needing to resupply user credentials. SSO permits Cisco supervisors or agents to sign on only once with a username and password to gain access to all of their Cisco browser-based applications and services within a single browser instance. By using SSO, Cisco administrators can manage all users from a common directory and enforce password policies for all users consistently.

Note

- SSO is an optional feature.
- The implementation requires you to use the HTTPS protocol only to access all the web applications. The HTTP access to web applications is not supported when the SSO is enabled.
- Use Fully Qualified Domain Names and not IP addresses to access the web applications.

SAML 2.0 Authentication

SSO uses Security Assertion Markup Language (SAML) to exchange authentication details between an Identity Provider (IdP) and a service provider. The identity provider authenticates user credentials and issues SAML assertions, which are pieces of security information transferred from the identity provider to the service provider for user authentication. Each assertion is an XML document that contains trusted statements about a subject including, for example, username and privileges. SAML assertions are usually digitally signed to ensure their authenticity.

A generic SAML authentication flow consists of:

- Client - A browser-based user client used to access a service.
- Service Provider - An application or service the user tries accessing.
- Identity Provider - An entity performing the user authentication.

The identity provider keeps actual credentials and authentication mechanism hidden. Based on the authentication process result, the identity provider issues SAML assertions.

Elements Used in SAML 2.0

The following is the list of elements that are used in SSO SAML 2.0 authentication:

- Client (the user's client)—A browser-based client or a client that can leverage a browser instance for authentication. For example, a system administrator's browser.
- Lightweight Directory Access Protocol (LDAP) users—Users are integrated with an LDAP directory. For example, Microsoft Active Directory or OpenLDAP.
- Security Assertion Markup Language (SAML) assertion—An assertion is an XML document that contains trusted statements about a subject. For example, a username. SAML assertions are digitally signed to ensure their authenticity. It consists of pieces of security information that are transferred from Identity Providers (IdPs) to the service provider for user authentication.
- Service Provider (SP)—An application or service that trusts the SAML assertion and relies on the IdP to authenticate the users. For example, Cisco Identity Service (IdS).

- An Identity Provider (IdP) server—This is the entity that authenticates user credentials and issues SAML assertions.
- SAML Request—An authentication request that is generated by a Cisco Identity Service (IdS). To authenticate the LDAP user, IdS delegates an authentication request to the IdP.
- Circle of Trust (Co-T)—It consists of the various service providers that share and authenticate against one IdP in common.
- Metadata—An XML file generated by the Cisco IdS (for example, Cisco Identity Service Management) and an IdP. The exchange of SAML metadata builds a trust relationship between the IdP and the service provider.
- Assertion Consumer Service (ACS) URL—A URL that instructs the IdPs where to post SAML assertions.

Cisco Identity Service (IdS)

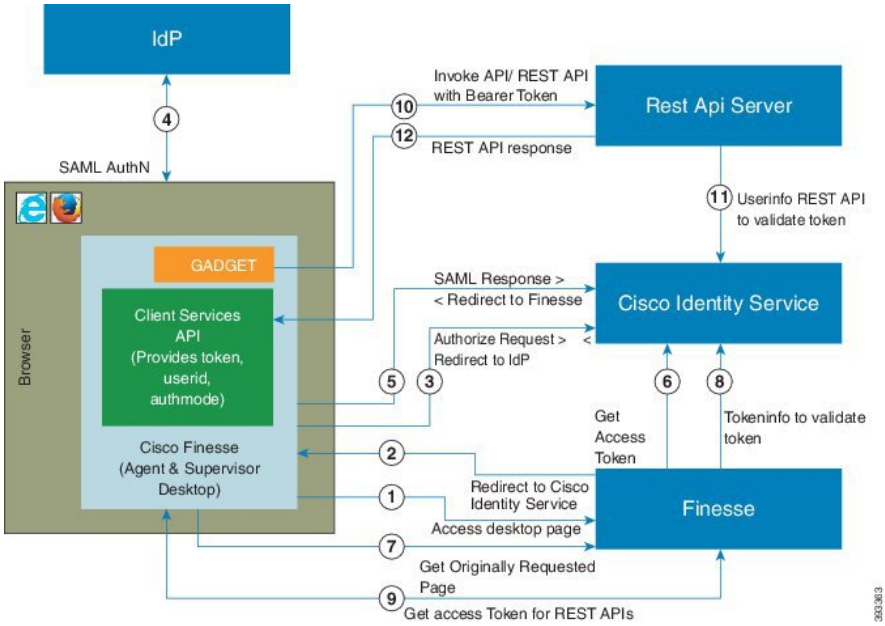
Authentication is managed for the contact center solution by the Cisco Identity Service (Cisco IdS). When an SSO-enabled user signs in, the Cisco IdS interacts first with the customer's Identity Provider (IdP) to authenticate the user. The IdP stores user profiles and provides authentication services to support SSO sign-ins. When the user is authenticated, the Cisco IdS exchanges information with the Cisco service the user is attempting to access to confirm that the user is authorized for the role they are requesting. When the user is both authenticated and authorized, the IdS issues an access token that allows the user to access the application. When the access is established during a particular session, the user can switch among contact center solution applications without presenting credentials again.

Authentication and Authorization Flow

The complete authentication and authorization flow has been simplified as:

- When you access an application with protected resources, the application will redirect you to the Cisco Identity Service for authentication. Cisco Identity Service leverages SAML and generates a SAMLRequest and redirects the browser to the Identity Provider.
- The browser authenticates directly against the Identity Provider. Applications are not involved in the authentication process and have no access to user credentials.
- The OAuth flow accesses the resource with a token which is then validated.
- Cisco Identity Service sends an authentication request through the browser to the identity provider.
- The user enters the login credentials to the identity provider for authentication. After the assertion is successful and the user attributes are read it will redirect to the original application that was accessed. Cisco Identity Service accompanied by an assertion that confirms successful authentication and includes user information and access rights for the web application.

Figure 12: Authentication and Authorization Flow



Accessibility

The Finesse desktop supports features that improve accessibility for low-vision and vision-impaired users. The following table shows how to navigate the Finesse desktop using the accessibility features.

Desktop Element	To Perform the Following Actions	Use the Following Keys
Address Bar	Move between the address bar and the frames	F6
Sign-in Page		
Language Selector Drop-Down	Access the drop-down	Tab and Shift-Tab from the ID field
	Open the drop-down	Alt-Down Arrow or Enter
	Scroll the drop-down	Up and Down Arrows
	Select a language	Enter
	Hide the drop-down	Esc
Mobile Agent Help Tooltips	Access and display a tooltip	Tab and Shift-Tab
	Hide a tooltip	Esc
Certificate Acceptance	Toggle between the certificate links	Tab and Shift-Tab
	Open the certificate link to accept the certifiate	Enter

Desktop Element	To Perform the Following Actions	Use the Following Keys
Call Control Gadget		
Incoming Call Popover	Accept the incoming call	Enter
Call Control Gadget Navigation	Access the call control gadget, phone book, and keypad	Tab and Shift-Tab
	Open and close the call control gadget	Enter
Phone Book	Navigate the phone book contact entries	Arrow keys
	Select the contact to make a call	Enter
	Select the contact to copy the number to the dialler	Enter
Dialpad	Toggle between the phone book and the keypad	Tab, Shift - Tab, and Enter
	Navigate the keypad number buttons	Arrow keys, Tab, and Shift - Tab
	Make a new call, Transfer a call, or consult a call	Press Enter in the number display field OR Navigate to the Call button and press Enter
Wrap-Up Reason Drop-Down	Access the drop-down	Tab and Shift-Tab
	Open the drop-down	Enter
	Scroll the list of wrap-up reasons	Up and Down Arrows
	Select a wrap-up reason	Space Bar
	Apply the wrap-up reasons	Enter
	Close the drop-down	Esc
Callback and Reclassify Dialog Boxes (Outbound Calls)	Access the Callback and Reclassify buttons	Tab and Shift-Tab
	Open the Callback and Reclassify dialog boxes	Enter (on the respective buttons)
	Close dialog boxes	Press Esc OR Navigate away from the dialog boxes using Tab or Shift-Tab

Desktop Element	To Perform the Following Actions	Use the Following Keys
Reclassify Dialog Box	Navigate the elements	Tab, Shift-Tab, Up and Down Arrows
	Select an option	Enter
	Close the Reclassify dialog box	Esc
Callback Date and Time Calendar	Navigate to and from the Calendar	Tab and Shift-Tab
	Navigate within the Calendar	Arrows
	Select a Calendar date	Enter
	Move to the first or last days of a month	Home and End
	Close the pop-up	Esc
Callback Date and Time Controls	Navigate the elements	Tab and Shift-Tab
	Increase and decrease the Hour and Minute values	Up and Down Arrows
	Toggle the AM/PM button	Enter
	Close the pop-up	Esc
Desktop Chat		
Certificate Acceptance	Toggle between the certificate links	Tab and Shift-Tab
	Open the certificate link to accept the certifiate	Enter
Change Status	Open the drop-down to change the status	Enter
	Toggle between the status	Arrow Keys, Tab and Shift-Tab
	Apply Status	Enter
Search Contacts	Toggles between the search results	Tab and Shift-Tab
	Close the search results drop-down	Esc
Contact List	Toggle between contacts and groups	Arrow Keys, Tab and Shift-Tab
	Select multiple contacts	Ctrl + Up and Down arrows
	After selecting multiple contacts, navigate to the Move or Delete options	Tab and Shift-Tab
	Select the Move or Delete option	Enter

Desktop Element	To Perform the Following Actions	Use the Following Keys
Contact	Navigate to contact header options	Tab
	Open contact header options	Enter
	Navigate contact header options	Arrow Keys, Tab and Shift-Tab
	Navigate through Add, Edit and Delete Contact windows	Tab and Shift-Tab
	Select an option	Enter
Group	Navigate to group header options	Tab
	Open group header options	Enter
	Navigate group header options	Arrow Keys, Tab and Shift-Tab
	Navigate through Edit and Delete Group windows	Tab and Shift-Tab
	Select an option	Enter
Team Message		
Team Message	Navigate the elements	Tab, Shift-Tab, Up and Down arrows
	Select an option	Enter
	Close the dialog box	Esc
	Show recent messages	Shift-Tab
	Back and Delete	Tab-Enter
Queue Statistics Gadget		
Queue Statistics Gadget	Access the Queue Statistics Gadget	Tab and Shift-Tab
	Navigate the Queue Statistics table header	Tab and Shift-Tab
	Navigate the Queue Statistics table cells	Tab and Shift-Tab
Desktop		
Send Error Report	Access and display a tooltip	Tab and Shift-Tab
	Hide a tooltip	Esc
	To send the error report	Enter
Sign out	To sign out of the Finesse desktop	Enter
Third-Party Gadget		

Desktop Element	To Perform the Following Actions	Use the Following Keys
Maximize Icon	Access the maximize icon	Tab and Shift-Tab
	Maximize and restore a third-party gadget	Enter
Digital Channels		
Agent State	Access the digital channel agent state gadget	Tab and Shift-Tab
	Open and close the gadget options drop-down.	Enter
	Close the gadget options drop-down.	Esc
	Navigating options in drop-down.	Up and Down Arrows
	Select an option in drop-down.	Enter

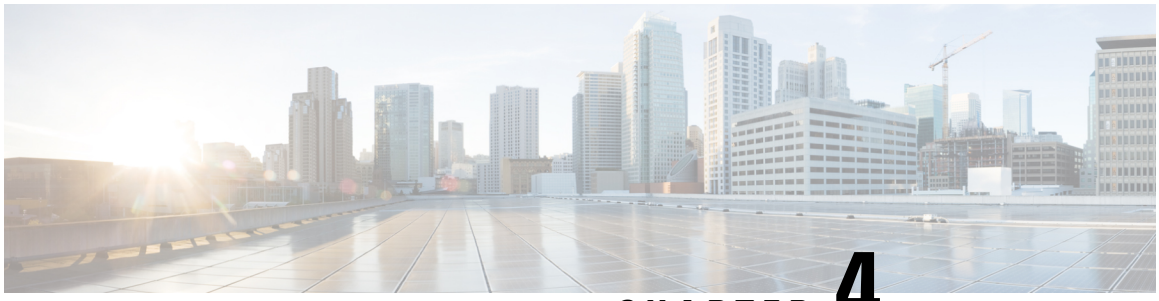
Note For Email and Chat Keyoard shortcut keys, see *Cisco Finesse Agent and Supervisor Desktop User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html.

Screen Reader Support

Cisco Finesse also supports JAWS screen reading software for the following elements:

Page or gadget	Element	Notes
Sign-in Page	Mobile agent help icon	The screen reader reads descriptive text for the help icon.
	Invalid Sign in error	When a sign-in error occurs due to invalid password or username, the screen reader reads the error.
Queue Statistics gadget	Title	The screen reader reads the gadget title (Queue Statistics).
Call Control Gadget	Phone Book	The screen reader reads the contents of the phone book. **Note** • The screen reader is not able to read the summary of this table by using CTRL+INSERT+T. As a workaround, use the heading key instead. • The phone book does not support use of CTRL+ALT+RIGHT/LEFT/UP/DOWN arrow keys to move between cells in the table. • The screen reader does not read the heading of each column in IE11.

Page or gadget	Element	Notes
	Keypad	The screen reader reads the number of the keypad and the letters that go with it (ABC, DEF, and so on). **Note** • In the table summary, if you select the table, the screen reader reads the summary of the table, which is Keypad. • If you press Enter on a Keypad button with JAWS enabled, the digits are not entered or displayed in the edit box on top of the Keypad. • If you use Ctrl+Alt+Right, Left, Up, and Down arrow keys to move between the cells, extra buttons are read on the Keypad.
	Call row errors	The screen reader reads the call row error messages.
Agent Desktop	Headings	The screen reader reads all the headings on the Agent Desktop (HTML elements <h1> to <h6]>).
	Failover Banner	During failover, the screen reader reads the statement from the red banner. When the Failover is complete, the screen reader reads the statement from the green banner.
	State Change text	Whenever the agent state changes, the screen reader reads the new state.
Desktop	Send clients logs help icon	The screen reader reads descriptive text for the help icon.



CHAPTER 4

Unified CCX Solution Design Considerations

- Core Components Design Considerations, on page 77

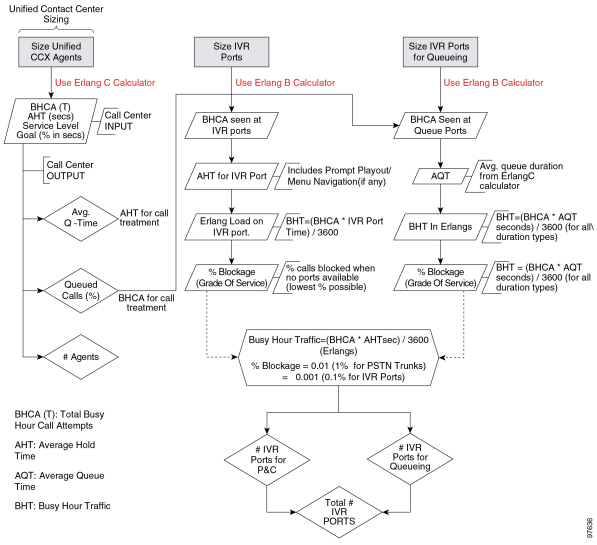
Core Components Design Considerations

General Solution Requirements

Principal Design Considerations for Call Center Sizing

This figure illustrates the principal steps and design considerations for sizing a call center.

Figure 13: Call Center Sizing - Voice Only



This figure is a general overview of the design considerations for call sizing. For a detailed description of the call center sizing design process, refer to the section on sizing call center resources in the *Cisco Unified Contact Center Enterprise Solution Reference Network Design Guide*, available online at the following URL:

http://www.cisco.com/go/ucsrnd

There are similar basic call center sizing considerations and steps for Unified CCE, and they also can be used in sizing a smaller contact center for Unified CCX. This call-sizing approach will provide you with the minimum number of IVR ports to support the total BHCA.

In addition, you should include the following design considerations, specific to Unified CCX, in your call center sizing calculations:

- At a minimum, plan on enough capacity to replace your existing system. The replacement system should perform at least as well as the one it is replacing.
- After all of the Erlang (C and B) calculations are complete for the call center sizing, any changes in queue times or agents will affect the total number of trunks and IVR ports required for an Unified CCX solution.
- As you increase the size of the agent pool, very small changes in the average queue time and percentage of queued calls will affect the required number of gateway trunks and IVR ports.
- Even if you perform all of the calculations for a call center, there are still some variables that you cannot plan for but that will affect the ports needed on a Unified CCX system. For example, one or more agents could call in sick, and that would affect the port count and queue time for each call. Just two agents calling in sick could increase the port count by over 12 percent. This would affect the price of the system and, if not planned for, would affect the ability of the call center to meet caller requirements. Properly sizing call center resources is integral to designing an effective Unified CCX system.

If all of the call sizing information is available, the next step is to apply Unified CCX sizing limits to the call center requirements. For this step, use the Cisco Unified Communications Sizing Tool, available online at:

http://tools.cisco.com/cucst

The Unified Communications downloadable sizing tools help you with the task of sizing Unified Communications deployments.

Preliminary Information Requirements

System designers are advised to create a sizing document to do the following:

- Scope out the preliminary configuration information for the Unified CCX server.
- Size the gateways for the system.

To determine the size of the call center, obtain answers to the following questions:

- How many IVR ports do you need?
- How many PSTN gateway trunk ports do you need?
- How many agents will answer incoming calls?

To answer these questions properly, you will need the sizing metrics and information listed in the following table.

Table 18: Call Center Sizing Metrics

Metric	Description
Average handle time (AHT)	Average duration (talk time) of a call plus after-call work time, which is the wrap-up time after the caller ends the call.

Metric	Description
Average IVR port usage time	The total time for prompt playout and/or menu navigation (if any) in the Unified CCX script. This time should not include the queue time the caller spends waiting in queue before an agent becomes available. Queue time is calculated using Erlang-C automatically.
Service level goal for agents	Percentage of calls answered by agents within a specific number of seconds.
Busy Hour Call Attempts (BHCA)	Average number of calls received in a busy hour.
Grade of service (% blockage) for gateway ports to the PSTN	Percentage of calls that get a busy tone (no gateway trunks available) out of the total BHCA.

All of the metrics in this table are basic call-sizing metrics. After this information is obtained, calculate the number of gateway trunk ports, IVR ports, and agents using standard Erlang B and C calculators.

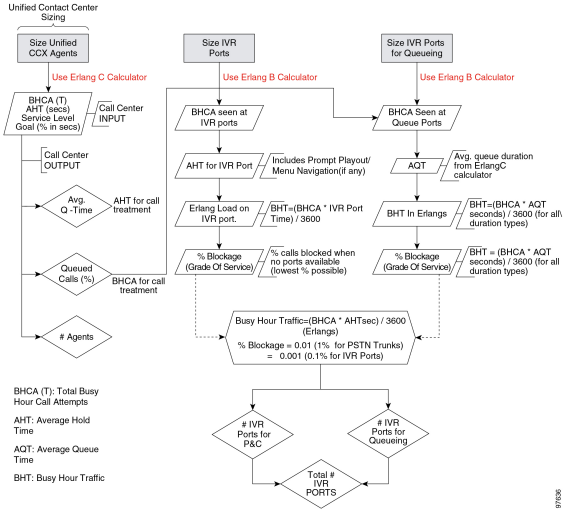
Note If the system being designed is a replacement for an existing ACD or an expansion to an installed Unified CCX or Cisco Unified IP IVR system, you might be able to use the historical reporting information from the existing system to arrive at the above metrics.

In addition, call sizing design considerations may vary if the call center is more self-service oriented.

Terminology

This figure illustrates the common port types and how they map to Unified CCX.

Figure 14: Call Center Port Types



Call center sizing differentiates the port types as follows:

- **Gateway or PSTN trunk ports** — Handles calls originating from the PSTN. They are purchased separately from Unified CCX.
- **Queue ports** — IVR ports that queue calls (when no agents are available) prior to transferring the caller to an available agent. These ports are included at no additional cost with Unified CCX. However, they must be sized for proper capacity planning for the Unified CCX server.
- **IVR ports** — Full-featured IVR ports available with the Cisco Unified IP IVR and Unified CCX Premium product.

If you want additional supporting features, such as automatic speech recognition (ASR), text-to-speech (TTS), email notification, web server or client functionality, and database operations, you only need to purchase the Premium package. Additional seats may also be purchased for IVR port licenses if the number of port licenses that come with the seat licenses is not sufficient.

The Unified CCX architecture differs slightly from the example TDM call center configuration in that IVR ports and queue ports (and P&C ports as well) are combined into one logical CTI port as shown in the figure above.

Effect of Performance Criteria on Unified CCX Server

System performance criteria fall into two general categories:

- Unified CCX and Cisco Unified IP IVR components — Applications, software versions, capabilities, server types, and options and quantities that your system requires.
- System usage — The average number of calls placed and received per hour, the average call length, the scripts that run, and the grammar used for ASR.

Effect of Performance Criteria

Each performance criterion can have an effect on the performance of the Unified CCX or Cisco Unified IP IVR system. In general, the more Unified CCX or Cisco Unified IP IVR components that you install and the heavier the system usage, the higher the demand on the server. However, the performance criteria can also interact in various non-linear ways to affect performance. The Cisco Unified Communications Sizing Tool for Unified CCX and Cisco Unified IP IVR can help you see and evaluate the effects of performance criteria on the Unified CCX and Cisco Unified IP IVR server.

Impact of Performance Criteria on the Unified CM Servers

Unified CM system performance is influenced by many criteria such as:

- Software release versions— Using the Cisco Unified Communications sizing tool, make sure to select the Unified Communications Manager software version with which Unified CCX will be working.
- The type and quantity of devices registered such as:
  - CTI ports (IP IVR ports for queuing, call treatment, and self-service)
  - Gateway (GW) ports
  - Agent phones
  - Route points
- The load processed by these devices (calls per second)

- Application call flows
  - IVR self-service
  - Call treatment/Prompt and collect
  - Routing to agents,% transfers and conferences
- Special Unified Communications Manager configuration and services
  - Other non-Unified CCX devices—IP phones, GW ports, Unity ports, and dial plan.
  - Music on Hold (MOH)
  - Tracing levels— Unified Communications Manager CPU resource consumption varies depending on the trace level enabled. Changing trace level from Default to Full on Unified CM can increase CPU consumption significantly under high loads. Changing tracing level from Default to No tracing can also decrease CPU consumption significantly at high loads (this configuration is not supported by Cisco TAC). CPU consumption due to default trace will vary based on load, Unified Communications Manager release, applications installed, and call flow complexity.
- Server platform type

Cisco Finesse Design Considerations

Cisco Finesse

Introduction

Cisco Finesse is a next-generation agent and supervisor desktop designed to provide a collaborative experience for the various communities that interact with your customer service organization.

Cisco Finesse provides:

- A browser-based administration console and a browser-based desktop for agents and supervisors; no client-side installations are required.
- IP phone based (FIPPA) agent login & state control with limited features.
- A single, customizable cockpit or interface, that gives customer care providers quick and easy access to multiple assets and information sources.
- REST APIs that simplify the development and integration of value-added applications and minimize the need for detailed desktop development expertise.
- Desktop Chat feature to agents who have a configured chat identity in Cisco IM&P server.

The following table lists the availability of the Cisco Finesse REST APIs by license packages:

Table 19: Cisco Finesse REST APIs availability by license packages

Service	Unified CCX Premium	Unified CCX Enhanced
Cisco Finesse REST APIs	Available	Available

The following table lists the availability of the Cisco Finesse service in the Unified CCX packages:

Table 20: Cisco Finesse service availability by license packages

Service	Unified CCX Premium	Unified CCX Enhanced	Unified IP IVR
Cisco Finesse	Available	Available	Not available

Cisco Finesse functionalities

Cisco Finesse supports the following functionalities:

- Basic call control—Answer, hold, retrieve, end, and make calls.
- Advanced call control—Make a consultation call and transfer or conference the call after the consultation.
- Not Ready and Sign Out reason codes—Reasons that agents can select when they change their state to Not Ready.
- Wrap-up codes—Reasons that agents can apply to calls.
- Phone books—List of contacts from which agents can select one to call.
- Live data gadgets—Display current state of agents, teams and CSQs in the contact center.
- Customizable third-party gadgets.
- Recording using Workforce Optimization.
- Scheduled call back—Request a callback at a specific callback phone number and also specify the time or date of the callback.
- Reclassify—Reclassify a direct preview outbound call as busy, answering machine, fax, invalid number, or voice.
- Outbound agent—Supports outbound dialing including progressive, predictive, and direct preview modes, allowing agents to handle both inbound and outbound dialing tasks.
- Multisession webchat—Allows agents to work on multiple chat sessions at the same time for increased agent resource usage.
- Multisession email—Allows agents to work on multiple email sessions at the same time for increased agent resource usage.
- Extension mobility—Allows users to temporarily access their Cisco Unified IP Phone configuration such as line appearances, services, and speed dials from other Cisco Unified IP Phones.
- Desktop Chat - Allows users to initiate chat sessions with any other user logged in to the Cisco IM&P either from the Desktop Chat gadget or from a desktop client like Jabber.
- Team Message - Allows supervisors to broadcast messages to their teams. Allows agents to view the messages broadcasted by their supervisors. This is a one-way communication from supervisors to agents.

Note

- Team composition changes in Cisco Finesse are not updated dynamically. Log in again or refresh the browser session to see the changes.
- Transition to Logout state is possible only from Not Ready state.

You can configure the Cisco Finesse Agent and Supervisor Desktops to use Cisco gadgets and third-party gadgets through a layout management method. You can customize the Cisco Finesse Agent and Supervisor Desktops through the Cisco Finesse administration console. The administrators can define the tab names that appear on the desktops and configure which gadgets appear on each tab.

For information about supported browsers and operating systems, see the Unified CCX Compatibility related information located at: http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Note Video is now supported if you are using Cisco Jabber as agent phone. The agent desktop where Jabber is used for Video should comply to the Cisco Jabber hardware requirements listed in the *Release Notes for Cisco Jabber for Windows* , located at http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-release-notes-list.html and in the *Release Notes for Cisco Jabber for Mac*, located at http://www.cisco.com/c/en/us/support/unified-communications/jabber-mac/products-release-notes-list.html.

Administration

The administrator can access the Cisco Finesse administration web user interface in read and write mode from the Unified CCX publisher node. The Unified CCX subscriber node provides read-only access.

Cisco Finesse REST API

Cisco Finesse provides a REST API that allows client applications to access the supported features. The REST API uses secure HTTP (HTTPS) as the transport with XML payloads.

Cisco Finesse provides a JavaScript library and sample gadget code that can help expedite third-party integration. You can find developer documentation for the REST API, the JavaScript library, and sample gadgets at this location: https://developer.cisco.com/site/finesse/.

Silent monitoring

The supervisors can monitor agents calls using Unified Communications Manager-based silent monitoring with Cisco Finesse.

Cisco Finesse does not support SPAN port-based monitoring and desktop monitoring to silent monitor the agent.

Recording

Cisco Finesse workflows can be used to record agent calls using Cisco Unified Communications Manager with Cisco Workforce Optimization.

Note The agent phone must have built-in-bridge (BIB) support enabled for Cisco Unified Communications Manager-based call recording and monitoring to work with Cisco Finesse.

For information about the phones that have built-in-bridge support, see the Unified CCX Compatibility related information located at: http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

For information about recording APIs, see the at http://developer.cisco.com/web/finesse/docs.

Multiline support

You can configure one or more secondary lines on an agent phone. Unified CCX monitors the first four configured lines. The agent's ACD line must be in button positions 1 - 4. Any calls on the observed lines are reported in the historical reports. Finesse displays the calls that are present in the Agent's ACD line.

Direct Transfer Across Line (DTAL) and Join Across Line (JAL) are not supported.

NAT support

Cisco Finesse supports static NAT only with one-to-one mapping between public and private IP addresses. Finesse desktops support Fully Qualified Domain Names (FQDNs) only, where FQDN resolves to the external IP address.

E.164 support

Unified CCX agents and supervisors can login to Finesse with '+' (plus sign) as prefix. Finesse also supports E.164 for the following:

- Enterprise Data
- Phone Book Contacts
- Workflow Rules or Conditions

Cisco Finesse IP Phone Agent

With Cisco Finesse IP Phone Agent (IPPA), agents and supervisors can access Finesse features on their Cisco IP Phones as an alternative to accessing Cisco Finesse through the browser. Cisco Finesse IPPA allows agents and supervisors to receive and manage calls if they lose or do not have access to Cisco Finesse through a browser. It supports fewer features than the Finesse desktop in the browser.

Supervisor Tasks

Cisco Finesse IPPA does not support supervisor tasks such as monitor, barge, and intercept, but supervisors can sign in and perform all agent tasks on their IP Phones. For reporting purpose the supervisor will have to log in to Cisco Unified Intelligence Center to view the live data reports.

Reason Code Limits

On the IP Phone, Cisco Finesse can display a maximum of 100 Not Ready or Sign Out reason codes. If more than 100 codes are configured, the phone lists the first 100 applicable codes (global codes or applicable team codes).

Desktop Chat

Desktop Chat is a XMPP browser based chat, which is powered by Cisco Instant Messaging and Presence (IM&P) service. Desktop Chat allows agents, supervisors, and Subject Matter Experts (SMEs) within the organization to chat with each other.

For more details see, https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.

Instant Messaging and Presence (IM&P) provides presence and chat capabilities within the Unified CM platform. The Desktop Chat interface is hosted by the Finesse Agent desktop and requires a separate log in to the IM&P service.

Note Desktop Chat does not support Cisco Mobile Remote Agent /VPN based access to the IM&P server. Desktop Chat requires direct access to the IM&P server to connect to the chat service.

Cisco Instant Messaging and Presence (IM&P)

IM&P incorporates the Jabber platform and supports XMPP protocol and can track the user's presence via multiple devices. IM&P pulls its user list from users who have been enabled for chat capabilities, from Unified CM (or LDAP if LDAP integration is enabled). Only Unified CM users enabled for chat capability can login to IM&P.

Identity, Presence, Jabber

A User is identified in the IM&P service with a unique identity which is in the form of username@FQDN.com.

A user is described in terms of the identity of the user, presence status, (available, unavailable, or busy) and the presence capabilities of the user.

The presence status of the user is not related to the Agent Status and has to be managed independently by the user post login.

Cisco IM&P service combines the presence status of user across multiple devices and publishes them for subscribers who have added the contact in their contact list.

IM&P supports a composed presence for the users, which is derived from the state matrix of all the devices that the agent is logged into. Cisco IM&P takes sources of presence from the XMPP client for the user, on-hook and off-hook status from CUCM, and in a meeting status from Microsoft Exchange to generate the users overall composed presence. Desktop Chat displays the composed presence of the user. For details about how to arrive at the composed presence, refer to the *Cisco IM&P User Guide* at: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-user-guide-list.html .

Irrespective of the deployment type, the Desktop Chat requires an explicit login using the IM&P identity of the user after logging into the Finesse Desktop.

SSO is not supported with Desktop Chat and thus an explicit login is required in SSO mode.

Desktop Chat presence indicates the availability of users to communicate across the configured devices.

Desktop Chat availability will also be reflected in the combined IM&P presence of the user.

Logging into Desktop Chat, by default sets the users state as available.

An agent logging into Desktop Chat can thus be seen as available in Jabber or other XMPP platforms connected with IM&P and can communicate with these users.

Note File transfer is supported only for users communicating using Desktop Chat. For more information on the supported file types and the maximum size of file attachments see, *Desktop Properties CLIs* section in the Cisco Unified Contact Center Express Administration and Operations Guide.

Example for Desktop Chat availability:

A Desktop Chat user can be logged into the Desktop Chat and Jabber at the same time. Incoming chats will be relayed to all the logged in clients including Desktop Chat. However, Desktop Chat does not support Multi-Device-Messaging. So messages being sent from other XMPP clients like Jabber will not be displayed within the Desktop Chat. Once alternate clients are used to respond to incoming chats, further messages are not shown in Desktop Chat until the user starts responding using the Desktop Chat.

For more information on network designs, refer to the *Solution Reference Network Design* guide https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.

Cisco IM&P Design Considerations

Finesse browser makes a separate connection to Cisco IM&P over HTTPS, after it retrieves the chat server URI from the Finesse server. This requires separate certificates to be accepted if self-signed certificates are employed, in an HTTPS deployment.

The chat interaction happens over XMPP protocol, on the HTTP connection with long polling or BOSH established with Cisco IM&P.

There are no other interactions between Finesse server and browser for chat related capabilities, except for retrieving the Cisco IM&P server configurations.

Chat log persistence is available with the browser during the desktop session.

User search capabilities require Unified CM LDAP integration. In its absence, remote contacts have to be manually added by the user.

If the user is an existing Jabber user, the same contacts are shared between the Desktop Chat and Jabber which are also persisted across sessions.

There are no limits on the number of ongoing chats or the contacts in Desktop Chat apart from the restrictions or guidelines advised by Cisco IM&P. For the limit on the number of ongoing chats or the contacts and how to configure the Cisco IM&P server for chat, see the IM&P Solution Reference Networking Guide.

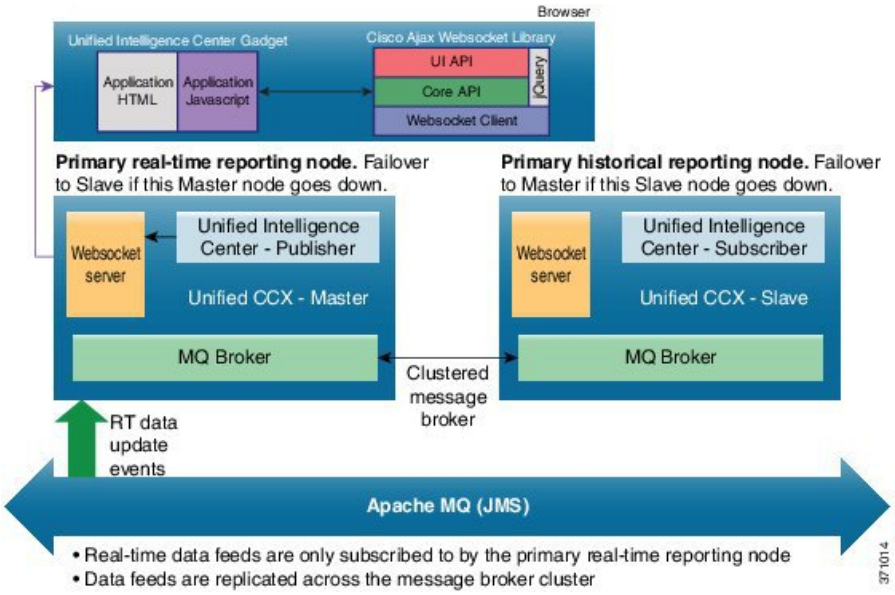
Note Desktop Chat requires the Cisco IM and Presence certificates to be trusted. For more information on accepting certificates, see the *Accept Security Certificates* section, in the *Common Tasks* chapter of *Cisco Finesse Agent and Supervisor Desktop User Guide for Cisco Unified Contact Center Express* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html.

Cisco Unified Intelligence Center Design Considerations

Unified Intelligence Center Deployments

In Unified CCX deployments, both Unified Intelligence Center and Finesse are coresident on the same server along with Unified CCX.

Figure 15: System Architecture - Cisco Unified Contact Center Express



The above diagram depicts the HA configuration of Unified CCX, where the primary node, by default, is the master, and the secondary node is the warm standby. Historical reports are not available as gadgets.

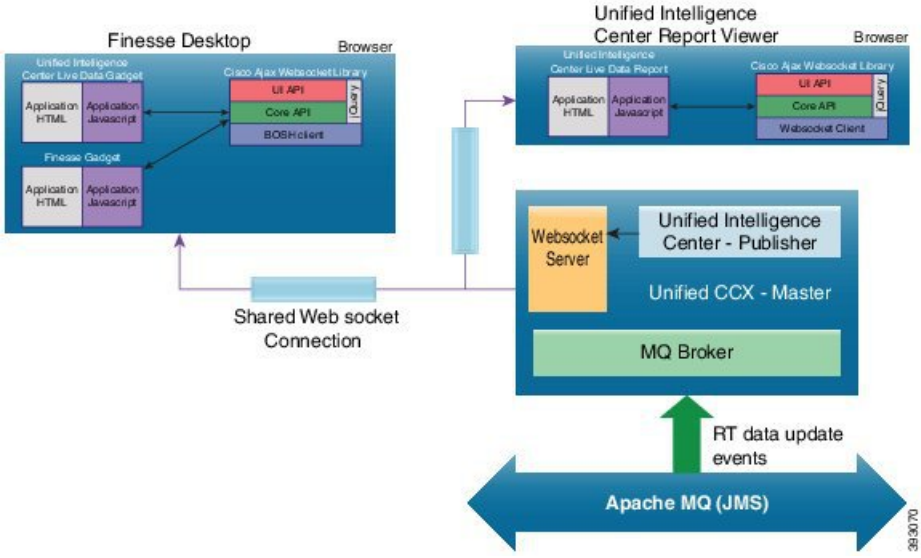
Websocket Server - Only one instance of Websocket server is installed in the Unified CCX node.

Live Data gadget on Finesse desktop - The live-data gadget is loaded on the Finesse desktop only after an Agent or Supervisor has logged in and the Finesse container is initialized. One of the reporting gadgets set up the websocket tunnel. This common tunnel is shared by all the Unified Intelligence Center gadgets.

Live Data report in Unified Intelligence Center Report Viewer or through a core permalink - All the Javascript libraries are required to create the Websocket tunnel and the OpenAjaxHub in the browser are loaded as part of the web page. A Websocket tunnel is then created from the client window to the Websocket server, and shared by all the Live Data reports that are run in the client window.

The system diagram for Live Data gadgets embedded in the Finesse desktop and for Live Data reports running in the Unified Intelligence Center Report Viewer is shown below.

Figure 16: Cisco Unified Contact Center Express - Live Data Gadgets



Standalone Cisco Unified Intelligence Center

Unified CCX 12.5(1) has been integrated with premium Cisco Unified Intelligence Center license. However, you can still use standalone Cisco Unified Intelligence Center.

The version of the standalone Cisco Unified Intelligence Center should be the same as the Unified Intelligence Center that is embedded in Unified CCX. The Standalone Cisco Unified Intelligence Center supports multiple data sources including Unified CCX.

In a Unified CCX High Availability deployment, the standalone Cisco Unified Intelligence Center should be connected to the standby node on Unified CCX to minimize the load on the master node. In case of failover of Unified CCX the Cisco Unified Intelligence Center connects to the new standby node. Standalone Cisco Unified Intelligence Center doesn't support high availability.

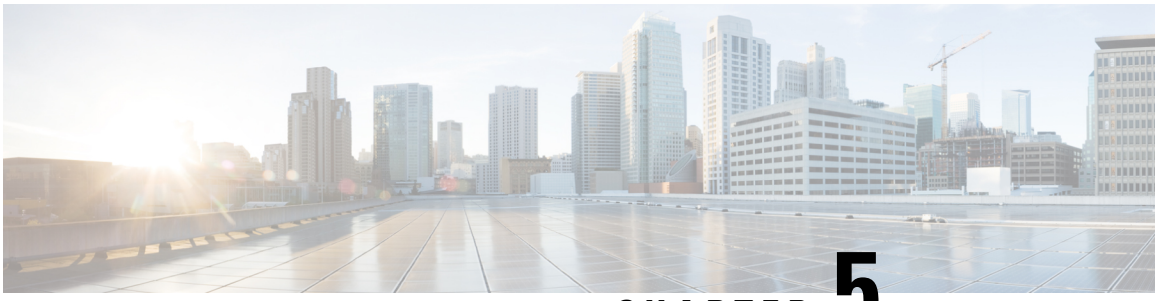
To install standalone Cisco Unified Intelligence Center, see the Installation and Upgrade Guide for Cisco Unified Intelligence Center, located at: http://www.cisco.com/en/US/products/ps9755/prod_installation_guides_list.html.

For more information on how to create custom reports, see the Cisco Unified Contact Center Express Report Developer Guide, located at: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_user_guide_list.html.

Note Live Data is not supported on the standalone Cisco Unified Intelligence Center.

Cisco Unified Intelligence Center user sync is not supported with the standalone Cisco Unified Intelligence Center and the Unified CCX server.

For standalone Cisco Unified Intelligence Center (CUIC), import the self-signed Tomcat certificate from CUIC and upload it into the Unified CCX Tomcat trust store.



CHAPTER 5

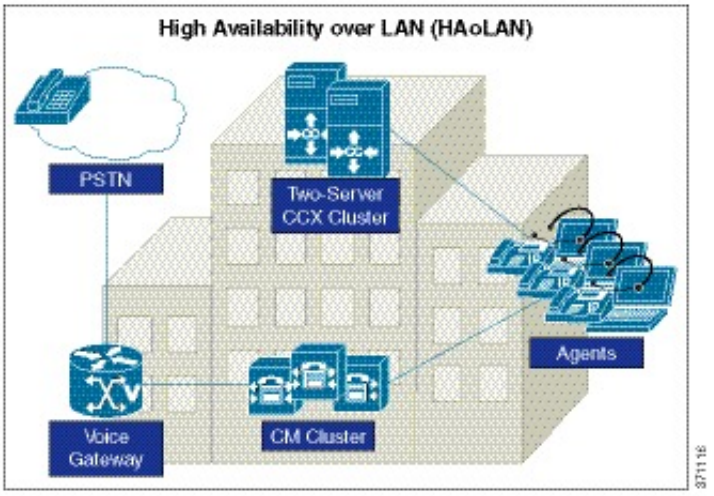
High Availability and Network Design

- Unified CCX High Availability over LAN, on page 89
- Unified CCX High Availability over WAN, on page 90
- Engine Redundancy, on page 94
- Cisco Finesse High Availability Considerations, on page 97
- Cisco Unified Intelligence Center High Availability Considerations, on page 100
- Customer Collaboration Platform High Availability Considerations, on page 101
- ASR TTS High Availability Considerations, on page 101
- Cisco IM&P High Availability Considerations, on page 101

Unified CCX High Availability over LAN

Unified CCX supports high availability over LAN to provide redundancy over LAN. The following figure depicts the deployment for Unified CCX high availability over LAN.

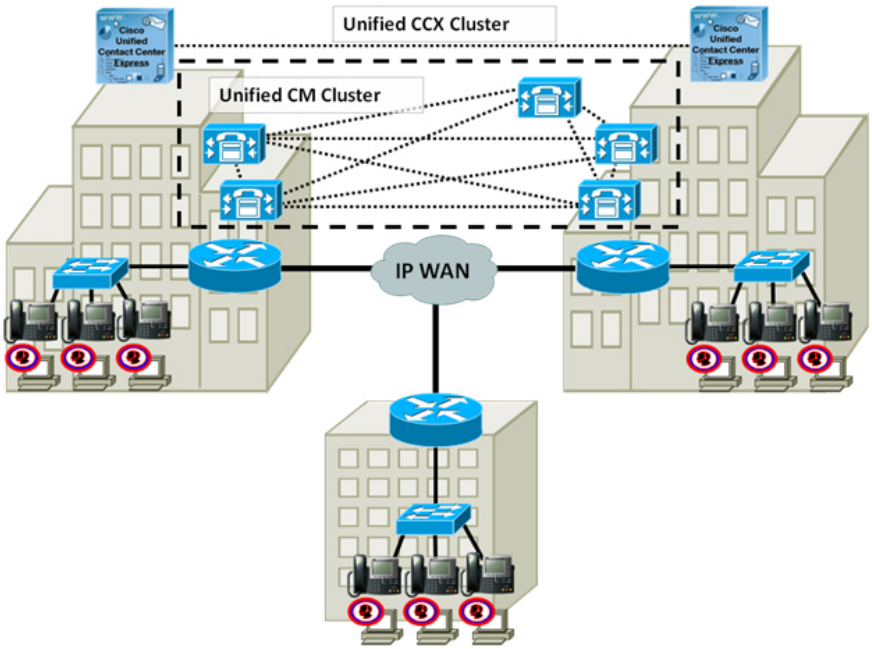
Figure 17: Unified CCX High Availability over LAN Deployment



Unified CCX High Availability over WAN

Unified CCX supports high availability over WAN to provide site redundancy. In this deployment, the Unified CCX servers are located in two different sites across the WAN. Each site should have at least one Unified CM server that is running CTI Manager with which Unified CCX communicates. The following figure depicts the deployment for Unified CCX high availability over WAN.

Figure 18: Unified CCX High Availability over WAN Deployment



Network Requirements

Observe the network requirements described in this section when deploying Unified CCX HA over WAN.

Delay

The maximum allowed round-trip time (RTT) between Unified CCX servers is 80 ms.

The maximum allowed round-trip time (RTT) between the Unified CCX server and the Unified CM server is 60 ms.

Note Do not use the ping utility on the Unified CCX server to verify RTT as it will not provide an accurate result. The ping is sent as a best-effort tagged packet and is not transported using the same QoS-enabled path as the WAN traffic. Therefore, verify the delay by using the closest network device to the Unified CCX servers, ideally the access switch to which the server is attached. Cisco IOS provides an extended ping capable of setting the Layer 3 type of service (ToS) bits to make sure that the ping packet is sent on the same QoS-enabled path that the WAN traffic will traverse. The time recorded by the extended ping is the round-trip time (RTT), or the time it takes to traverse the communications path and return. Refer to the Cisco IOS document available at

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f22.shtml#extend_ping for more detail.

Bandwidth

Sufficient bandwidth must be provisioned for Unified CCX cluster, Unified CM cluster, and other optional components to deploy HA over WAN.

The following components must be accounted for, while calculating the bandwidth requirements:

- Unified CCX Cluster and Unified CM Cluster

  Unified CCX cluster consumes bandwidth between the Unified CCX servers in high availability. If the Unified CM running CTI Manager that Unified CCX communicates with is remote, there would be additional bandwidth utilized by Unified CCX.

  Unified CM could consume significantly higher bandwidth for Intra-Cluster Communication Signaling (ICCS) between sites when deploying with Unified CCX. This is due to the additional number of call redirects and CTI/JTAPI communications encompassed in the intra-cluster communications.

  Unified CCX can be deployed as ACD to route and queue contacts for available agent or as IP-IVR to perform self-service. The bandwidth requirements for Unified CCX and Unified CM clusters are different depending on the deployment type.

  The following table shows the minimum bandwidth requirement for Unified CCX and Unified CM clusters when deploying HA over WAN.

Table 21: Unified CCX HA over WAN Bandwidth Requirement

Deployment type	Unified CCX Cluster		Unified CM Cluster	
	Between Unified CCX Servers	Between Unified CCX and Remote Unified CM Servers	Database[2]	ICCS
ACD	1.2 Mbps	800 kbps	1.544 Mbps (T1)	70 kbps per 100 BHCA[3]
IP-IVR	1.2 Mbps	200 kbps	1.544 Mbps (T1)	25 kbps per 100 BHCA

[2] This column shows the database bandwidth required for Unified CM clustering over WAN and could be subject to change. For the final authorized value, refer to *Cisco Unified Communications Solution Reference Network Design (SRND)* available at: http://www.cisco.com/go/ucsrnd
[3] BHCA (Busy Hour Call Attempt) is the number of calls entering the system in the busy hour for Unified CCX or IP-IVR.

For Unified CCX Cluster in the preceding table:

- The traffic between Unified CCX servers includes database replication, heartbeat, and other communication between the Unified CCX HA servers.
- The traffic between Unified CCX server and remote Unified CM server running CTI Manager is the JTAPI call signaling.

For Unified CM Cluster in the preceding table:

- *Database* column includes traffic for database and other inter-server traffic for every Cisco Unified CM subscriber server remote to the Unified CM publisher.
- *ICCS* column shows all the ICCS traffic between CallManager/CallManager services and CallManager/CTI Manager services running in the Unified CM nodes across sites.

As an example, assume the Unified CCX HA over WAN deployment has two sites and is used as ACD. Site 1 has the Unified CCX, one Unified CM publisher and two Unified CM subscribers. Site 2 has the other Unified CCX and two Unified CM subscribers. Unified CCX in site 1 communicates with Unified CM subscriber in site 2 for JTAPI signaling. In the busy hour, there are 1500 calls coming into Unified CCX that get routed or queued for agents.

Note

- The maximum supported RTT between the Unified CCX server and the Microsoft Exchange server is 80 ms.
- A minimum bandwidth of 64 Mbps must be provisioned between two nodes of Unified CCX for intra-cluster communication and for fetching Unified Intelligence Center reports from non-master node. The maximum latency allowed is 80 ms. For bandwidth calculation, see the Cisco Unified CCX Bandwidth Calculator located at, https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-technical-reference-list.html.

For Unified CCX cluster, bandwidth required is:

1.2 Mbps + 800 kbps (0.8 Mbps) = 2 Mbps

For Cisco Unified CM cluster, there are two Unified CM subscribers remote from the Unified CM publisher and the BHCA is 1500. Bandwidth required is:

1.544 Mbps × 2 + 70 kbps × 15 (1.05 Mbps) = 4.138 Mbps

In total, 6.138 Mbps between sites is required for this deployment.

- Agents and Supervisors

  In HA over WAN deployment, agents and supervisors could reside in either Unified CCX sites or they could be remote depending on the location of active Unified CCX server at the time of operation.

Bandwidth should be provisioned for remote agents between sites using the maximum number of agents from the two sites. Estimate the required bandwidth using the Unified CCX Bandwidth Calculator available at:

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-technical-reference-list.html

- Optional Components

  Customers might have the following optional components deployed across the WAN from Unified CCX or Unified IP IVR. Ensure to account for the additional bandwidth required in their HA over WAN deployment.

  - **Wallboard Server**— Determine the amount of data that is retrieved from Unified CCX database to the remote wallboard server.
  - **Enterprise Database**— Estimate the total amount of data that is retrieved through the database steps from the remote enterprise database.
  - **SMTP Server**— If the SMTP server is remote from the Unified IP IVR, determine the average size of each outgoing email and calculate the total.

- To calculate bandwidth for Finesse, see the *Unified CCX Bandwidth Calculator* , available at:

  https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-technical-reference-list.html

Quality of Service

Quality of Service (QoS) must be enabled and engineered correctly on the network to provide consistent and predictable end-to-end levels of service. Unified CCX software does not mark any network packet, so ensure that you mark the traffic at the network edge routers.

The following table shows the QoS markings for Unified CCX HA over WAN deployment.

Table 22: QoS Considerations for Unified CCX HA Over WAN

Traffic	QoS Marking
JTAPI Call Signaling	IP Precedence 3 (DSCP 24 or PHB CS3)
Database Replication between Unified CCX nodes[4]	IP Precedence 0 (DSCP 0 or PHB BE)

[4] The database traffic may be reprioritized to a higher priority data service (for example, IP Precedence 2 [DSCP 18 or PHB AF21] if required by the particular business needs). An example of this is the usage of outbound dialer in Unified CCX, which relies on writing data to the Config Datastore.

For more information on QoS requirements of VoIP, refer to the Enterprise QoS Solution Reference Network Design Guide available here:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoSIntro.html#wp46447

Deployment Considerations

Consider the following when deploying high availability over WAN with Unified CCX:

- Deploy the ASR or TTS server locally in each Unified CCX site
- Set up Unified CCX to use the local Unified CM servers for both primary and secondary in the following configurations. If this is not possible, at least the primary Unified CM server should be local.
  - AXL Service Provider
  - JTAPI Provider for Unified CM Telephony Subsystem
  - JTAPI Provider for Resource Manager/Contact Manager Subsystem

Note Significant delays in agent login will occur during Unified CCX failover if AXL and JTAPI communications are over WAN, especially under load conditions.

- Assign the two sets of CTI Ports (one for the master and the other for the standby engine) to different device pools, regions and locations, in the CTI Port Group.
- Data in Historical Datastore and Repository Datastore start merging after the network partition is restored. This situation could potentially generate heavy data traffic over WAN. Restore the WAN link during after hours to minimize the performance impact.
- Do not support VPN tunneling across the WAN.

Unified CCX-Finesse deployment

Cisco Finesse is supported in both single-node deployment and high-availability deployment over LAN and WAN.

Unified CCX-Cisco Customer Collaboration Platform deployment

Customer Collaboration Platform (CCP) doesn't have an HA but works with a Unified CCX in HA.

Engine Redundancy

Any incoming call arriving at Cisco Unified Communications Manager that are destined for Unified CCX route points can be accepted by the Unified CCX engine if all Unified CCX call treatment and ACD routing services are operational.

If the active Unified CCX server fails, the ACD subsystem will not be able to route calls to the agents until the automatic logging in process completes. The agents are then logged in back to the same state (Ready or Not Ready) that they were in before the failover. However, if the agent was in an active call, they are logged back into the Not Ready State and the call continues uninterrupted.

When the Master Engine is Down

Once the master engine goes down, the engine on the other node will be selected as the new master. Calls which were queued by the previous primary engine are dropped after a failover. New calls coming in while agents are re-logging will stay in the queue until agents log in. Historical data will be written to the new master engine’s local database.

Automatic Call Distribution (ACD)

The HA failure of the active server is detected and the ACD subsystem can automatically fail over from the active to the standby server. All ACD functions are restored on the standby server within 5 seconds.

Interactive Voice Response

When an active server fails in a HA system, IVR subsystem will automatically failover.

All calls in queue and calls receiving IVR call treatment will be lost. Calls already transferred to the agent will be preserved.

Unified CCX Outbound Dialer

Behavior Under High Availability

The Config Data Store (CDS) is required for general operation of outbound for call status and call result updates of contact records. When deploying in a two-node high availability system, the CDS must be running on both nodes to enable the database write operation. The Outbound subsystem will be operational as long as the Publisher CDS is up and running. In a high availability environment, only the dialer in the master node is active.

If a contact is imported for a campaign and failover occurs before the contact is dialed out, then the contact is retried the next day. The number of contacts that can be retried for each campaign is as mentioned below:

- For direct preview campaigns, the count is the maximum value that is configured for Contact Records Cache Size field.
- For IVR-based progressive and predictive campaigns, the count is the Number of Dedicated Ports multiplied with the Lines Per Port (LPP) values configured.
- For agent-based progressive and predictive campaigns, the count is 45 for medium or large VM profiles and is 15 for small VM profiles.

Failover Scenarios for Preview Outbound:

- If a preview outbound call not in reserved state is waiting for the agent to accept the call and when the master engine goes down, the agent is automatically logged out and the preview call disappears from the agent desktop. If the master engine restarts during failover, the call status for that contact record is set to unknown. If the master engine does not restart during failover, the contact is called when the campaign starts and there are available agents.
- If a preview outbound call not in reserved state is accepted by the agent and the call is ringing on the customer phone, there is no change on the call. However, the agent is logged out and will be able to use call control capabilities only through the phone.

Failover Scenarios for Progressive and Predictive IVR-Based Outbound:

- The CTI ports on the master engine will go out of service on a failover and the calls that are in progress between customers and CTI ports will be disconnected. The standby server will continue dialing out the remaining contacts in the campaign after the failover.

Failover Scenarios for Progressive and Predictive Agent-Based Outbound:

- If an agent is currently on an outbound call and Cisco Finesse service restarts or agent closes the browser and reopens, then the agent is automatically logged in after 60 seconds and the state of the agent is set to Not Ready. If the customer is still on the call, then the agent continues to handle the call but outbound specific options will not be available on the agent desktop.

WAN Link Failure Between Sites—Island Mode

Connectivity failure creates a scenario called 'Island mode' where each node (on either side of the network) assumes mastership and handles calls. Each node behaves as if the other side has failed and declares itself master (Engine and Data Stores components). The node that was already the master, continues as is. Phones and Finesse need to register with Unified CM and server on the same side of the network. This operation happens automatically. The following lists the failover behaviors:

- Historical data is written to local Data Stores
- Real Time Reporting (RTR) shows the status of each node independently
- No configuration changes are allowed
- Enterprise Database access across the network is not possible
- Outbound will be impaired as these do not support high availability

If the Island mode occurs for more than four days, DB replication between the nodes will be broken and will need to be reestablished from Unified CCX Administration web interface when the WAN link is restored.

Note Backup scripts are executed on the publisher, and it backs up the database that has mastership. In Island mode, only one node gets backed up and the data getting collected on the other node does not get backed up. The backup is inconsistent, and if restored, there will be loss of data.

When Connectivity is Restored

Once the network connectivity is restored, convergence of engine mastership occurs. Two masters cannot exist and one of the nodes will drop mastership. All active calls being handled by that node will be dropped.

Similarly, convergence happens for the data stores with no disruption in call activity. All data will be replicated as soon as convergence is done only if the link was up within a predetermined replication retention period, otherwise, the customer needs to initialize the replication from datastore control center pages.

Tip You can use the Unified CCX Administration Datastore control center pages or the CLI to check the replication status.

WAN Link and Single Engine Failure

When the WAN goes down, CTI functionality, which was provided by Unified CM Sub 1 across the WAN is no longer available. The master engine on node 2 fails over to Unified Communications Manager Sub 2. All calls still in the queue are dropped.

Some agents will remain in Not Ready state since the corresponding agent's phones are registered with the Unified Communications Manager Sub 1. There is no automatic function to force phones to re-register.

This situation is corrected when the WAN link is restored.

Chat and Email

With high availability, failure of the active server can be detected and the Web Chat subsystem automatically fails over from the active server to the standby server. All unanswered chats are moved to the new active server.

An active chat session is available until the browser gets redirected to the standby server. The chat session is terminated after the redirect is complete and the message is displayed as, 'The Chat has Ended.' During an engine failover, the agent gets a message that, 'Chat and Email are temporarily down due to Outages.' All queued contacts are discarded in Chat whereas it is reinjected in Email.

The fault tolerance for Web Chat is provided in the Unified CCX. In an HA deployment, Customer Collaboration Platform is configured to communicate with both the Unified CCX nodes. When a new contact arrives at Customer Collaboration Platform, both the Unified CCX nodes are notified.

In the case of a failover, all emails that were previously queued and were assigned to an agent get requeued and get assigned to the agents.

Attention Cisco Customer Collaboration Platform does not support HA deployment options. Chat and email will not be available if Customer Collaboration Platform is down.

Note Web Chat and email do not support the Island mode scenario.

Cisco Finesse High Availability Considerations

This section describes Cisco Finesse Desktop behavior during the failover of one of the following:

- Unified CCX Engine failure
- Cisco Finesse Server failure
- Notification Service failure
- CM failure
- Netwrok failure between two centers
- Network failure between agent and supervisor desktop

For HA deployment the Cisco Finesse is in service on both the nodes, based on the following requirements:

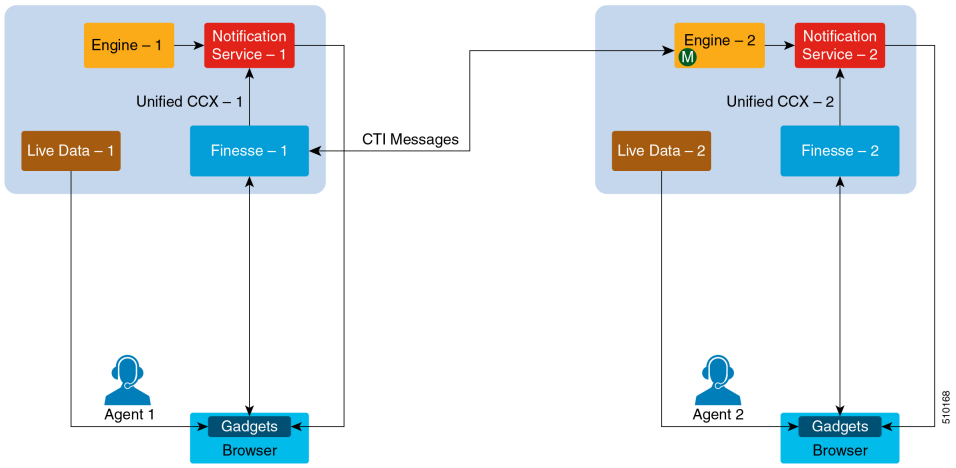
- On Unified CCX Master node:
  - Finesse is in In Service if its connected to the Unified CCX engine, and Notification service on the same node.

- On Unified CCX Non-Master Node:
  - Finesse is in In Service if it is able to connect to the Master CCX engine (remote).
  - Unified CCX engine is running in slave mode on the Non-Master node.
  - Notification Service is running on Non-Master node.

This enables the desktop failover to happen independent of the engine mastership status.

The following image describes the high level view of the Cisco Finesse Desktop Failover scenario.

Figure 19: High Level View Architecture Diagram of Cisco Finesse Desktop Failover Scenario



Note Agent logging into both the Finesse nodes simultaneously is not supported.

Unified CCX does not support load balancing of agent login. All agents must log in to the Master Node only. The enhancement in behavior is for failover support only.

For voice calls, Finesse connects to CTI server on master CCX Engine.

For agents to log in to Finesse in the secondary node, Notification Service, Engine and LiveData services (Socket.IO Service) have to be running on the secondary node.

Failure Scenarios in HA Deployment

This table describes failure scenarios that you might encounter in high availability deployment when the Unified CCX Node 1: Master, Unified CCX Node 2: Non-master before failover.

Failure Scenario	Unified CCX HA Behavior	Cisco Finesse Service on Node 1	Cisco Finesse Service on Node 2	Cisco Finesse Client Behavior

Unified CCX Engine fails over from master to Non-Master node	Engine Mastership changes from master to non-master.	Finesse goes **OUT_OF_SERVICE** and will return to **IN_SERVICE** as soon as it connects to the new master engine.	Finesse goes **OUT_OF_SERVICE** and will return to **IN_SERVICE** as soon as it connects to the new master engine.	Agent would see the red disconnection bar, and will automatically relogin into the Finesse side that comes to **IN_SERVICE** first. It can be either Node 1 or Node 2.
Unified CCX Engine Failure on Non-Master node	Unified CCX Engine on Node 1 continues to be Master, thus no change.	Finesse will continue to be in **IN_SERVICE**.	Finesse goes **OUT_OF_SERVICE**.	Agents connected to Node 1 will continue to be logged in. Agents connected to Node 2 will be temporarily disconnected and will connect to the Finesse Service on the node that is **IN_SERVICE**.
Finesse Service Out of Service on Node 1	Engine mastership is not affected.	**OUT_OF_SERVICE**	Finesse on Node2 will continue to be in **IN_SERVICE**.	Any agents connected to Node 1 will be temporarily disconnected and will connect to Finesse on Node 2. Agents connected to Node 2 will not be impacted.
Finesse Service Out of Service on Node 2	Engine mastership is not affected.	Finesse on Node 1 will continue to be in **IN_SERVICE**.	**OUT_OF_SERVICE**	Any agents connected to Node 2 will be temporarily disconnected and will connect to Finesse on Node 1. Agents connected to Node 1 will not be impacted.
Unified CCX Notification Service Failure on Node1	Engine mastership is not affected	**OUT_OF_SERVICE**	Finesse on Node 2 will continue to be **IN_SERVICE**.	Any agents connected to Node1 will be temporarily disconnected and will connect to Finesse on Node 2. Agents connected to Node 2 will not be impacted.

Unified CCX Notification Service Failure on Node 2	Engine mastership is not affected	Finesse on Node 1 will continue to be **IN_SERVICE**	Finesse service on the node where notification service failed, remain **OUT_OF_SERVICE** until notification service comes up.	Any agents connected to Node 2 will be temporarily disconnected and will connect to Finesse on Node 1. Agents connected to Node1 will not be impacted.
Island Mode	Both HA nodes become Master	Finesse on Node 1 will continue to be **IN_SERVICE** and will be connected to Engine on Node 1.	Finesse goes Out Of Service and will return to **IN_SERVICE** as soon as it connects to the engine on Node 2 which is also the master.	Agents connected to Node 1 will continue to be logged in. Agents connected to Node 2 will be temporarily disconnected and will connect to the Finesse Service on the Node 2.

Finesse IP Phone Agent Failure Behavior

The Finesse IP Phone Agent does not automatically failover to the alternate Finesse server. To ensure continued operations in a failure situation, you must configure at least two Finesse IP Phone services in Unified CM, each pointing to different Finesse servers.

When the Finesse server fails, Finesse IPPA attempts to reconnect to it every 5 seconds. After three attempts, if the Finesse server is not in service, Finesse IPPA displays a server unavailable message to the agent. The total time to go out of service is approximately 15 seconds.

In a failure scenario, the Finesse IPPA agents must exit from the current Finesse service and manually sign in to another configured Finesse service that points to an alternate Finesse server. After they successfully sign in to an alternate Finesse service, the agents can resume usual operations.

Cisco Unified Intelligence Center High Availability Considerations

Server is Down

In a two-node high availability (HA) setup, you can connect to any node to access reports. If the node you are connected to goes down, then manually log in to the other node to access reports as this doesn't happen automatically.

Island Mode

If WAN is down, the nodes function in Island mode and both of the nodes independently assume mastership (engine and data stores components). You can access reports from either of the nodes.

Note There will be a data discrepancy in the reports as there is no data replication between the nodes till the connectivity is restored.

Standalone CUIC has no high availability.

Customer Collaboration Platform High Availability Considerations

Cisco Customer Collaboration Platform (CCP) does not support high availability.

CCP uses either a small or large, single-server, all-in-one, deployment. You cannot use a load-balancing, split site deployment.

ASR TTS High Availability Considerations

solution supports redundant ASR/TTS servers. In a basic configuration, the VXML Gateway first passes all incoming requests to the primary ASR/TTS server. If the primary server is unreachable, the gateway then passes that request to the backup server. Any request that reaches the backup server stays on that server for the duration of the request.

You can add a load balancer to spread the incoming requests across your ASR/TTS servers.

Cisco IM&P High Availability Considerations

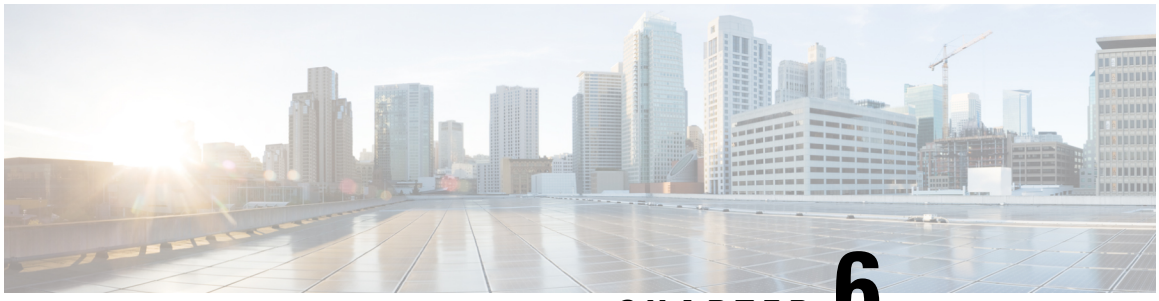
Failover is supported for Desktop Chat and any Cisco IM&P node failure results in automatic connection to the node pair peer, as configured for the user.

Desktop Chat Failover

The following table lists the desktop chat failover scenarios:

Failover Type	Desktop Chat Behavior
Cisco IM&P server failover	The desktop chat status is retained, and all active chat sessions are lost.
Finesse server failover	The desktop chat status is retained, and all active chat sessions are lost.
server failover	The desktop chat status and all chat sessions are retained.

See the Cisco Finesse Administration Guide for failover details with Desktop Chat.



CHAPTER 6

Solution Security

- Security, on page 103
- Transport Layer Security, on page 104
- Cross-Origin Resource Sharing (CORS), on page 105
- Gadget Source Allowed List, on page 105
- Secure Real-Time Protocol (Secure RTP or SRTP), on page 105
- Federal Information Processing Standards 140-2 Level 1, on page 106

Security

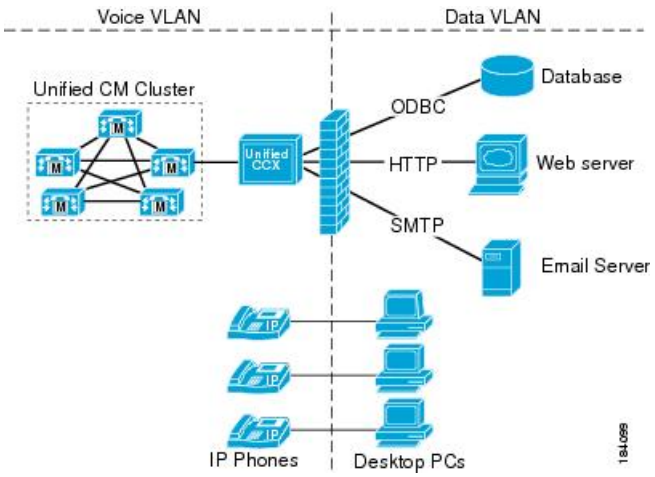
Security can be implemented on many levels. Applications security is dependent upon security implemented at the infrastructure level. For more details on security at the network infrastructure level, refer to the security design considerations in the *Cisco IP Telephony Solution Reference Network Design* documentation, available here:

http://www.cisco.com/warp/public/779/largeent/it/ese/srnd.html

Corporate Data Access

In addition to call routing, Unified CCX or Cisco Unified IP IVR scripts often process enterprise data from existing corporate data stores such as a database or a corporate directory server for functions such as account authentication and order status. These data stores often already exist and share data with other enterprise applications. This figure shows an example of a network where voice and data components reside in separate VLANs and are separated by a firewall.

Figure 20: Unified CCX Accessing Data Stores



Unified CCX can communicate with these external sources through its subsystems, provided that Network Address Translation (NAT) is not used.

SSL HTTPS Connection

The certificates uploaded using the Cisco Unified OS Administration interface to the Tomcat trust store is available to secure all HTTP connections made during script execution. The following can be secured:

- Document steps
- VoiceXML script
- Custom java code that provides web services

Enhanced Security API (ESAPI)

A new security filter is added to the Application Administration component. This filter identifies malicious user input and protects the application against XSS attacks.

If the Application Administration users find any user activity that was allowed earlier is now blocked by the security filter, then disable the security filter using a CLI command.

Transport Layer Security

The Cisco Unified Contact Centre Express supports the TLS version 1.2. The following command line interface commands can be used to show and set the TLS minimum version in the server and the client applications:

- show tls server min-version
- show tls client min-version
- set tls server min-version
- set tls client min-version

Note

- You must relaunch Cisco Unified CCX Editor and Cisco Unified Real-Time Monitoring Tool after the upgrade of Unified CCX.
- Ensure that the Unified CCX server and the client application is restarted for the changes to take effect.

Cross-Origin Resource Sharing (CORS)

Finesse supports CORS requests and allows the customization of the domains which are allowed to make CORS requests to the Finesse desktop. Once CORS is enabled via the CLI **utils finesse cors enable**, the CORS origin request from external domains is blocked by the browser. To enable specific domains to access Finesse desktop via CORS, the domains need to be added to the CORS origin allowed list using the CLI **utils finesse cors allowed_origin add**. For more information on the CORS CLIs, see *Cisco Finesse CLI*.

Gadget Source Allowed List

Shindig proxies requests from the Finesse desktop to external servers and this introduces the possibility of server side request forgery (SSRF). To prevent SSRF, you can choose to restrict outgoing connections requested by the gadgets to specific URIs by enabling shindig allowed list CLIs and adding the required URIs to the allowed list. For more information on Gadget Source Allowed List CLIs, see *Cisco Finesse CLIs*.

Secure Real-Time Protocol (Secure RTP or SRTP)

Secure Real-Time Transport Protocol (SRTP) provides authentication and encryption to secure privacy and confidentiality for voice conversation and other media. It also provides protection against replay attacks. Signaling authentication validates that no tampering has occurred to signaling packets during transmission. The confidentiality of the media is protected with cryptographic procedures as defined in IETF RFC 3711.

Voice security feature supports the following capabilities between voice gateway and IP phones:

- Media encryption and authentication of voice RTP streams using SRTP.
- Exchange of RTP Control Protocol (RTCP) information using SRTP.
- SRTP to RTP fallback for calls between secure and non-secure endpoints.
- When SRTP is enabled, a secure JTAPI connection is established between the following subsystems and Unified CM:
  - Unified CM Telephony
  - RmCm

SRTP Considerations

Before enabling SRTP in your Unified CCX deployment, ensure the following points:

- Voice gateway or the router is secure.
- SIP trunks between CUCM and voice gateway are secure.
- Cluster Security Mode is set to Mixed mode in CUCM.
- CUCM AXL Webservice is running on CUCM AXL Service Provider node.
- CAPF service is running on CUCM Publisher and it is accessible.
- None of the certificates are expired on any of the CUCM nodes.
- Unified CCX Engine is running on all Unified CCX nodes.
- The **Access Control Groups** in CUCM, **Standard CTI Allow Reception of SRTP Key Material** and **Standard CTI Secure Connection** is associated with the application user.
- Agent and Supervisor phones are secure. Supervisors phones must be secure to monitor the agents phones.
- Refer to the Unified CCX Compatibility Matrix for CUCM version that is supported for SRTP.

When SRTP is enabled in FIPS 140-2 mode, if you perform a Unified CCX DRF restore, ensure to re-sync JTAPI and restart Unified CCX Engine on all the nodes.

Note The media leg between Unified CCX and gateway uses SRTP. However, media leg between Unified CCX and Nuance Speech server uses RTP.

SRTP is not applicable for Home Agents with Extend and Connect.

For more information on how to enable SRTP, see *System Parameters* section in *Cisco Unified Contact Center Express Administration and Operations Guide* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

Federal Information Processing Standards 140-2 Level 1

Federal Information Processing Standards (FIPS) 140-2 Level 1 is a U.S. and Canadian government certification standard that defines minimum security requirements for cryptographic modules protecting sensitive information in computer and telecommunications systems. It also defines algorithms that are allowed to be used to encrypt sensitive information. These strictly defined requirements are important for government agencies, hospitals, and other customers, who would require a higher level of security.

Use CLI to enable or disable FIPS 140-2 mode on Unified CCX.

Caution FIPS 140-2 mode is supported only on releases that have been through FIPS compliance.

FIPS 140-2 Level 1 Considerations

For using FIPS 140-2 mode, consider the following points:

- Backup the system before and after enabling FIPS 140-2 mode.

- Ensure that SRTP is disabled before enabling or disabling FIPS 140-2 mode in Unified CCX. You can enable SRTP after enabling or disabling FIPS 140-2 mode in Unified CCX.
- If you upgrade Unified CM when SRTP is enabled in FIPS 140-2 mode, you must resync JTAPI and restart Unified CCX Engine on all the nodes after completing the upgrade.

Note For more information about SRTP, see the previous section in this chapter.

- After enabling or disabling FIPS 140-2 mode, the existing application certificates are re-generated.
  - For third-party CA issued Tomcat certificate:
    - Upload the re-signed certificate to Unified CCX server.
    - Upload the CA root certificate of Unified CCX to CCP.
  - For third-party CA issued IPsec certificates, re-sign the certificates and upload them to the respective nodes.
  - For Self-Signed certificates, you must upload the newly generated Unified CCX certificate to CCP.
- After enabling FIPS 140-2 mode, you may not be able to access any of the Unified CCX applications due to HTTP Strict Transport Security (HSTS) settings in the browser. To add the HSTS exception and access the Unified CCX applications, please refer to the respective browser documentation.
- Ensure that FIPS 140-2 mode is disabled before registering or unregistering Cloud Connect services. You can enable FIPS 140-2 mode after registering or unregistering Cloud Connect services.

For more information on how to enable and disable FIPS 140-2 mode, see *utils fips* section in *Cisco Unified Contact Center Express Administration and Operations Guide* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

FIPS 140-2 Mode Restrictions

Communication with the following interfaces will not operate in FIPS 140-2 mode:

Table 23: FIPS 140-2 Mode Restrictions

Interface	Restrictions
SNMP v3	FIPS mode does not support SNMP v3 with MD5 or DES. When FIPS 140-2 mode is enabled, if you have SNMP v3 configured, you must configure **SHA** as the Authentication Protocol and **AES128** as the Privacy Protocol.
External Database through Unified CCX Scripts	Communication with external database by using Unified CCX engine DB Steps.
CTI Client	Communication with third-party CTI clients.

Interface	Restrictions
Unified CCX Notification Client	Communication to Cisco Unified CCX Notification Service through 5223 or 7443 ports.
Email through Unified CCX Scripts	Email server communication by using scripts with eMail steps.
ASR/TTS	Communication with ASR and TTS Servers.

Supported Ciphers

Cisco Tomcat

The applications **Cisco Unified CCX Administration**, **Cisco Unified Serviceability**, **Cisco Unified CCX Serviceability**, **Cisco Unified OS Administration**, and **Disaster Recovery System** use Cisco Tomcat.

The following are the Ciphers that are supported in FIPS mode:

- `TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048)`
- `TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048)`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)`
- `TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)`
- `TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)`

The following are the Ciphers that are supported in Non-FIPS mode:

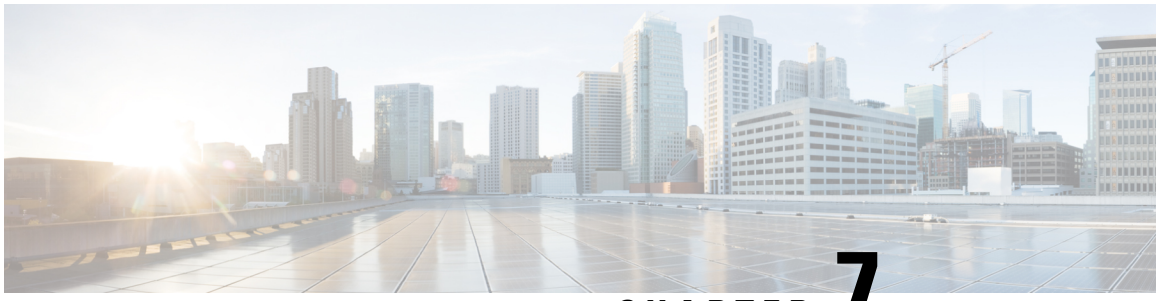
- `TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024)`
- `TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 1024)`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)`
- `TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)`
- `TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)`

Cisco Finesse Tomcat, Cisco Identity Service, and Cisco Unified Intelligence Center Reporting Service

All the following Ciphers are supported in both FIPS and Non-FIPS Mode:

- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)`

- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048)



CHAPTER 7

Design Considerations for Integrated Features

- Single Sign-On (SSO) Considerations, on page 111

Single Sign-On (SSO) Considerations

The Single Sign-on feature authenticates and authorizes users for all the contact center solution applications and services. Authentication is the process of validating the identity of a user: "you are who you say you are." Authorization is the process of confirming that an authenticated user is permitted to perform the action they are requesting: "you can do what you are asking to do." When you enable SSO in the contact center solution, users only sign in once to gain access to all of their Cisco browser-based applications and services.

To support SSO for the contact center solution, you must install and configure an Identity Provider (IdP) that is compliant with the Security Assertion Markup Language 2.0 (SAML v2) Oasis standard. For a current list of supported Identity Provider products and versions, see the Unified CCX Compatibility related information located at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Authentication and authorization are managed for the contact center solution by the Cisco Identity Service (Cisco IdS). When an SSO-enabled user signs in, the Cisco IdS interacts first with your Identity Provider (IdP) to authenticate the user. The IdP stores user profiles and provides authentication services to support SSO sign-ins. When the user is authenticated, the Cisco IdS exchanges information with the Cisco service the user is attempting to access to confirm that the user is authorized for the role they are requesting. When the user is authenticated, the Cisco IdS issues an access token that allows the user to access the application. Once access is established during a particular session, the user can switch among contact center solution applications without presenting credentials again.

Note The user credentials are only presented to the IdP. The contact center solution applications and services only exchange tokens; they do not see the users' information.

To integrate your IdP with your contact center solution, you perform the following administrative tasks:

- Establish a trust relationship between the Cisco IdS and the Identity Provider.
- Set the SSO mode in your system to enable users for SSO.
- Register on the Single Sign-On web page to onboard the single sign-on components.

- Perform **Test SSO Setup** on the single sign-on web page to test the status of registration of each component. You will be redirected to the Identity Provider for authentication. If the **Test SSO Setup** is successful then the **Enable** option is enabled.

SSO Message Flow

An SSO user's access token is issued by Cisco IdS to validate the users accessing the corresponding applications. When the user is found valid each application performs the authorization locally. Cisco IdS supports authorization Code Grant Flow as defined in OAuth 2.0 and in turn uses SAML v2.0 to authenticate users before issuing auth code.

When a user browses to a web page for an SSO-enabled service, the authentication request is redirected to the Cisco Identity Service. Cisco Identity Service generates a SAML authentication request and directs it to the Identity Provider. The IdP presents a sign-in page to the user at the browser to collect the user's credentials. After the IdP authenticates the user, the IdP issues a SAML assertion to the Cisco IdS. The assertion contains trusted statements about the user, for example, username and privileges.

The assertions must have attributes. The Cisco IdS extracts **uid** and **user principal** and generates and delivers authorization code to the SSO enabled application. The application on receiving the authorization code will request IDs For Access and Refresh Tokens.

Access Tokens are used by applications to validate user information and Refresh Token are used to request new Access Tokens. These token have a validity period associated with each one of them.

Note A new Access token and Refresh token pair can be obtained only before the Auth code expires.

Access Tokens can be refreshed only when both the current access token and the refresh token are valid and not expired.

If the refresh tokens expire you can not refresh an access token. Thus you need to be authenticated again and the auth code need to ne requested again.

Together SAML and OAuth make it possible for a user to authenticate while only exposing user credentials to the authentication provider. The username and password are only presented to the IdP. The contact center solution applications and services do not see the user information. Only the SAML assertion and the OAuth token are exchanged.

Single Sign-On High Availability Considerations

Every core component in the contact center solution has the Cisco Identity Service client that supports an high availability mode. Any SSO enabled application can connect to either to the local Cisco Identity Service instance or to the remote.

By default it will connect to the local instance of Cisco Identity Service. The Local Cisco Identity Service is the default and the preferred Cisco Identity Service that runs locally.

Cisco Identity Service client supports failover if the remote Cisco Identity Service is configured when the local Cisco Identity Service fails. When the local Cisco Identity Service is available again the Cisco Identity Service client fails back to the local Cisco Identity Service.

The below table provides the details of Cisco Identity Service client failover and failback in different states of the local and remote Cisco Identity Service:

Table 24: Failover and Failback Scenarios of Cisco Identity Service Client Based on the State of Cisco Identity Service

Local Cisco Identity Service	Remote Cisco Identity Service	Cisco Identity Service Client Connects to
IN_SERVICE	Not Applicable	Local Cisco Identity Service
PARTIAL_SERVICE	IN_SERVICE	Remote Cisco Identity Service
PARTIAL_SERVICE	PARTIAL_SERVICE	Local Cisco Identity Service
OUT_OF_SERVICE	PARTIAL_SERVICE	Remote Cisco Identity Service
OUT_OF_SERVICE	OUT_OF_SERVICE	None
OUT_OF_SERVICE	Not Configured	None

Single Sign-On Design Impacts

This section details few of the design impacts of the Single Sign-On (SSO) feature. The implementation requires you to use only HTTPS protocol to access all the web applications. The HTTP access to web applications is not supported when the SSO is enabled.

Authentication Modes in Unified CCX

You can choose from two different authentication modes when deciding about implementing SSO:

- **SSO** - Enable **all** agents, supervisors, and administrators (administrators of the Cisco Unified CCX Administration or Cisco Unified CCX Serviceability application) in the deployment for SSO.
- **Non-SSO** - Use existing Unified CM-based or local authentication.

Applications in SSO Mode

- Cisco Unified Intelligence Center (CUIC)
- Cisco Finesse
- Cisco Finesse-hosted gadgets
- Cisco Unified CCX Administration
- Cisco Unified CCX Serviceability.

Note The Cisco Finesse IP Phone Agent is not supported in SSO enabled mode.

Single Sign-On can independently function on Unified CM and Unified CCX. It is not inter dependant on each other.

Applications not SSO Enabled

The following applications are not Single Sign-On enabled:

- Cisco Finesse Administration
- Cisco Identity Service Administration
- Disaster Recovery System
- Cisco Unified OS Administration
- Cisco Unified Serviceability
- Standalone Cisco Unified Intelligence Center
- Cisco Unified CCX Editor
- Real Time Monitoring Tool
- Cisco Customer Collaboration Platform
- Cisco Workforce Optimization
- Cisco Finesse Desktop Chat
- Any Third Party Application.

Qualified Identity Providers

If you use any Identity Provider (IdP) outside of the listed IdPs in the table below, Cisco IdS supports the IdP as long as the IdP is SAML 2.0 compliant and meets the following requirements described in the subsequent SAML Request and Response sections:

- SAML Request Attributes
- Expectations from SAML Response

IdP Metadata Schema

When you configure IdS and exchange Metadata between Cisco Identity Service (IdS) and the Identity Provider (IdP), ensure that the IdP Metadata file should confirm to the SAML metadata schema at:

https://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd

SAML Request Attributes

SAML request supports the following SAML 2.0 bindings:

- **HTTP-POST** binding
- NameIDFormat in SAML request must be **urn:oasis:names:tc:SAML:2.0:nameid-format:transient**
- SAML request must be signed using **SHA-256**.

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
       ID="s25f4fb66688cf429e430034f4cceac00b6124570d" Version="2.0"
       IssueInstant="2018-10-29T10:01:39Z"
Destination="https://win-adfs30-151.uccxteam.com/adfs/ls/"
       ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
```

```
       AssertionConsumerServiceURL="https://ccxssodemo1.cisco.com:8553/ids/saml/response">
    <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">ccxssodemo1.cisco.com</saml:Issuer>
    <samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
           Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
          SPNameQualifier="ccxssodemo1.cisco.com" AllowCreate="true"></samlp:NameIDPolicy>
</samlp:AuthnRequest>
```

Expectations from SAML Response

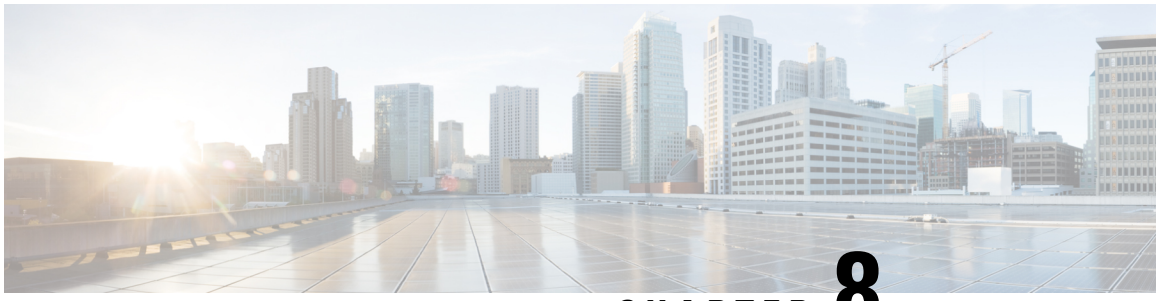
The following are the expectations from SAML Response:

- The entire SAML response (message and assertion) is signed or only the message is signed but not the SAML assertion alone is signed.
- SAML Assertion must not be encrypted.
- SAML response must be signed using **SHA-128**.
- SAML response must be signed using **SHA-256**.
- NameIDFormat in SAML response must be **urn:oasis:names:tc:SAML:2.0:named-format:transient**.
- **uid** and **user_principal** attributes should be present in SAML assertion in the AttributeStatement section.

  The "uid" attribute value must be the user Id using which users log in to Cisco contact centre applications that are SSO enabled and the "user_principal" attribute value must be in uid@domain format.

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
Destination="https://ids-ssp-node.cisco.com:8553/ids/saml/response"
    ID="_6a309495-d3c2-4a28-b8e3-289f8f5355bd"
InResponseTo="s21c84ba20862f573f5daec121c305ba6aac877843"
    IssueInstant="2017-08-10T13:20:26.556Z" Version="2.0">
    <Issuer
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://ADFSServer.cisco.com/adfs/services/trust

    </Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
 />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
            <ds:Reference URI="#_6a309495-d3c2-4a28-b8e3-289f8f5355bd">
            ..........
            </ds:Reference>
        </ds:SignedInfo>
        ..........
        ..........
     </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_df3bdbcf-a225-4e97-b00a-a199bdda3d2c"
        IssueInstant="2017-08-10T13:20:26.556Z" Version="2.0">
        <Issuer>http://ADFSServer.cisco.com/adfs/services/trust</Issuer>
        ..............

        ..............
            <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                NameQualifier="http://ADFSSserver.cisco.com/adfs/services/trust"
```

```
                    SPNameQualifier="ids-ssp-node.cisco.com">CISCO\Admin121</NameID>
                <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <SubjectConfirmationData
                        InResponseTo="s21c84ba20862f573f5daec121c305ba6aac877843"
                        NotOnOrAfter="2017-08-10T13:25:26.556Z"
                        Recipient="https://ids-ssp-node.cisco.com:8553/ids/saml/response" />
                </SubjectConfirmation>
            </Subject>
            <Conditions NotBefore="2017-08-10T13:20:26.556Z"
                NotOnOrAfter="2017-08-10T14:20:26.556Z">
                <AudienceRestriction>
                    <Audience>ids-ssp-node.cisco.com</Audience>
                </AudienceRestriction>
            </Conditions>
            <AttributeStatement>
                <Attribute Name="user_principal">
                    <AttributeValue>Admin121@cisco.com</AttributeValue>
                </Attribute>
                <Attribute Name="uid">
                    <AttributeValue>Admin121</AttributeValue>
                </Attribute>
            </AttributeStatement>
            <AuthnStatement AuthnInstant="2017-08-10T13:18:12.086Z"
                SessionIndex="_df3bdbcf-a225-4e97-b00a-a199bdda3d2c">
                <AuthnContext>

<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</AuthnContextClassRef>

                </AuthnContext>
            </AuthnStatement>
        </Assertion>
</samlp:Response>
```



CHAPTER 8

Bandwidth, Latency, and QoS Considerations

• Bandwidth, Latency, and QoS for Core Components, on page 117

Bandwidth, Latency, and QoS for Core Components

Estimating Bandwidth Consumption

Bandwidth plays a large role in deployments involving:

- The centralized call processing model (Unified CCX at the central site)
- Any call deployment model that uses call admission control or a gatekeeper

Unified CCX Bandwidth Calculator

The Unified CCX Bandwidth Calculator is a spreadsheet that can be used as reference while provisioning the bandwidth for the different operations between:

- Client applications to Unified CCX
- Unified CCX to External Systems.

The bandwidth calculator details how the bandwidth provisioning can be estimated for the following features between the Unified CCX solution components:

- Email
  - Bandwidth that can be provisioned between Agent desktop and Customer Collaboration Platform.
  - Bandwidth that can be provisioned between Email Server and Customer Collaboration Platform.
- Chat
  - Bandwidth that can be provisioned between Agent desktop and Customer Collaboration Platform.
- External System Interactions
  - Bandwidth that can be provisioned for Enterprise Database (EDBS) flow using the JDBC.
  - Bandwidth that can be provisioned for REST APIs in HTTP and HTTPS mode.

- Unified Intelligence Center Reports
  - Bandwidth that can be provisioned for the Unified Intelligence Center Reports related flow.
- Finesse IPPA
  - Bandwidth that can be provisioned for the Finesse IPPA flow.

For more information on how to estimate the bandwidth consumption see, Cisco Unified CCX Bandwidth Calculator located at, https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-technical-reference-list.html.

Remote Agent Traffic Profile

Unified CCX signaling represents only a very small portion of control traffic (Agent and Supervisor Desktop to and from the Unified CCX Server) in the network. For information on TCP ports and Differentiated Services Code Point (DSCP) marking for Unified CCX and CTI traffic.

Bandwidth estimation becomes an issue when voice is included in the calculation. Because WAN links are usually the lowest-speed circuits in an IP Telephony network, particular attention must be given to reducing packet loss, delay, and jitter where voice traffic is sent across these links. G.729 is the preferred codec for use over the WAN because the G.729 method for sampling audio introduces the least latency (only 30 milliseconds) in addition to any other delays caused by the network.

Where voice is included in bandwidth, system architects should consider the following factors:

- Total delay budget for latency (taking into account WAN latency, serialization delays for any local area network traversed, and any forwarding latency present in the network devices). The generally agreed-upon limit for total (one-way) latency for applications in a network is 150 milliseconds.
- Impact of delays inherent in the applications themselves. The average Unified CCX agent login time with no WAN delay is 8 seconds. This includes the exchange of approximately 1,000 messages between the agent application and various servers. The overall time to log in agents increases by approximately 30 seconds for each 30 milliseconds of WAN delay.
- Impact of routing protocols. For example, Enhanced Interior Gateway Routing Protocol (EIGRP) uses quick convergence times and conservative use of bandwidth. EIGRP convergence also has a negligible impact on call processing and Unified CCX agent logins.
- Method used for silently monitoring and recording agent calls. The method used dictates the bandwidth load on a given network link.

Use the following table to estimate the number of Unified CCX agents that can be maintained across the WAN (with IP Telephony QoS enabled). These numbers are derived from testing where an entire call session to Unified CCX agents, including G.729 RTP streams, is sent across the WAN. Approximately 30 percent of bandwidth is provisioned for voice. Voice drops are more of an issue when you are running RTP in conjunction with Cisco Finesse and other background traffic across the WAN. These voice drops might occur with a specific number of agents at a certain link speed, and those possible scenarios are denoted by the entry N/A (not applicable) in the following table.

Table 25: Remote Agents Supported by Unified CCX Across a WAN Link

Frame Relay	128 KB	256 KB	512 KB	768 KB	T1
G.729	3	7	15	25	38

Frame Relay	128 KB	256 KB	512 KB	768 KB	T1
G. 711	N/A	N/A	N/A	N/A	14

In remote agent deployments, QoS mechanisms should be used to optimize WAN bandwidth utilization. Advanced queuing and scheduling techniques should be used in distribution and core areas as well. For provisioning guidelines for centralized call processing deployments, refer to the *Cisco IP Telephony Solution Reference Network Design* documentation, available online at: http://www.cisco.com/go/ucsrnd.

External System Interactions

Unified CCX application supports interactions with external systems to include the transaction logic in the business logic while creating customer applications. There are four Database (DB) steps that use the JDBC infrastructure and REST API steps in HTTP and HTTPS mode to achieve the interactions with external systems. Using these script-based steps, the transactions can be done in the Unified CCX application seamlessly.

For bandwidth requirements, while performing the external system interactions with the external database and REST APIs see, Cisco Unified CCX Bandwidth Calculator located at, https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-technical-reference-list.html.

IP Call Bandwidth Usage

An IP phone call consists of two streams of data. One stream is sent from phone A to phone B. The other stream is sent from phone B to phone A. The voice data is encapsulated into packets that are sent over the network. The amount of data required to store a voice stream is dependent upon the Codec used to encode the data.

The voice data itself is transmitted over the network using the Real-Time Transport Protocol (RTP). The RTP protocol supports *silence suppression*. When silence suppression is used, no voice packets are sent over the network if there is no sound.

Otherwise, even packets that contain silence are sent. This situation lowers the average required bandwidth for a call. Although it supports silence suppression, the lower bandwidth requirements for silence suppression should not be used when provisioning the network because the worst case scenario would be where there is not silence in the call, requiring the full call bandwidth as if silence suppression was not enabled.

When calculating bandwidth for an IP call, you must use the size of the RTP packet plus the additional overhead of the networking protocols used to transport the RTP data through the network.

For example, G.711 packets carrying 20 ms of speech data require 64 kbps (kilobytes per second) of network bandwidth per stream. These packets are encapsulated by four layers of networking protocols (RTP, UDP, IP, and Ethernet). Each of these protocols adds its own header information to the G.711 data. As a result, the G.711 data, once packed into an Ethernet frame, requires 87.2 kbps of bandwidth per data stream as it travels over the network. Because an IP phone call consists of two voice streams, in this example, a call would require 174.4 kbps.

The amount of voice data in a single packet also influences the size of the packet and bandwidth. The example above used packets containing 20 milliseconds of speech for its calculations, but this value can be changed in the Unified CM configuration for each supported Codec. Configuring packets to contain more speech information reduces the number of packets sent over the network and reduces the bandwidth because there are fewer packets containing the additional networking headers, but the packet sizes increase.

The following table shows the bandwidth required for a phone call for the different combinations of Codec and amount of speech per packet.

Table 26: Per-call Packet Size Bandwidth Requirements

Codec	Milliseconds of speech per packet	Bandwidth required (Kbps) for a call
G.711	10	220.8
G.711	20	174.4
G.711	30	159.0
G.729	10	108.8
G.729	20	62.4
G.729	30	47.0
G.729	40	39.2
G.729	50	34.6
G.729	60	31.4

Note

- The calculations are based on G.711 using a sampling rate of 64 kbps speech encoding and the G.729 using 8 kbps. This means one second of speech encoded into the G.711 Codec requires 65,536 bits (or 8,192 bytes) to represent one second of sound.
- For full-duplex connections, the bandwidth speed applies to both incoming and outgoing traffic. (For instance, for a 100-Mbps connection, there is 100 Mbps of upload bandwidth and 100 Mbps of download bandwidth.) Therefore, an IP phone call consumes the bandwidth equivalent of a single stream of data. In this scenario, a G.711 IP phone call with no silence suppression and containing 20 milliseconds of speech per packet requires 87.2 kbps (174.4 / 2) of the available bandwidth.
- Unified CCX supports a-law and μ-law for G.711.

Bandwidth Available for Monitoring and Recording

The following tables display the percentage of total bandwidth available, based on the network connection, which is required for simultaneous monitoring sessions handled by a VoIP provider.

Table 27: Available Upload Bandwidth Percentage for Simultaneous Monitoring Sessions with G.729 Codec

Number of Simultaneous Monitoring Sessions	Percentage of Available Bandwidth Required (No Silence Suppression)							
	100 Mbps	10 Mbps	1.544 Mbps	640 kbps	256 kbps	128 kbps	64 kbps	56 kbps
Call only	0.1	0.9	5.6	13.6	34.1	68.1	Not supported (NS)[5]	
1	0.3	2.6	16.8	40.9	NS	NS	NS	NS
2	0.4	4.4	28.1	68.1	NS	NS	NS	NS

Number of Simultaneous Monitoring Sessions	Percentage of Available Bandwidth Required (No Silence Suppression)							
	100 Mbps	10 Mbps	1.544 Mbps	640 kbps	256 kbps	128 kbps	64 kbps	56 kbps
3	0.6	6.1	39.3	95.4	NS	NS	NS	NS
4	0.8	7.8	50.5	NS	NS	NS	NS	NS
5	1.0	9.6	61.7	NS	NS	NS	NS	NS
6	1.1	11.3	72.9	NS	NS	NS	NS	NS
7	1.3	13.1	84.2	NS	NS	NS	NS	NS
8	1.5	14.8	95.4	NS	NS	NS	NS	NS
9	1.7	16.6	NS	NS	NS	NS	NS	NS
10	1.8	18.3	NS	NS	NS	NS	NS	NS

[5] The bandwidth of the connection is not large enough to support the number of simultaneous monitoring sessions.

Table 28: Available Upload Bandwidth Percentage for Simultaneous Monitoring Sessions with G.711 Codec

Number of Simultaneous Monitoring Sessions	Percentage of Available Bandwidth Required (No Silence Suppression)						
	100 Mbps	10 Mbps	1.544 Mbps	640 kbps	256 kbps	128 kbps	64 kbps
Call only	0.0	0.3	2.0	4.9	12.2	24.4	48.8
1	0.1	0.9	6.0	14.6	36.6	73.1	Not supported (NS)[6]
2	0.2	1.6	10.0	24.4	60.9	NS	NS
3	0.2	2.2	14.1	34.1	85.3	NS	NS
4	0.3	2.8	18.1	43.9	NS	NS	NS
5	0.3	3.4	22.1	53.6	NS	NS	NS
6	0.4	4.1	26.1	63.4	NS	NS	NS
7	0.5	4.7	30.1	73.1	NS	NS	NS
8	0.5	5.3	34.1	82.9	NS	NS	NS
9	0.6	5.9	38.1	92.6	NS	NS	NS
10	0.7	6.6	42.2	NS	NS	NS	NS

[6] The bandwidth of the connection is not large enough to support the number of simultaneous monitoring sessions.

The following notes apply to the bandwidth requirements shown in the previous tables:

- The bandwidth values are calculated based on the best speed of the indicated connections. A connection's true speed can differ from the maximum stated due to various factors.
- The bandwidth requirements are based on upload speed. Download speed affects only the incoming stream for the IP phone call.
- The values are based upon each voice packet containing 20 milliseconds of speech.
- The number of bytes in each packet include the entire Ethernet encapsulation.
- The data represents the Codecs without silence suppression. With silence suppression, the amount of bandwidth used may be lower.
- The data shown does not address the quality of the speech of the monitored call. If the bandwidth requirements approach the total bandwidth available and other applications must share access to the network, latency (packet delay) of the voice packets can affect the quality of the monitored speech. However, latency does not affect the quality of recorded speech.
- The data represents only the bandwidth required for monitoring and recording. It does not include the bandwidth requirements for Cisco Finesse.

Web Chat Feature

When deploying the Unified CCX along with Cisco Customer Collaboration Platform, observe the following network requirements:

Delay—The maximum allowed round-trip time (RTT) between the Unified CCX server and Customer Collaboration Platform is 150 ms.

Bandwidth—In addition to the requirements for the Unified CCX and Unified CM clusters, provision sufficient bandwidth for Customer Collaboration Platform, the customer web server, and remote agent or supervisor desktops to deploy Web Chat successfully.

Consider the bandwidth required for the following components:

- **Unified CCX and Customer Collaboration Platform**—If Customer Collaboration Platform and the Unified CCX are not co-located, there is an additional bandwidth requirement for the communication and contact signaling.
- **Customer Collaboration Platform and Cisco Finesse Agent Desktop**—When a chat session starts, depending on the chat transcript size and communication frequency, there is an additional bandwidth requirement between Customer Collaboration Platform and the Cisco Finesse Agent Desktop.
- **Customer Collaboration Platform and Customer Website**—The customer website transfers all new chat contact requests to Customer Collaboration Platform. When a chat contact request reaches Customer Collaboration Platform, an active chat session is maintained by Customer Collaboration Platform to carry chat messages between Customer Collaboration Platform and the browser. After the chat contact request is transferred to Customer Collaboration Platform, the customer website server is no longer a part of the active chat session.

The following table shows the minimum bandwidth requirement for the Unified CCX and Customer Collaboration Platform when they are not located in the same network.

Note These numbers depend on overall network efficiency.

	Between Unified CCX and CCP(KBps)	Between Unified CCX and Agent Desktop (KBps)	Between CCP and Agent Desktop (KBps)	Between Customer Web Server and CCP (KBps)
Actual data bandwidth	3.35 [1]	4.02 [2]	12 [3]	12 [3]
Data bandwidth considering HTTP traffic and other factors	40	40	100	100

[1] Allocate network bandwidth for signal communication based on this formula:

Signaling network bandwidth (in KBps) = Number of new chat sessions per second × Number of messages per chat session × Average message size

Agent Email Feature

When you deploy Unified CCX along with Cisco Customer Collaboration Platform, observe the following network requirements:

Delay—The maximum allowed round-trip time (RTT) between the Unified CCX server and Customer Collaboration Platform is 150 ms.

Bandwidth—In addition to the requirements for the Unified CCX and Unified Communications Manager clusters, you must provision sufficient bandwidth for Customer Collaboration Platform, the mail server, and remote agent/supervisor desktops to deploy Agent Email successfully.

The following table shows the minimum bandwidth requirement for Unified CCX and Customer Collaboration Platform when they are not located in the same network.

Note These numbers depend on overall network efficiency.

	Between Unified CCX and CCP (KBps)
Actual data bandwidth	0.67 [1]
Data bandwidth considering HTTP traffic and other factors	40

[1] Allocate network bandwidth for signal communication based on this formula:

Signaling network bandwidth (in KBps) = Number of new email sessions per second × Number of messages per email session × Average message size

Example

If you have 400 emails (maximum supported) per hour, you will have 0.11 email sessions per second. On average, if each email session has six messages for state signaling and contact injection and each message is 1 KB (500 characters), then bandwidth utilization is 0.11 x 6 x 1 KB = 0.67 KBps.

	Between Unified CCX and Agent Desktop (KBps)
Actual data bandwidth	2.22 [2]
Data bandwidth considering HTTP traffic and other factors	40

[2] Allocate network bandwidth for signal communication based on this formula:

Signaling network bandwidth (in KBps) = Number of new email sessions per second × Number of messages per email session × Average message size

Example

If you have 400 emails (maximum supported) per hour and an agent can handle five concurrent emails, you will have 0.11 emails per second. The agent can requeue or respond to that email directly. Assuming on average 10% of email messages are requeued and there are 100 Email CSQs in the system, three messages, each 1 KB, and the requeue list message is 10 KB, the bandwidth requirement is calculated as follows:

network bandwidth (in KBps) = number of concurrent emails x number of new email sessions per second x [(number of messages per email session x average message size) + (percentage of emails requeued x size of requeue list message)]

5 x 0.11 x ((3 x 1 KB) + (0.1 x 10 KB)) = 2.22 KBps

Agent Email Flow

There are four types of Agent Email flows that exist between the Agent Desktop, Customer Collaboration Platform, and the Exchange Server.

- Basic Email flow—No attachments and no requeue.
- Email with attachments flow—The customer's email contains attachments and the agent's reply has attachments.
- Email requeue flow—The customer's email is sent to another queue.
- Email requeue with attachments flow—The customer's email contains attachments. The email is requeued and the agent's reply contains attachments.

The flows listed above represent the extreme cases which makes the calculations conservative.

Requeues and attachments are expected to occur 10% of the time. The maximum number of emails per hour is 400. The occurrence of each type of flow is determined by first calculating the number of basic and requeue flows followed by the number of basic and requeue flows that contain attachments:

- Total basic email flow = Maximum email per hour – [maximum email per hour x (requeue percent / 100)]
  - Email with attachments flow = total basic email flow x (attachment percent / 100)
  - Basic email flow = total basic email flow – email with attachments flow
- Total email requeue flow = Maximum email per hour x (requeue percent / 100)

- Email requeue with attachments flow = total email requeue flow x (attachment percent / 100)
- Email requeue flow = total email requeue flow – email requeue with attachments flow

After considering the maximum values, the calculation is:

- Total basic email flow = 360
  - Email with attachments flow = 36
  - Basic email flow = 324
- Total email requeue flow = 40
  - Email requeue with attachments flow = 4
  - Email requeue flow = 36

Each of the flows has a set of messages with different bandwidth requirements. The requirements are derived based on the following constants:

- Customer email size = 6 KB
- Attachment size = 5120 KB
- Agent reply size = 6 KB
- SLA = 60 minutes
- Save draft interval = 3 minutes

Agent Email Routing Configuration

Emails are fetched on every polling interval configured by the administrator. A snapshot age (in minutes) is defined by the administrator. Based on this configuration, Customer Collaboration Platform determines the oldest email to be fetched and emails are fetched in the oldest first order from the mail server and then injected to the Unified CCX engine. Later, the Unified CCX engine presents the emails to the agent.

In the event of any disruption (Customer Collaboration Platform or Unified CCX engine or network connectivity between Unified CCX and Customer Collaboration Platform goes down and comes back), Customer Collaboration Platform re-injects the email contacts to Unified CCX in the oldest first order.

Agent Desktop and Customer Collaboration Platform

If Customer Collaboration Platform and Unified CCX are not co-located, additional bandwidth is required for communication and contact signaling.

	Between Agent Desktop and CCP
Actual data bandwidth	3560160 KB per hour
Data bandwidth considering HTTP traffic and other factors	1024 KBps

Customer Collaboration Platformand Mail Server

Customer Collaboration Platform must retrieve emails, save drafts, and send emails from the Agent Desktop to the mail server. If the mail server is not on the same network as Customer Collaboration Platform, you must ensure that the bandwidth requirement is based on mean per-session email traffic.

	Between CCP and Mail Server (KBps)
Actual data bandwidth	1516720 KB per hour
Data bandwidth considering HTTP traffic and other factors	512 KBps

- Ensure maximum RTT between Customer Collaboration Platformand Office 365 SMTP and IMAP hosts are within 100 ms (including network traversals via SOCKS5 proxy if applicable).
- Follow the considerations for provisioning Office 365 accounts geographically based on information provided by Microsoft support.
- Gmail requires SOCKS proxy configuration if Customer Collaboration Platform is deployed in a non-DMZ setup. There is no direct access to Internet or Gmail Server.
- Emails operations are slower with Gmail when compared to Microsoft Exchange as it is hosted over Cloud.
- The maximum size of attachment allowed in an email is dependent on the bandwidth provisioned between the following:
  - Agent desktop to Unified CCX and Customer Collaboration Platform
  - Email Server to Customer Collaboration Platform

  The minimum assured bandwidth required can be calculated using the Unified CCX Bandwidth Calculator.

QoS and Call Admission Control

Quality of service (QoS) becomes an issue when more voice and application-related traffic is added to an already growing amount of data traffic on your network. Accordingly, Unified CCX and time-sensitive traffic such as voice need higher QoS guarantees than less time-sensitive traffic such as file transfers or emails (particularly if you are using a converged network).

QoS should be used to assign different qualities to data streams to preserve Unified CCX mission-critical and voice traffic. The following are some examples of available QoS mechanisms:

- Packet classification and usage policies applied at the edge of the network, such as Policy Based Routing (PBR) and Committed Access Rate (CAR).
- End-to-end queuing mechanisms, such as Low Latency Queuing (LLQ). Because voice is susceptible to increased latency and jitter on low-speed links, Link Fragmentation and Interleaving (LFI) can also be used to reduce delay and jitter by subdividing large datagrams and interleaving low-delay traffic with the resulting smaller packets.
- Scheduling mechanisms such as Traffic Shaping to optimize bandwidth utilization on output links.

Unified CCX and Application-Related Traffic

The table lists TCP ports and DSCP markings for use in prioritizing Unified CCX and Unified CM mission-critical CTI traffic. The DSCP markings for call signaling traffic between Unified CCX and Cisco Unified Communication Manager and for voice traffic played from the Unified CCX server are set by default according to the traffic classification guidelines documented in *Cisco Unified Communications System Design Guidance*, available here:

http://www.cisco.com/go/ucsrnd.

Unified CCX does not mark any network traffic other than those mentioned here. As a result, traffic should be marked and prioritized at the edge according to the values in the table.

The performance criteria used in classifying this traffic includes:

- No packet drops on the outbound or inbound interface of the WAN edge router
- Voice (G.729) loss under 1percent
- One-way voice delay under 150 ms

A detailed description of QoS is not within the scope of this design guide. For QoS design considerations, refer to the quality of service design guide available here:

http://www.cisco.com/go/designzone

Table 29: QoS Classifications for Unified CCX Interfaces

Unified CCX Component	Interface / Protocol	Port	DSCP Marking
Unified CCX Engine — CTI-QBE messaging destined to Unified CM from Unified CCX	CTI-QBE	TCP 2748	CS3
Unified CCX Administration and BIPPA Service — HTTP traffic destined for web administration and BIPPA interface on Unified CCX	HTTP / HTTPS	TCP 8443	AF21
Unified CCX Engine and Unified CCX Administration — SOAP AXL HTTPS messaging destined to Unified CM from Unified CCX	HTTPS / SOAP	TCP 8443	AF21
Unified CCX Engine — CTI messaging destined to Unified CCX from CAD clients	CTI	TCP 12028	CS3
Unified CCX Engine — RTP voice bearer traffic (bi-directional)	RTP	UDP 16384 - 32767	EF

CAC and RSVP

Unified CM supports Resource-Reservation Protocol (RSVP) between endpoints within a cluster. RSVP is a protocol used for Call Admission Control (CAC) and is used by the routers in the network to reserve bandwidth for calls. The bandwidth being controlled is only for the voice streams, call signalling traffic is not part of CAC.

Before RSVP, each Unified CM cluster maintained its own calculation of how many active calls were traversing between locations in order to calculate bandwidth usage. If more than one Unified CM cluster shared the same link, bandwidth would have to be carved out and dedicated for each cluster, and this led to inefficient use of available bandwidth. RSVP also enables customers to deploy complex network topology while location-based CAC is limited to a hub-and-spoke type of topology.

RSVP solves this problem by tracing the path between two RSVP Agents that reside on the same LAN as the IP Phones. A software MTP or transcoder resource that runs on Cisco IOS routers can be RSVP Agents. The RSVP Agents are controlled by Unified CM and are inserted into the media stream between the two IP phones when a call is made. The RSVP Agent of the originating IP Phone will traverse the network to the destination IP Phone's RSVP Agent, and reserve bandwidth. Since the network routers (and not Unified CM) are keeping track of bandwidth usage, multiple phone calls can traverse the same RSVP controlled link even if the calls are controlled by multiple Unified CMs.

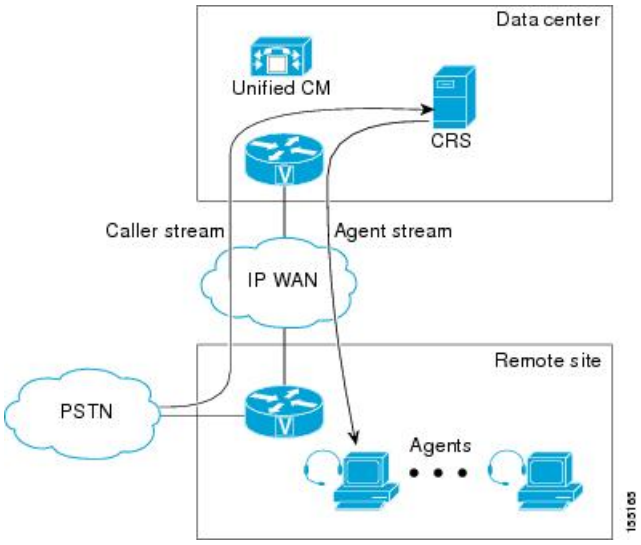
For more information, see the RSVP chapter in *Cisco Unified Communications Solution Reference Network Design (SRND).*

Unified CCX selects a call center agent independent of the mechanism, using either RSVP or location-based CAC. Unified CCX routes a call to an available agent even though the agent phone might not be able to receive the call due to lack of bandwidth. Proper sizing of bandwidth between sites is very important.

For any call transfer, there are moments when two calls are active. If any of the active calls traverses between sites, then CAC is used. Even when the original call is placed on hold during a transfer, that call still takes up the same amount of bandwidth just like an active call.

In the two examples that follow, the voice gateway and agents are at a remote site, while the Unified CCX server is at another site. A call from PSTN reaches the voice gateway at the remote site and connects to Unified CCX at the site. This takes one call bandwidth over the WAN link, which is represented by the caller stream. Once an agent is available and selected at the remote site, Unified CCX transfers the call to the agent.

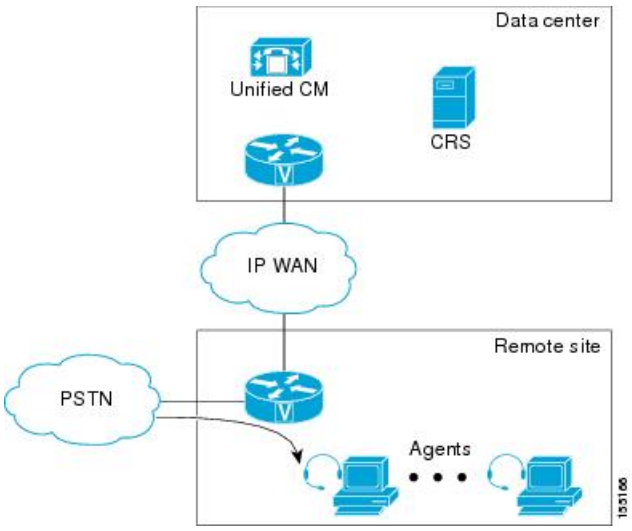
Figure 21: Call From PSTN to Unified CCX Server to Agent



During the transfer, before the agent picks up the call, there is another call setup between Unified CCX and the agent phone. It takes up another call bandwidth over the WAN, and is represented by the agent stream in the previous example. Once the agent picks up the call, the voice traffic is between the voice gateway and the agent phone, which are both at the remote site. At that time, no bandwidth is reserved over the WAN, as illustrated in the following example. This example shows how call bandwidth is reserved in a contact center

call that is eventually routed to an agent. Depending on where the voice gateway, the agents, and the Unified CCX server are located, proper WAN bandwidth should be provisioned.

Figure 22: After Agent Picks Up Call



Bandwidth, Latency, and QoS for Cisco Finesse

Bandwidth requirement for Cisco Finesse client to server

The agent and supervisor login operation involves loading web pages, 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.

As Cisco Finesse is a web application, caching can significantly impact the required bandwidth. To minimize the amount of bandwidth required for login, make sure that caching is enabled in the browser.

To help you with the bandwidth calculation, Cisco Unified CCX provides a bandwidth calculator (Cisco Unified CCX Bandwidth Calculator) to estimate the bandwidth required to accommodate the client login time.

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

The bandwidth listed in the bandwidth calculator must be available for Cisco Finesse after you account for the bandwidth used by other applications, including voice traffic that may share this bandwidth. The performance of the Cisco Finesse interface, and potentially the quality of voice sharing this bandwidth, may degrade if sufficient bandwidth is not continuously available.

Cisco Finesse Desktop Latency

Cisco Finesse Agent and Supervisor Desktops can be located remotely from Unified CCX. The round-trip time between the Unified CCX server and the agent desktop must not exceed 400 ms.

QoS for Cisco Finesse

Cisco Finesse does not support configuration of QoS settings in network traffic. Generally, have the QoS classification and marking of traffic done at the switch or router level. You can prioritize signaling traffic there, especially for agents who are across a WAN.

Bandwidth, Latency, and QoS for Unified Intelligence Center

The two bandwidth considerations in a Unified Intelligence Center installation include the following:

- Bandwidth between the Unified Intelligence Center and data source
- Bandwidth between the user and Unified Intelligence Center

The Unified CCX database is local to the server. In the usual operating mode, the bandwidth between Unified Intelligence Center and the data source can be ignored.

Note Each report requires about 2.6 Mbps of bandwidth between the user and Unified Intelligence Center.

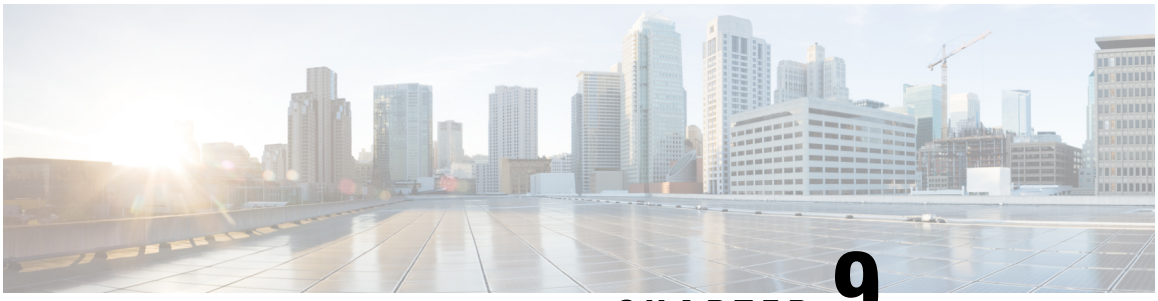
The configuration parameters that affect bandwidth include the following:

- Size of each row: 500 bytes
- HTML size overhead for each row: 500 bytes
- Time to transfer the rendered report from Unified Intelligence Center to the browser: 3 seconds

Reporting Scaling Considerations

Following are the reporting considerations:

- A maximum of eight reporting users logged in concurrently on Cisco Unified Intelligence Center can view:
  - Four Live Data reports with 50 rows of 10 fields refreshing every 3 seconds.
  - Two historical reports with 2000 rows with 10 fields each refreshing every 30 minutes.
- A maximum of 42 Finesse supervisors can view:
  - Three Live Data reports with 50 rows of 10 fields refreshing every 3 seconds.
- A maximum of 358 Finesse agents can view:
  - Three real-time reports with 20 rows of 10 fields refreshing every 3 seconds.



CHAPTER 9

Sizing Operating Conditions for Reference Design

- Contact Center Basic Traffic Terminology, on page 131
- Operating Considerations for Reference Design Compliant Solutions, on page 138

Contact Center Basic Traffic Terminology

It is important to be familiar with, and to be consistent in the use of, common contact center terminology. Improper use of these terms in the tools used to size contact center resources can lead to inaccurate sizing results.

The terms listed in this section are the most common terms used in the industry for sizing contact center resources. There are also other resources available on the internet for defining contact center terms.

Busy Hour or Busy Interval

A busy interval can be one hour or less (such as 30 minutes or 15 minutes, if sizing is desired for such smaller intervals). The busy interval occurs when the most traffic is offered during this period of the day. The busy hour or interval varies over days, weeks, and months. There are weekly busy hours and seasonal busy hours. There is one busiest hour in the year. Common practice is to design for the average busy hour (the average of the 10 busiest hours in one year). This average is not always applied, however, when staffing is required to accommodate a marketing campaign or a seasonal busy hour such as an annual holiday peak. In a contact center, staffing for the maximum number of agents is determined using peak periods, but staffing requirements for the rest of the day are calculated separately for each period (usually every hour) for proper scheduling of agents to answer calls versus scheduling agents for offline activities such as training or coaching. For trunks in most cases it is not practical to add or remove trunks or ports daily, so these resources are sized for the peak periods. In some retail environments, additional trunks can be added during the peak season and disconnected afterwards.

Busy Hour Call Attempts (BHCA)

The BHCA is the total number of calls during the peak traffic hour (or interval) that are attempted or received in the contact center. For the sake of simplicity, we assume that all calls offered to the Voice Gateway are received and serviced by the contact center resources. Calls generally originate from the PSTN, although calls to a contact center can also be generated internally, such as by a help-desk application.

Calls Per Second as reported by Call Router (CPS)

These are the number of call routing requests received by the Unified CCX Call Router per second. Every call will generate one call routing request in a simple call flow where the call comes in from an ingress gateway and is then sent to an Agent; however, there are conditions under which a single call will need more than one routing request to be made to the Unified CCX Call Router to finally get to the right agent.

Servers

Servers are resources that handle traffic loads or calls. There are many types of servers in a contact center, such as PSTN trunks and gateway ports, agents, and voicemail ports.

Talk Time

Talk time is the amount of time an agent spends talking to a caller, including the time an agent places a caller on hold and the time spent during consultative conferences.

Wrap-Up Time (After-Call Work Time)

After the call is terminated (the caller finishes talking to an agent and ends the call), the wrap-up time is the time it takes an agent to wrap up the call by performing such tasks as updating a database, recording notes from the call, or any other activity performed until an agent becomes available to answer another call.

Average Handle Time (AHT)

AHT is the mean (or average) call duration during a specified time period. It is a commonly used term that refers to the sum of several types of handling time, such as call treatment time, talk time, and queuing time. In its most common definition, AHT is the sum of agent talk time and agent wrap-up time.

Erlang

Erlang is a measurement of traffic load during the busy hour. The Erlang is based on having 3600 seconds (60 minutes, or 1 hour) of calls on the same circuit, trunk, or port. (One circuit is busy for one hour regardless of the number of calls or how long the average call lasts.) If a contact center receives 30 calls in the busy hour and each call lasts for six minutes, this equates to 180 minutes of traffic in the busy hour, or 3 Erlangs (180 min/60 min). If the contact center receives 100 calls averaging 36 seconds each in the busy hour, then total traffic received is 3600 seconds, or 1 Erlang (3600 sec/3600 sec).

Use the following formula to calculate the Erlang value:

Traffic in Erlangs = (Number of calls in the busy hour * AHT in sec) / 3600 sec

The term is named after the Danish telephone engineer A. K. Erlang, the originator of queuing theory used in traffic engineering.

Busy Hour Traffic (BHT) in Erlangs

BHT is the traffic load during the busy hour and is calculated as the product of the BHCA and the AHT normalized to one hour:

BHT = (BHCA * AHT seconds) / 3600, or
BHT = (BHCA * AHT minutes) / 60

For example, if the contact center receives 600 calls in the busy hour, averaging 2 minutes each, then the busy hour traffic load is (600 * 2/60) = 20 Erlangs.

BHT is typically used in Erlang-B models to calculate resources such as PSTN trunks. Some calculators perform this calculation transparently using the BHCA and AHT for ease of use and convenience.

Grade of Service (Percent Blockage)

This measurement is the probability that a resource or server is busy during the busy hour. All resources might be occupied when a user places a call. In that case, the call is lost or blocked. This blockage typically applies to resources such as Voice Gateway ports, PBX lines, and trunks. In the case of a Voice Gateway, grade of service is the percentage of calls that are blocked or that receive busy tone (no trunks available) out of the total BHCA. For example, a grade of service of 0.01 means that 1% of calls in the busy hour is blocked. A 1% blockage is a typical value to use for PSTN trunks, but different applications might require different grades of service.

Blocked Calls

A blocked call is a call that is not serviced immediately. Callers are considered blocked if they are rerouted to another route, if they are delayed and put in a queue, or if they hear a tone (such as a busy tone) or announcement. The nature of the blocked call determines the model used for sizing the particular resources.

Service Level

This term is a standard in the contact center industry, and it refers to the percentage of the offered call volume (received from the Voice Gateway and other sources) that are answered within x seconds, where x is a variable. A typical value for a sales contact center is 90% of all calls answered in less than 10 seconds (some calls are delayed in a queue). A support-oriented contact center might have a different service level goal, such as 80% of all calls answered within 30 seconds in the busy hour. Your contact center's service level goal determines the number of agents needed, the percentage of calls that are queued, the average time calls spend in queue, and the number of PSTN trunks needed.

Queuing

When agents are busy with other callers or are unavailable (after call wrap-up mode), subsequent callers must be placed in a queue until an agent becomes available. The percentage of calls queued and the average time spent in the queue are determined by the service level desired and by agent staffing. Cisco's Unified CCX solution uses a IVR to place callers in queue and play announcements. It can also be used to handle all calls initially (call treatment, prompt and collect such as DTMF input or account numbers or any other information gathering) and for self-service applications where the caller is serviced without needing to talk to an agent (such as obtaining a bank account balance, airline arrival/departure times, and so forth). Each of these scenarios requires a different number of IVR ports to handle the different applications because each has a different average handle time and possibly a different call load.

Server Capacities and Limits

OVA Profile

The following table displays Open Virtualization Alliance (OVA) configuration settings to be used for Unified CCX:

Note From Release 12.5(1), 300 Agent profile is not supported. Existing customers must upgrade to 400 Agent profile and make necessary memory enhancement.

Table 30: OVA Settings

Agent Capacity	vCPU	vRAM	vDisk
100 agents	2	10 GB-Without Cloud Services 14 GB-With Cloud Services	1 x 146GB
400 agents	4	20 GB	2 x 146GB

The following table provides a selected list of capacity limits when deploying Unified CCX.

Table 31: Capacity Limits

Deployment	Capacity
Maximum number of teams	8 **Note** This maximum of eight teams is mentioned considering that each team has five supervisors. However, more teams can be created if the number of supervisors are less for each team. **For example**: If one team is assigned with one supervisor, you can have a maximum of 40 teams.
Maximum number of supervisors in a team	5
Maximum number of inbound agents	400
Maximum number of preview outbound agents	150
Maximum number of remote agents	100
Maximum number of concurrent supervisors	42
Maximum number of teams that a supervisor can be assigned	5
Maximum number of agents in a team	50
Maximum number of IVR ports	400
Maximum number of outbound IVR ports	150
Maximum number of progressive and predictive outbound agents	150
Maximum number of team messages that can be created or deleted per hour	100
Maximum number of active team messages	1600

Deployment	Capacity
Maximum number of contacts in an outbound campaign	100 thousand
Maximum number of contacts that can be imported at a time in an outbound campaign	20,000

This table shows absolute limits. Reaching the limits for multiple criteria in a specific configuration might not be possible. Use the Cisco Unified Communications Sizing Tool to validate your configuration. This tool is available at:

http://tools.cisco.com/cucst

The Cisco Unified Communications Sizing Tool is available to Cisco partners only. For more details and to validate your configuration, contact your Cisco sales engineer or Cisco partner to access this tool.

For information on capacity and sizing of Cisco Workforce Optimization, refer to the *Cisco Workforce Optimization System Configuration Guide*.

The summary overview of system maximums for inbound and outbound voice that are listed in the table is for reference only.

Table 32: Reference Capacities for Inbound Deployment

Inbound-Only Deployment- Maximum Capacities				
	Standalone Server		**Two-Server Cluster**	
OVA profile	3	1	3	1
Agents	400	100	400	100
Supervisors	42	10	42	10
Chat volume per hour	2400[7]	1200 [8]	2400 [9]	1200 [10]
Silent Monitoring	42	10	42	10
Recording and Playback using Finesse	The recording limit is based on the number of recording licenses deployed on Unified CCX.			
Contact Service Queue (CSQ)	250	35	250	35
Skills	250	250	250	250
Historical reporting sessions	8	3	16	10
IVR ports[11]	400	100	400	100
ASR ports	100	50	100	50
TTS ports	160	40	160	40
VoiceXML ports	80	40	80	40
Busy Hour Call Completions (BHCC)	6000	2000	6000	2000

Inbound-Only Deployment- Maximum Capacities				
Number of CSQs with which an agent can associate (includes total combined email CSQs and voice CSQs)	25	25	25	25
Number of skills with which a CSQ can associate	50	50	50	50
Number of CSQs for which a call can queue	25	25	25	25
Number of agents per team	50	50	50	50

[7] Large profile of Customer Collaboration Platform is supported.
[8] Small profile of Customer Collaboration Platform is supported.
[9] Large profile of Customer Collaboration Platform is supported.
[10] Small profile of Customer Collaboration Platform is supported.
[11] The number of IVR ports is also limited by the maximum number supported for a given server platform. In case of virtualized deployment, the maximum number of IVR ports is limited by the maximum number supported for a given virtual machine template.

Table 33: Reference Capacities for Email Deployment

	Standalone Server		Two-Server Cluster	
OVA Profile	3	1	3	1
Total Agents	400	100	400	100
Agents assigned to handle Emails	120	60	120	60
Email volume per hour (MS Exchange) with Small Attachments[12]	400	100	400	100
Email volume per hour (Office 365 or Gmail) with Small Attachments[13]	300	75	300	75
Email volume per hour (MS Exchange, Office 365 or Gmail) with Larger Attachments[14]	100	25	100	25
Maximum CSQs for Agent Email	100	100	100	100

[12] (a). Maximum size of each attachment is less than 2 MB. (b). Maximum size of combined attachments in an email sent is 5 MB and 10 MB in a received email. (c). Maximum number of attachments in an email is 10.
[13] (a). Maximum size of each attachment is less than 2 MB. (b). Maximum size of combined attachments in an email sent is 5 MB and 10 MB in a received email. (c). Maximum number of attachments in an email is 10.
[14] (a). Maximum size of each attachment can range between 2-10 MB. (b). Maximum size of combined attachments in an email can range between 10-20 MB. (c). Maximum number of attachments in an email is 10. The limits have been tested and validated for 15% of total Emails with maximum attachment size.

Note The maximum concurrent Chat sessions for any type of OVA profile used must not exceed 120.

The maximum number of emails in the Office 365 inbox folder (folder from which, emails are fetched) must not exceed 100,000.

Table 34: Reference Capacities for Blended Deployments

Blended Deployment- Maximum Capacities				
	Standalone Server		**Two-Server Cluster**	
Agents	400	100	400	100
Supervisors	42	10	42	10
Silent Monitoring	42	10	42	10
Contact Service Queue (CSQ)	250	35	250	35
Skills	250	250	250	250
IVR ports	400	100	400	100
ASR ports	100	50	100	50
TTS ports	160	40	160	40
VoiceXML ports	80	40	80	40
Chat volume per hour	2400 [15]	1200 [16]	2400 [17]	1200 [18]
Blended or Preview Agents	150	75	150	75
Blended or Progressive/Predictive Agents	150	75	150	75
Preview Outbound BHCC	6000	2000	6000	2000
Progressive and Predictive Outbound BHCC	6000	2000	6000	2000
Outbound IVR BHCC	6000	2000	6000	2000
Total BHCC[19]	6000	2000	6000	2000
Number of skills with which an agent can be associated	50	50	50	50
Number of CSQs with which an agent can be associated	25	25	25	25
Number of skills with which a CSQ can be associated	50	50	50	50

Blended Deployment- Maximum Capacities				
Number of CSQs for which a call can be queued	25	25	25	25
Number of email CSQs	100	100	100	100
Outbound IVR ports	150	75	150	75
Maximum number of configured agents	2000	2000	2000	2000

[15] Large profile of Customer Collaboration Platform is supported.
[16] Small profile of Customer Collaboration Platform is supported.
[17] Large profile ofCustomer Collaboration Platform is supported.
[18] Small profile of Customer Collaboration Platform is supported.
[19] For high-availability (HA) deployments, the BHCC listed in the table is for LAN deployments. For WAN deployments, BHCC is 5000 and 750 for OVA profile 3 and 1 respectively. In addition, the BHCC contributed by the preview outbound dialer should not exceed 1000 and 750 for OVA profile 3 and 1 respectively. The BHCC contributed by Outbound IVR should not exceed 1000 for OVA profile 3. These reduced BHCCs apply only to HA over WAN deployments.

Note All the capacities stated in this section are system maximums.

Operating Considerations for Reference Design Compliant Solutions

Time Synchronization

To ensure accurate operation and reporting, all the components in your contact center solution must use the same value for the time. You can synchronize the time across your solution using a Simple Network Time Protocol (SNTP) server. The following table outlines the needs of various component types in your solution.

Important Use the same NTP sources throughout your solution. When you configure the Unified CCX node ensure to point to a Stratum-1, Stratum-2, or Stratum-3 NTP server to ensure that the cluster time is synchronized correctly with an external time source. The NTP information for second node is pulled from the first node.

Type of component	Notes
ESXi hosts	All ESXi hosts must point to the same NTP servers.
Unified CCX components	Components such as Standalone Unified Intelligence Center, Customer Collaboration Platform, and Unified Communications must point to the same NTP servers.

Type of component	Notes
External components used in Unified CCX solution	MS Exchange and any Identity Provider (IdP) that is configured with Unified CCX. To point to Time Synchronized common NTP source as that of CCX components. Follow the Microsoft documentation to synchronize directly with the NTP server.
Cisco Integrated Service Routers	To provide accurate time for logging and debugging, use the same NTP source as the solution for the Cisco IOS Voice Gateways.
Agent Desktop	Agent desktops must be in synchronization with NTP server so that the time in the auto incrementing fields of Live Data reports match the server time.

IPv6 Support

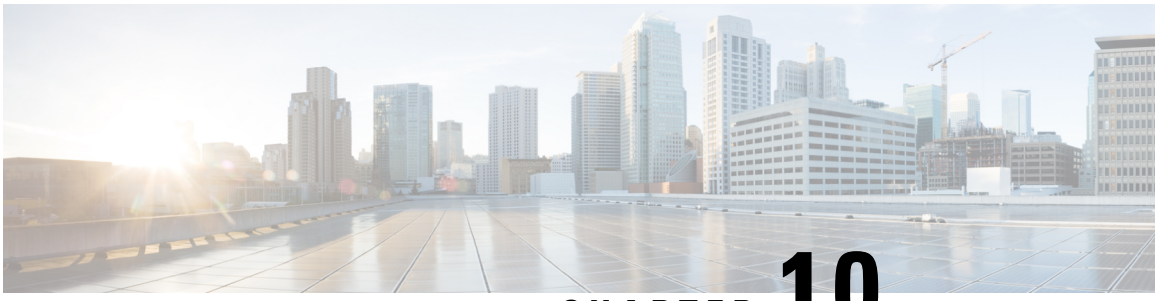
Unified CCX can be deployed as part of a dual stack IPv4 and IPv6 solution. Unified CCX servers and other optional servers (for example, ASR/TTS, WFM, QM etc) should be running in IPv4 segment. However, Unified CM, IP Phones and Gateways can be configured as either IPv4 or IPv6. If the calling device is in IPv6 and the receiving device is in IPv4, Unified CM dynamically inserts a media termination point (MTP) to convert the media between the two devices from IPv4 to IPv6 or vice versa. This would have an impact on Unified CM performance.

For more information on IPv6 deployment with Unified CM, refer to the document *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager* available here:

http://www.cisco.com/go/ucsrnd

SIP Support

Unified CCX CTI ports are notified of caller-entered digits (DTMF input) via JTAPI messages from Unified CM. Unified CCX does not support any mechanism to detect in-band DTMF digits where DTMF digits are sent with voice packets. In deployments with voice gateways or SIP phones that only support in-band DTMF or are configured to use in-band DTMF, an MTP resource must be invoked by Unified CM to convert the in-band DTMF signaling so that Unified CM can notify Unified CCX of the caller-entered digits. Ensure to enable out-of-band DTMF signaling when configuring voice gateways in order to avoid using the previous MTP resources. For detailed design consideration related to DTMF handling, media resources and voice gateway deployments, see the Cisco Unified Communications Solution Reference Network Design at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.



CHAPTER 10

Cisco Webex Experience Management

- Overview, on page 141
- Post-Call Voice Survey Call Flow, on page 142
- SMS or Email Post-Call Survey Call Flow, on page 143

Overview

Cisco Webex Experience Management is a Customer Experience Management (CEM) platform, enabling you to see your business from your customers' perspective and their experience with the brand. Experience Management powers customer journey mapping, text analytics, and predictive modeling using the feedback collected from customers via different channels such as email, SMS and IVR.

Surveys are used to collect feedback from customers to determine the performance of the contact center and the services that are offered. With Experience Management, you can configure post-call surveys that can be initiated over IVR when agents end the calls from Finesse desktop or can be sent to the customer via Email or SMS after the call ends.

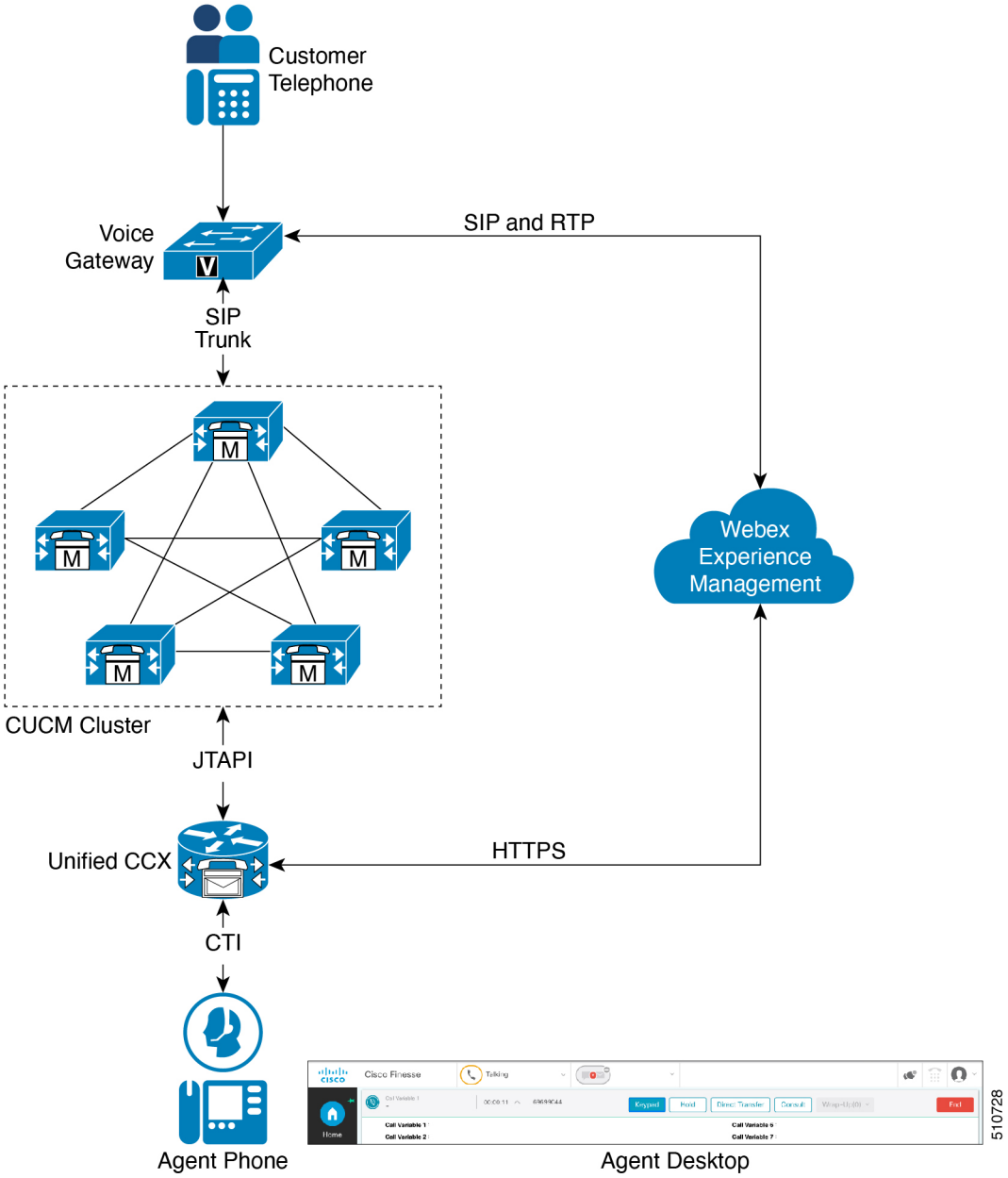
In case of survey over IVR, after an agent ends the call, Unified CCX transfers the call to Experience Management and the survey is played to the customer. Customer uses the keypad to answer the survey.

For survey via email or SMS, Unified CCX can be configured to send out an email or SMS containing a message along with a link to launch the survey and provide feedback.

The data that is collected through various surveys can be analyzed and presented to agents and supervisors as gadgets on the Finesse desktop.

A script (in conjunction with application) enables or disables Experience Management post-call survey on a per-call basis by testing for conditions and setting a session variable that controls triggering of the survey.

Post-Call Voice Survey Call Flow



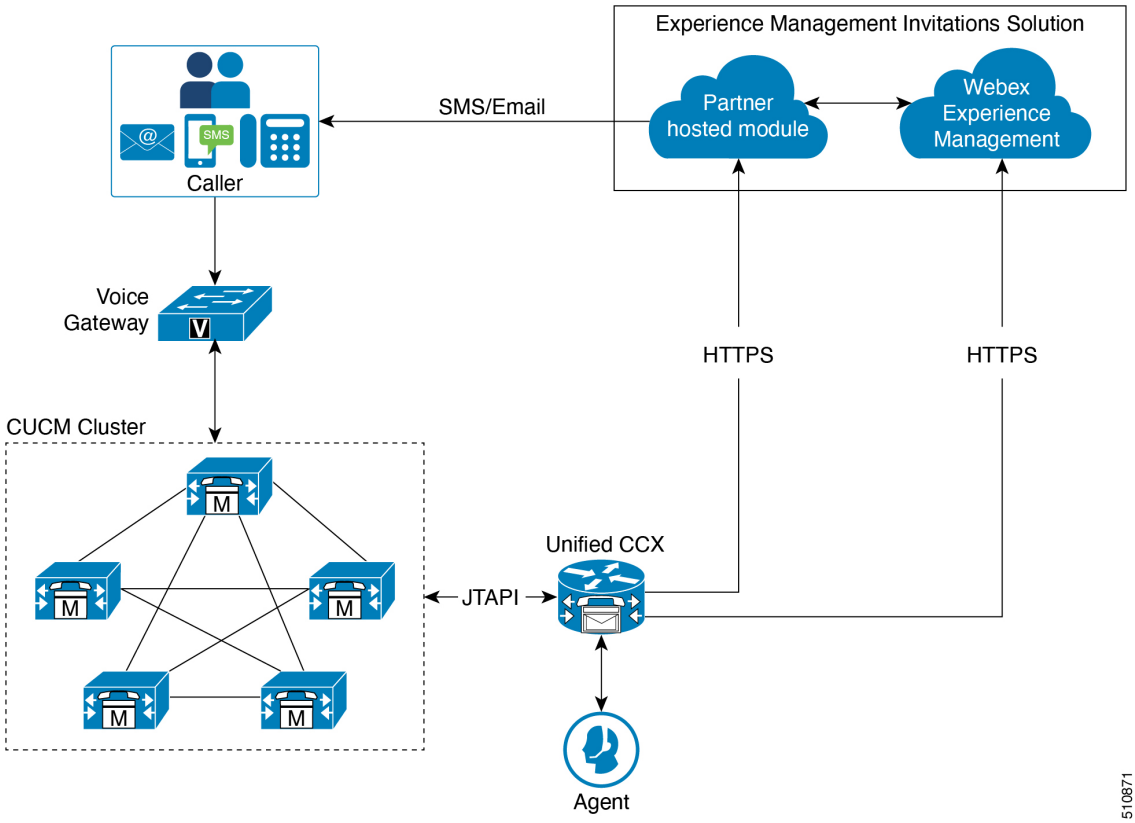
After integrating Experience Management with Unified CCX, the Post-Call Survey Call Flow is as follows:

1. Customer calls the Contact Center route point (Unified CCX application) on which, Experience Management post-call survey is enabled.
2. The call information flows through Voice Gateway, CUCM, and reaches Unified CCX.
3. Unified CCX identifies an agent and call is transferred to the agent.

Note If Experience Management gadgets are configured in Finesse desktop and prior survey data is collected, the earlier feedback from the calling customer is displayed in the Customer Experience Journey gadget.

4. When an agent ends the call from Finesse desktop, Unified CCX sends a secure REST API (https) request to Experience Management to construct a unique SIP URI for the call.
5. Unified CCX informs CUCM to transfer the call to the SIP URI that is constructed.
6. CUCM transfers the call to SIP URI through Voice Gateway and the survey is played to the customer.

SMS or Email Post-Call Survey Call Flow



After integrating Experience Management with Unified CCX, the SMS/Email Post-Call Survey call flow is as follows:

1. Customer calls the Contact Center route point (Unified CCX application) on which, Experience Management post-call survey is enabled.
2. The call information flows through Voice Gateway, CUCM, and reaches Unified CCX.
3. Unified CCX identifies an agent and transfers the call to the agent.

4. Unified CCX adds call details into an in-memory cache.
5. Periodically Unified CCX dispatches all the records accumulated in a dispatch to the partner hosted module of the Experience Management Invitations solution. The Experience Management Invitations solution consists of the partner hosted module along with Experience Management module. For more information about Experience Management Invitations solution, see Experience Management Invitation Architecture
6. The Experience Management Invitations solution sends the SMS/Email survey to the customer based on the configurations set in Experience Management Invitations solution.

Note:

Experience Management also allows handling of Personally Identifiable Information (PII) about a customer in a sensitive manner by avoiding storing PII data on the platform. For more information about how to take advantage of PII, see Experience Management PII.