Contact Center Express Solutions Overview

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:

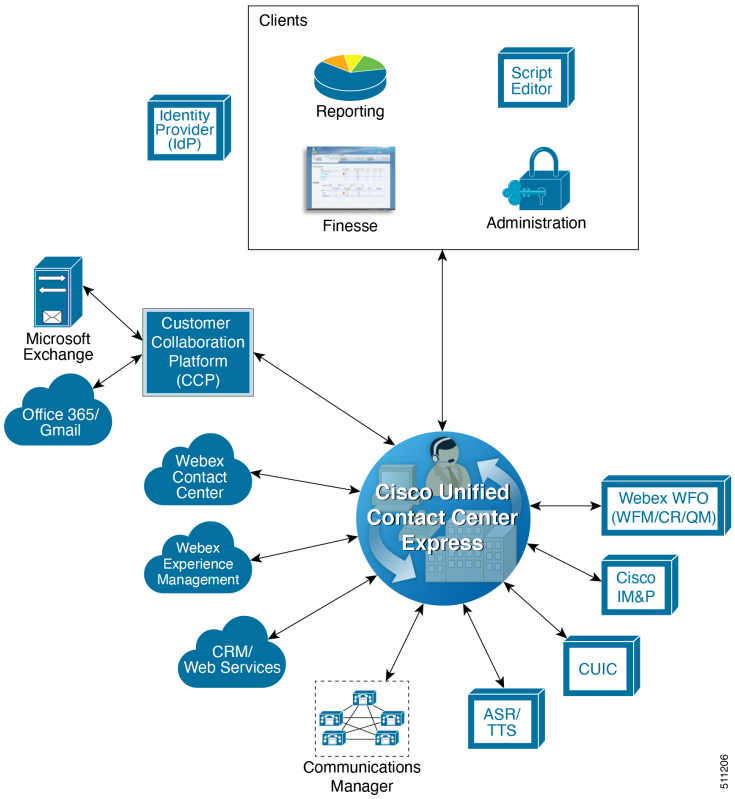
- Historical and Real Time Reporting.
- Browser-based Cisco Finesse Desktops

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 1: 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 1: 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 2: 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 3: 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 4: 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 5: 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 6: 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 7: 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 8: 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 9: 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.

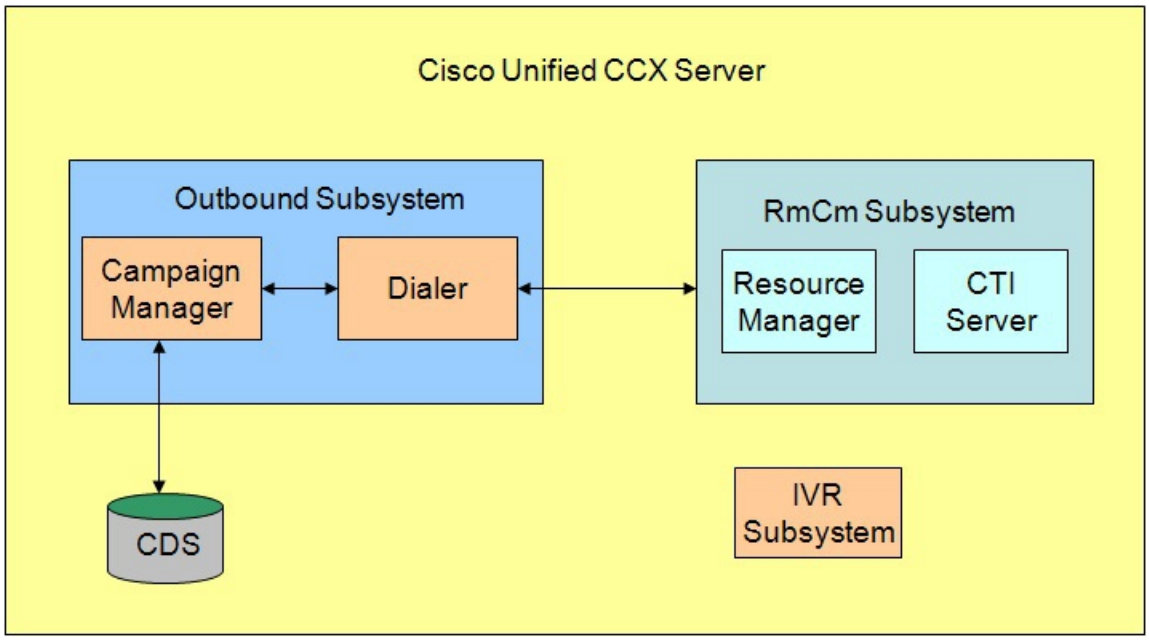
Unified CCX Outbound IVR Dialer allows for Outbound calls to be placed to contacts in a campaign and subsequently for live contacts to be serviced by an IVR application. Call Progress Analysis (CPA) capabilities of the SIP Voice gateway are used to filter non-live contacts (which could be fax and no 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 2: 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 10: 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 11: 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

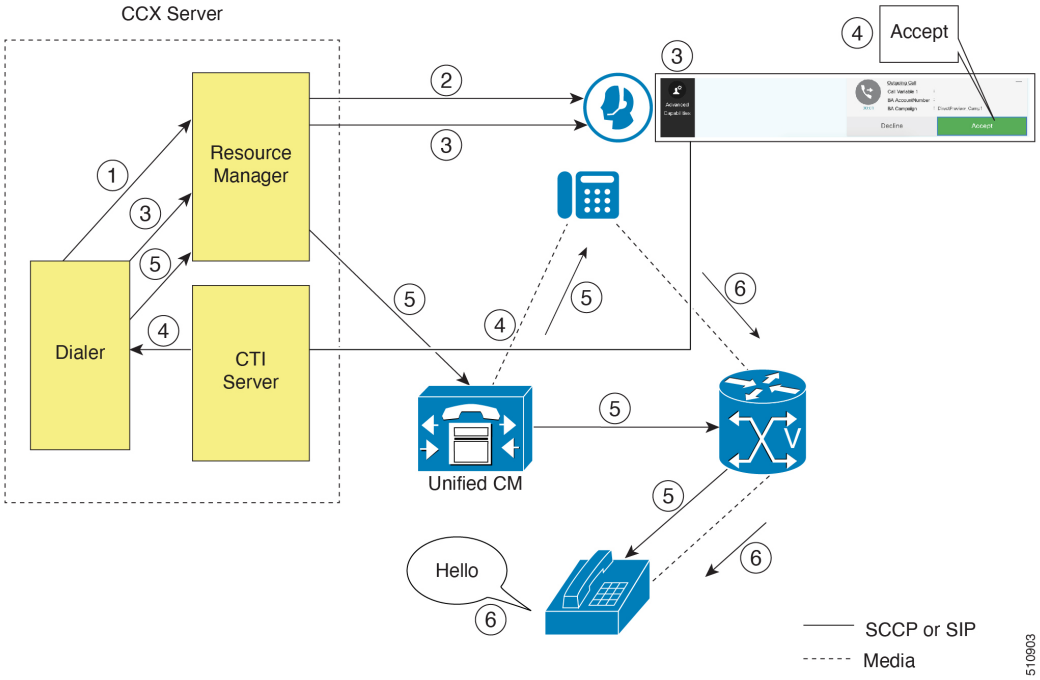
Refer to the "Configuring Unified CCX Dialer" chapter of the *Unified CCX Administration Guide* for details on how the numbers of active IVR ports for inbound and outbound are determined by the above parameters.

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 3: 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.

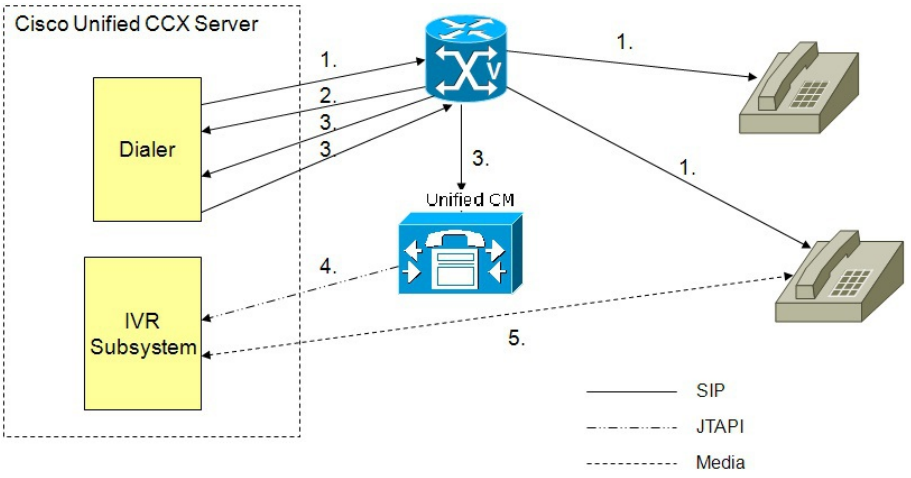
2. The Resource Manager reserves the agent by moving the agent to Reserved state.
3. The Dialer sends a reservation call to the agent desktop and, at the same time, a screen pops that contains the customer information and is presented to the agent. The agent reviews the customer data and decides whether 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 4: 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

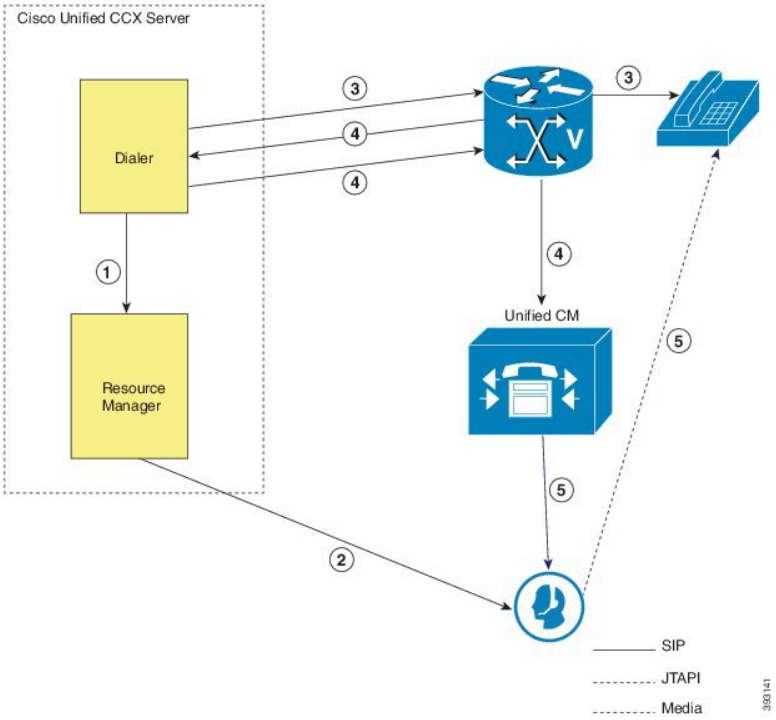
sends a SIP refer message to the SIP gateway which in turn transfers the call to the configured CTI Route Point on Cisco Unified CM.

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 5: 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**

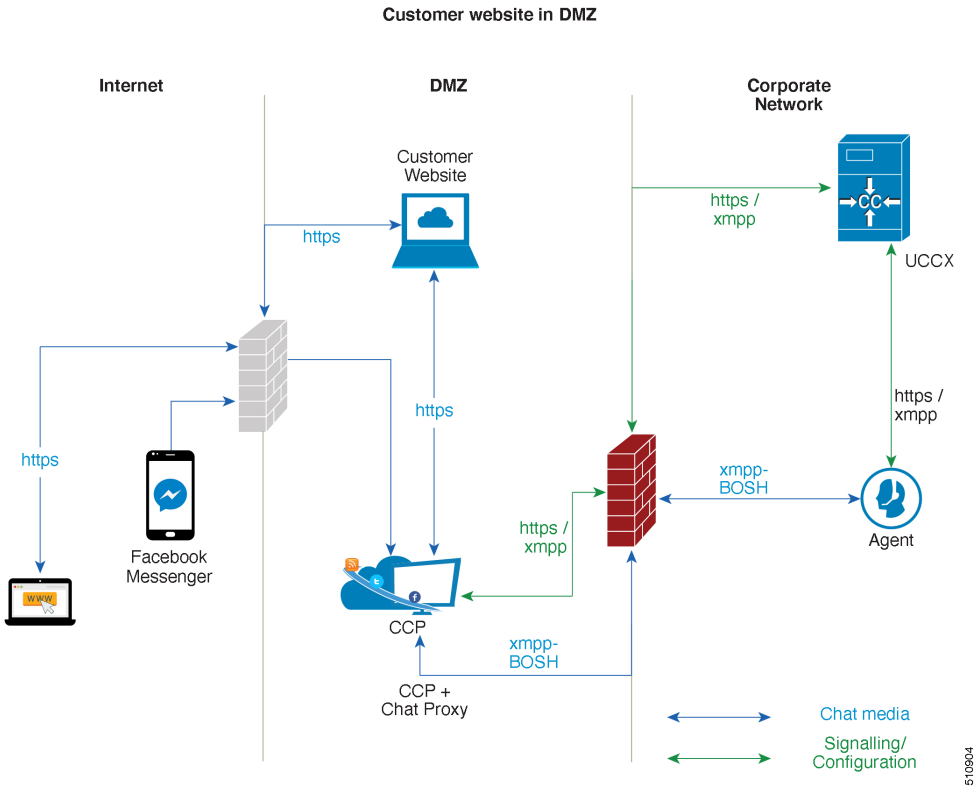
  Unified CCX agents can service customer chat requests using the Web Chat gadget in Cisco Finesse. Customers can initiate a chat session from the organization website. The chat web form is hosted on the organization website that enables the customers to initiate a chat.

- **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 6: Customer Web Site in DMZ



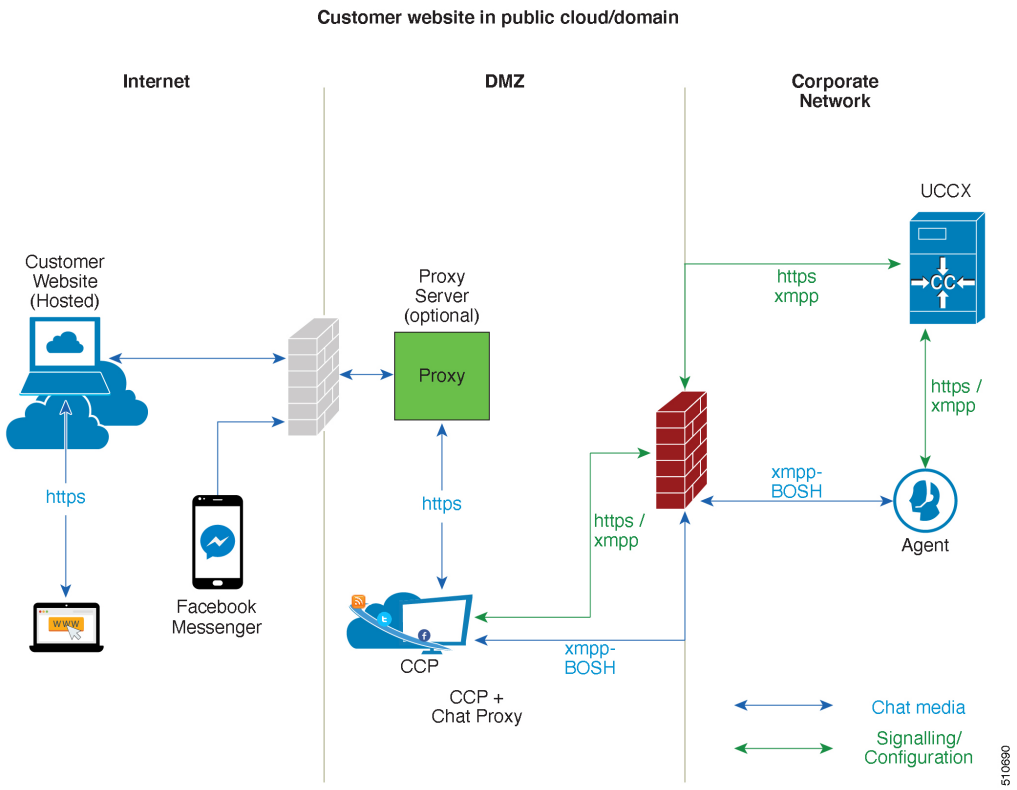
The Cisco Unified CCX is deployed inside the enterprise firewall and Customer Collaboration Platform is deployed inside company premises in the DMZ along with the customer website. The DMZ is open to all HTTPS traffic from the Internet. For Unified CCX Web Chat deployment to work, allow bidirectional 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 7: 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 12: 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 13: 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 14: 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).

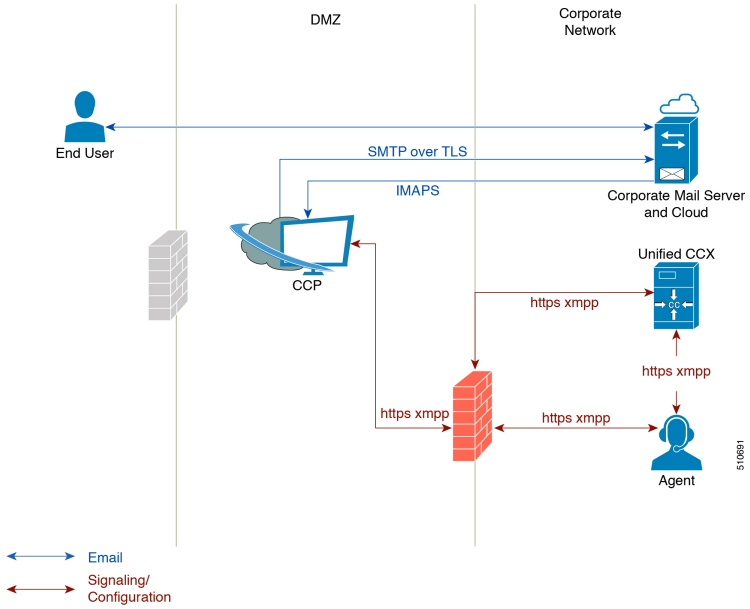
For more information about enabling IMAPS, see section “Mail Server Configuration” in *Cisco Unified Contact Center Express Administration and Operations Guide* at:

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 8: 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 15: 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 16: 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”.

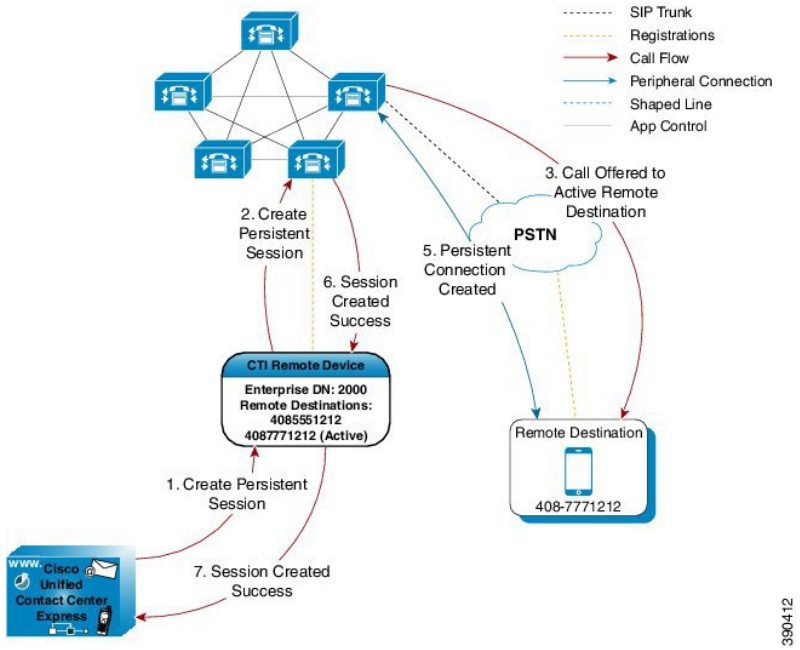
After the persistent connection is established for incoming calls, Unified CCX plays an announcement on persistent connection provided that announcement is configured with identifier as "UCCX Customer Call Prompt". The agent’s remote device displays the caller ID during the ICD call provided that the 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.

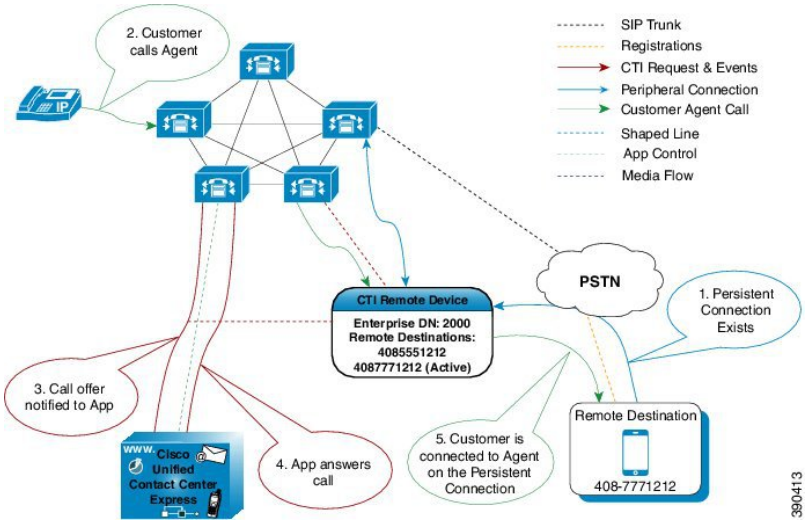
The following figure shows the persistent connection call flow:

Figure 9: Persistent Connection Call Flow



The following figure shows a persistent connection incoming call:

Figure 10: Persistent Connection Incoming Call

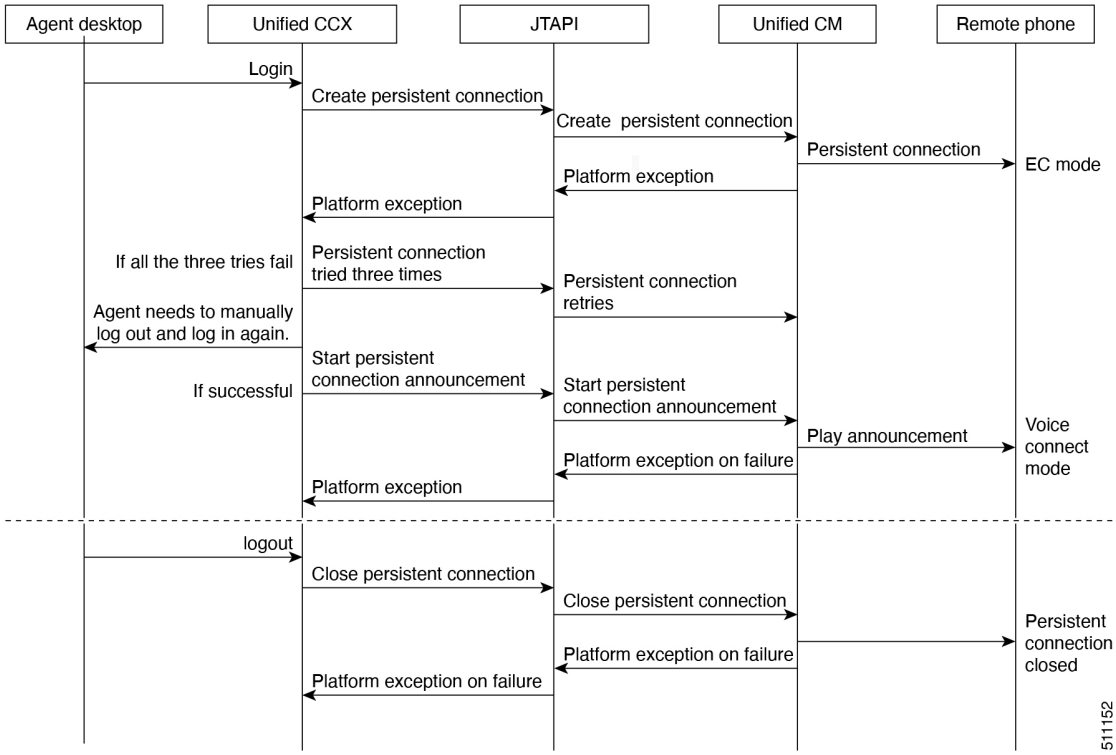


For remote phones that have persistent connection, the following features are not supported:

- 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)

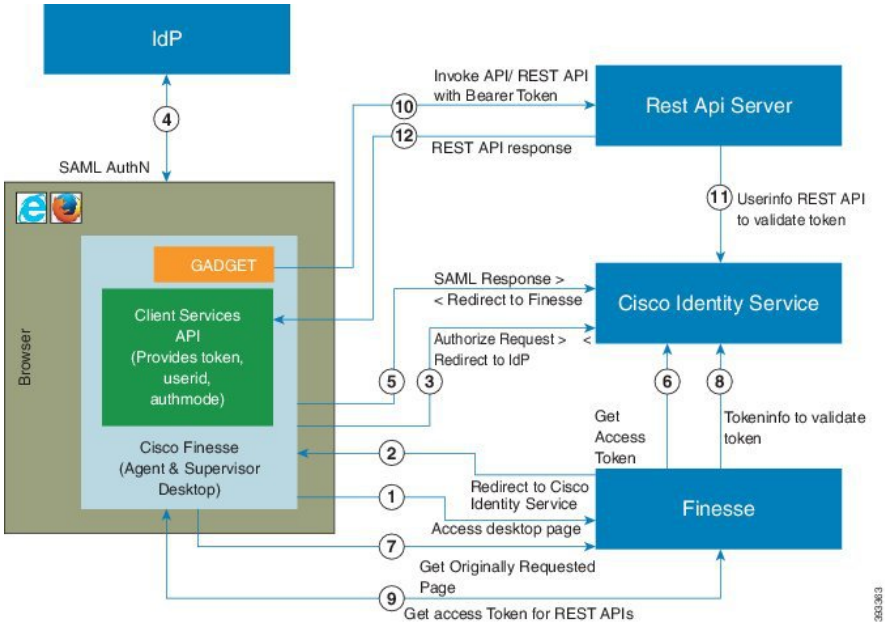
Authentication is managed for the contact center solution by the Cisco Identity Service (Cisco IdS). When an SSO-enabled user signs in, the Cisco IdS interacts first with the customer's Identity Provider (IdP) to authenticate the user. The IdP stores user profiles and provides authentication services 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 11: 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.