Cisco Unified Contact Center Express Features Guide, Release 12.5(1)

First Published: 2020-01-31

Last Modified: 2020-07-02

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

CONTENTS

Preface

Change History

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

Change	See	Date
Added note to save Contact Service Queues after changing agent competence level.	Digital Channels > Task Flow to Enable Digital Channels > Contact Service Queues	20 December 2022
Introduce License Control	Smart Licensing>Overview	**July 2020**
Added Specific License Reservation	Smart Licensing>Specific License Reservation	

Change	See	Date
Updated Document for Release 12.5(1) SU1 EFT1		**May 2020**
Cisco Webex Experience Management	Cisco Webex Experience Management >> Task Flow for Experience Management Post-Call Survey Cisco Webex Experience Management >> Task Flow for Account Setup Cisco Webex Experience Management >> Task flow to Integrate Experience Management and Unified CCX Cisco Webex Experience Management >>Task Flow to Configure IVR Experience Management Post-Call Survey Cisco Webex Experience Management >> Task Flow to Configure SMS/Email Experience Management Post-Call Survey	
Introduced Specific License Reservation	Smart Licensing >> Specific License Reservation Smart Licensing >> Specific License Reservation >> Request Specific License Reservation for Your Smart Account Smart Licensing >> Specific License Reservation >> Enable Specific License Reservation Smart Licensing >> Specific License Reservation >> Modify Specific License Reservation Smart Licensing >> Specific License Reservation >> Remove Specific License Reservation	
Initial Release of Document for Release 12.5(1)		**January 2020**

Change	See	Date
Cisco SocialMiner (SM) has been renamed as Customer Collaboration Platform (CCP).	Digital Channels >> License Requirements Digital Channels >> Install Cisco Customer Collaboration Platform Digital Channels >> Customer Collaboration Platform Configuration Digital Channels >> Contact Service Queues Digital Channels >> Configuration of Proxy Based on Deployment of Customer Collaboration Platform Digital Channels >> Certificate Management Digital Channels >> Unified CCX Agent Email	
Introduced Smart Licensing.	Smart Licensing	
Added Customer Smart Account.	Customer Smart Account	
Context Service related information has been removed.	-	
Procedure	Single Sign-On>>Configure the Cisco Identity Service Single Sign-On>>Configure the Cisco Identity Service>>Establish Trust Relationship for Cisco IdS Digital Channels>>Task Flow to Enable Digital Channels>>Configure Customer Collaboration Platform in Unified CCX>>Customer Collaboration Platform Configuration Digital Channels>>Task Flow to Enable Digital Channels>>Contact Service Queues	
Cisco Unified Operating System (Unified OS)	Digital Channels>>Task Flow to Enable Digital Channels>>Install Cisco Customer Collaboration Platform	

Change	See	Date
Widget Type has been removed.	Digital Channels>>Task Flow to Enable Digital Channels>>Chat Widgets>>Chat Widgets Page	
Updated the content to reflect Bubble Chat information.	Digital Channels>>Task Flow to Enable Digital Channels>>Chat Widgets>>Chat Widget Configuration	
Removed Classic Chat Widget topic.	Digital Channels>>Task Flow to Enable Digital Channels>>Chat Widgets>>Chat Widget Configuration	
Updated the description of Dynamic reskilling.	Digital Channels>>Unified CCX Agent Email>>Agent Email Features	
Introduced Cisco Webex Experience Management.	Cisco Webex Experience Management	

About This Guide

This guide explains features you can use in conjunction with Cisco Unified Contact Center Express. For each feature, there is a description, procedures for initial setup, and details on the functionality the feature provides.

Audience

This guide is prepared for Contact Center administrators who configure and run the contact center, manage agents, and address operational issues.

Related Documents

Document or Resource	Link
Cisco Unified Contact Center Express Documentation Guide	https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_documentation_roadmaps_list.html
Cisco Unified CCX documentation	https://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html
Cisco Unified Intelligence Center documentation	https://www.cisco.com/en/US/products/ps9755/tsd_products_support_series_home.html
Cisco Finesse documentation	https://www.cisco.com/en/US/products/ps11324/tsd_products_support_series_home.html

Document or Resource	Link
Cisco SocialMiner documentation **Note** From Unified CCX Release 12.5(1), CCP documents are available in the Cisco Unified CCX documentation folder.	https://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/tsd-products-support-series-home.html
Cisco Mediasense documentation	https://www.cisco.com/c/en/us/support/customer-collaboration/mediasense/tsd-products-support-series-home.html
Cisco Unified CCX Virtualization Information	https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-contact-center-express.html
Cisco Unified CCX Compatibility Information	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html

Documentation and Support

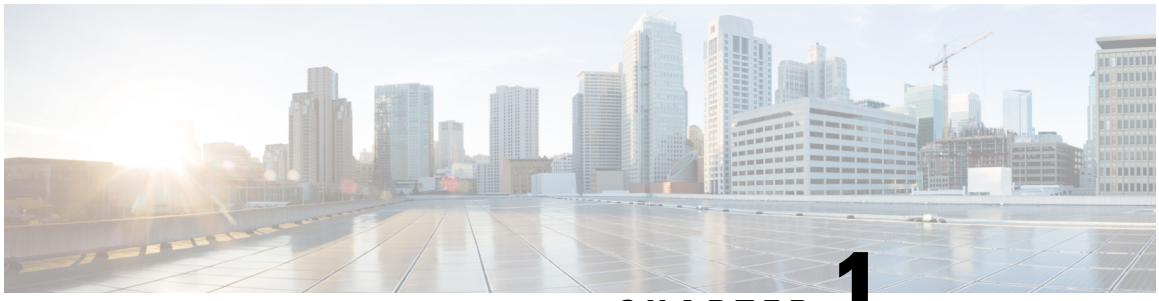
To download documentation, submit a service request, and find additional information, see *What's New in Cisco Product Documentation* at https://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

You can also subscribe to the *What's New in Cisco Product Documentation* RSS feed to deliver updates directly to an RSS reader on your desktop. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

Documentation Feedback

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

contactcenterproducts_docfeedback@cisco.com



CHAPTER 1

Contact Center Prerequisites

This chapter details the prerequisites that are required for a contact center to be set up. The setup of a Cisco Contact Center Express requires the installation of the contact center solution and all the required optional components. The bandwidth calculations must be performed to set up the contact center for an effective functioning. The bandwidth calculations are also based on the type of supported contact center media channels.

Install Unified CCX

Unified CCX installation has the following installation options:

- Standard installation - This option allows you to install Unified CCX software from the installation disc.
- Unattended installation - This option allows you to use the installation disc and a preconfigured USB disk to install Unified CCX software unattended.

Procedure

Step 1 Based on the installation scenarios and system requirements, ensure that the important considerations before installation are verified.

Step 2 Perform the preinstallation tasks as documented in the Cisco Unified Contact Center Express Install and Upgrade Guide.

Step 3 Follow the procedure documented in the Cisco Unified Contact Center Express Install and Upgrade Guide to install Unified CCX.

Contact Center Planning and Bandwidth Calculations

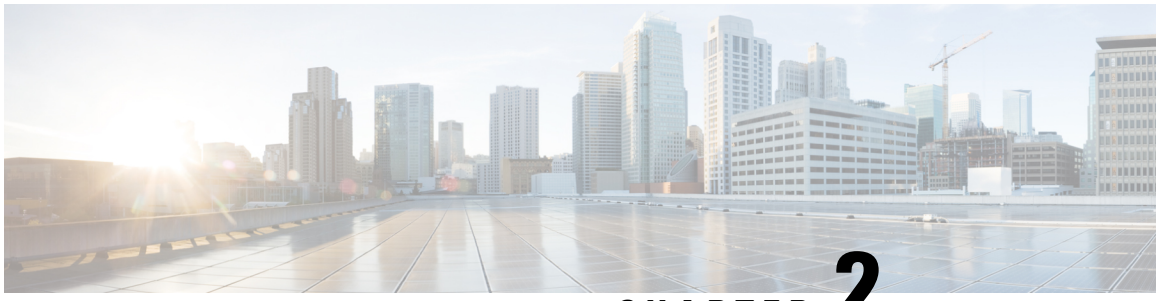
The calculation of bandwidth requirements and planning of a contact center must be done based on the type of contact center. You can plan the contact center for agents accepting one or more of the following customer service channels like Voice channels or Digital channels.

- Dedicated Voice

- Blended
- Email and Chat
- Priority Voice over Email and Chat

To calculate the bandwidth requirements based on the type of customer service channels planned for, see the Cisco Unified Contact Center Express Bandwidth Calculator. The bandwidth calculations are done based on various factors for the following requirements in the contact center:

- Cisco Finesse Desktop Sign in
- Cisco Finesse Features
- Cisco Finesse Live Data Report
- Email
- Chat
- External Database Services (EDBS)
- REST APIs
- Unified Intelligence Center Reporting
- Cisco Finesse IPPA
- Cisco Webex Experience Management
- Data Streaming to Cisco Webex Cloud



CHAPTER 2

Single Sign-On

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)

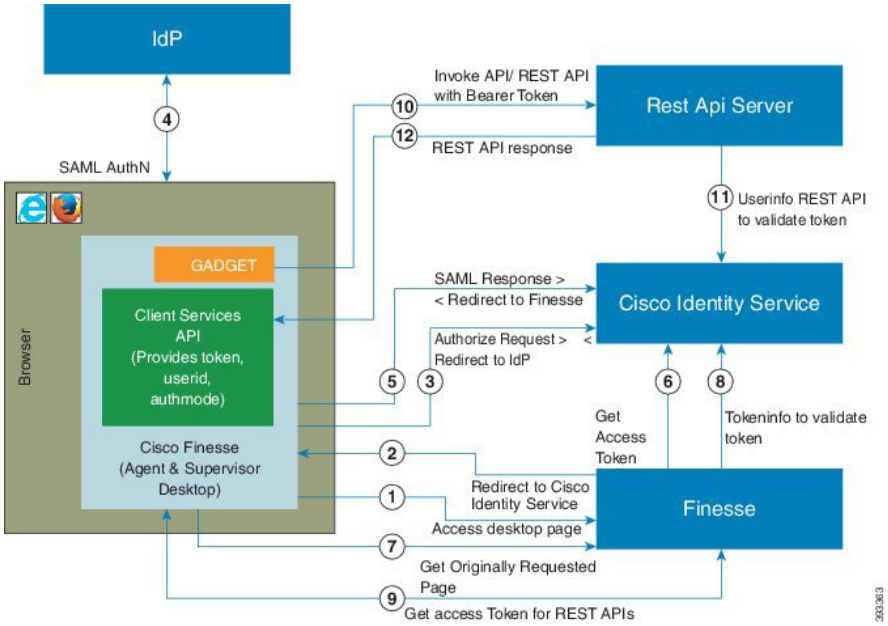
Authentication is managed for the contact center solution by the Cisco Identity Service (Cisco IdS). When an SSO-enabled user signs in, the Cisco IdS interacts first with the customer's Identity Provider (IdP) to authenticate the user. The IdP stores user profiles and provides authentication services 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 1: Authentication and Authorization Flow



Single Sign-On (SSO) Considerations

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

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

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

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

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

- Establish a trust relationship between the Cisco IdS and the Identity Provider.
- Set the SSO mode in your system to enable users for SSO.
- Register on the Single Sign-On web page to onboard the single sign-on components.
- Perform **Test SSO Setup** on the single sign-on web page to test the status of registration of each component. You will be redirected to the Identity Provider for authentication. If the **Test SSO Setup** is successful then the **Enable** option is enabled.

SSO Message Flow

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

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

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

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

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

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

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

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

Single Sign-On High Availability Considerations

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

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

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

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

Table 1: Failover and Failback Scenarios of Cisco Identity Service Client Based on the State of Cisco Identity Service

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

Single Sign-On Design Impacts

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

Authentication Modes in Unified CCX

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

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

Applications in SSO Mode

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

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

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

Applications not SSO Enabled

The following applications are not Single Sign-On enabled:

- Cisco Finesse Administration
- Cisco Identity Service Administration
- Disaster Recovery System
- Cisco Unified OS Administration
- Cisco Unified Serviceability
- Standalone Cisco Unified Intelligence Center
- Cisco Unified CCX Editor
- Real Time Monitoring Tool
- Cisco SocialMiner
- Cisco Media Sense
- Cisco Workforce Optimization
- Any Third Party Application.

Configure the Cisco Identity Service

The Cisco Identity Service (Cisco IdS) provides authorization between the Identity Provider (IdP) and applications.

When you configure the Cisco IdS, you set up a metadata exchange between the Cisco IdS and the IdP. This exchange establishes a trust relationship that then allows applications to use the Cisco IdS for single sign-on. You establish the trust relationship by downloading a metadata file from the Cisco IdS and uploading it to the IdP. You can then select settings related to security, identify clients of the Cisco IdS service, and set log levels and, if desired, enable Syslog format.

Procedure

Step 1 In Administration, navigate to **System** > **Single Sign-On**.

Note Use a log in name in the format *username@FQDN* to log in to the Administration.

Step 2 Click **Identity Service Management**.

Result:

The Cisco Identity Service Management window opens.

Step 3 Enter your user name, and then click **Next**.

Step 4 Enter your password, and then click **Sign In**.

The Cisco Identity Service Management page opens, showing the **Nodes**, **Settings**, and **Clients** icons in the left pane.

Step 5 Click **Nodes**.

The **Nodes** page opens to the overall Node level view and identifies which nodes are in service. The page also provides the **SAML Certificate Expiry** details for each node, indicating when the certificate is due to expire. The node **Status** options are **Not Configured**, **In Service**, **Partial Service**, and **Out of Service**. Click a status to see more information. The star to the right of one of the Node names identifies the node that is the primary publisher.

Step 6 Click **Settings**.

Step 7 Click **IdS Trust**.

Step 8 To begin the Cisco IdS trust relationship setup between the Cisco IdS and the IdP, click **Download Metadata File** to download the file from the Cisco IdS Server.

Step 9 Click **Next**.

Step 10 To upload the trusted metadata file from your IdP, browse to locate the file.

The **Upload IdP Metadata** page opens and includes the path to the IdP. When the file upload finishes, you receive a notification message. The metadata exchange is now complete, and the trust relationship is in place.

Step 11 Clear the browser cache.

Step 12 Enter the valid credentials, when page is redirected to IdP.

Step 13 Click **Next**.

The **Test SSO Setup** page opens.

Step 14 Click **Test SSO Setup**.

A message appears telling you that the Cisco IdS configuration has succeeded.

Step 15 Click **Settings**.

Step 16 Click **Security**.

Step 17 Click **Tokens**.

Enter the duration for the following settings:

- **Refresh Token Expiry** -- The default value is 10 hours. The minimum value is 2 hours. The maximum is 24 hours.
- **Authorization Code Expiry** -- The default value is 1 minute, which is also the minimum. The maximum is 10 minutes.
- **Access Token Expiry** -- The default value is 60 minutes. The minimum value is 5 minutes. The maximum is 120 minutes.

Step 18 Set the **Encrypt Token** (optional); the default setting is **On**.

Step 19 Click **Save**.

Step 20 Click **Keys and Certificates**.

The **Generate Keys and SAML Certificate** page opens and allows you to:

- Regenerate the **Encryption/Signature key** by clicking **Regenerate**. A message appears to say that the Token Registration is successful and advises you to restart the system to complete the configuration.

- Regenerate the **SAML Certificate** by clicking **Regenerate**. A message appears to say that the SAML certificate regeneration is successful.

Step 21 Click **Save**.

Step 22 Click **Clients**.
The **Clients** page identifies the existing Cisco IdS clients, providing the client name, the client ID, and a redirect URL. To search for a particular client, click the Search icon above the list of names and type the client's name.

Step 23 To add a client:

a) Click **Add Client**.
b) Enter the client's name.
c) Enter the Redirect URL. To add more than one URL, click the plus icon.
d) Click **Add** (or click **Clear** and then click the X to close the page without adding the client).

Step 24 To edit or delete a client, highlight the client row and click the ellipses under **Actions**. Then:

- Click **Edit** to edit the client's name, ID, or redirect URL. On the **Edit Client** page, make changes and click **Save** (or click **Clear** and then click the X to close the page without saving edits).
- Click **Delete** to delete the client.

Step 25 Click **Settings**.

Step 26 From the **Settings** page, click **Troubleshooting** to perform some optional troubleshooting.

Step 27 Set the local log level by choosing from **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.

Step 28 To receive errors in Syslog format, enter the name of the Remote Syslog Server in the Host (Optional) field.

Step 29 Click **Save**.

You can now:

- Register components with the Cisco IdS.
- Enable (or disable) SSO for the entire deployment.

Establish Trust Relationship for Cisco IdS

To enable applications to use Cisco Identity Service (Cisco IdS) for Single Sign-On, perform the metadata exchange between the Cisco IdS and the Identity Provider (IdP).

- Download the SAML SP Metadata file, `sp.xml`, on the Cisco IdS publisher primary node.
  1. Open Identity Service Management by doing either of the following:
     - Open the Identity Service Management window: `https://<Unified CCX server address>:8553/idsadmin`.
     - In Administration, navigate to **System** > **Single Sign-On** and click **Identity Service Management**.
  2. On the **Settings** > **IdS Trust** tab, download the SAML SP Metadata file, `sp.xml`.

- Download the Identity Provider Metadata file, federationmetadata.xml, from the IdP. For example,

  1. For AD FS, download the Identity Provider Metadata file from the IdP at the location:

     `https://<ADFSServer FQDN>/federationmetadata/2007-06/federationmetadata.xml`.

  2. On the **Identity Service Management** page, upload the Identity Provider Metadata file that was downloaded in the previous step.

The SAML SSO uses trust authentication certificates to exchange authentication and authorization details between the IdP (such as AD FS) and the Cisco IdS. This secures the communication between the servers.

Note

- Cisco IdS supports SAML self-signed certificates for authentication.
- If the IdP certificates are automatically rolled-over, manually renewed, or updated by the administrator, then re-establish the trust relationship between the IdS and the IdP.

Configure an Identity Provider

To support SSO for the contact center solution, configure an Identity Provider (IdP) that is compliant with the Security Assertion Markup Language 2.0 (SAML v2) Oasis standard. The IdP stores user profiles and provides authentication services to the contact center solution.

This section provides details on the qualified Identity Providers (IdPs) and the reference links to configure the IdPs.

Qualified Identity Providers

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

- SAML Request Attributes
- Expectations from SAML Response

IdP Metadata Schema

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

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

SAML Request Attributes

SAML request supports the following SAML 2.0 bindings:

- **HTTP-POST** binding

- NameIDFormat in SAML request must be **urn:oasis:names:tc:SAML:2.0:nameid-format:transient**

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
       ID="s25f4fb66688cf429e430034f4cceac00b6124570d" Version="2.0"
       IssueInstant="2018-10-29T10:01:39Z"
Destination="https://win-adfs30-151.uccxteam.com/adfs/ls/"
       ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
       AssertionConsumerServiceURL="https://ccxssodemo1.cisco.com:8553/ids/saml/response">
    <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">ccxssodemo1.cisco.com</saml:Issuer>
    <samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
           Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
          SPNameQualifier="ccxssodemo1.cisco.com" AllowCreate="true"></samlp:NameIDPolicy>
</samlp:AuthnRequest>
```

Expectations from SAML Response

The following are the expectations from SAML Response:

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

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

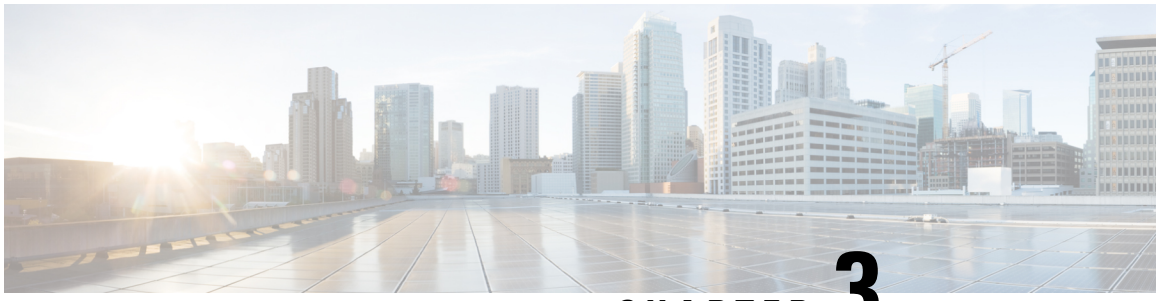
```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
Destination="https://ids-ssp-node.cisco.com:8553/ids/saml/response"
    ID="_6a309495-d3c2-4a28-b8e3-289f8f5355bd"
InResponseTo="s21c84ba20862f573f5daec121c305ba6aac877843"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

    </Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
 />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
            <ds:Reference URI="#_6a309495-d3c2-4a28-b8e3-289f8f5355bd">
            ..........
            </ds:Reference>
        </ds:SignedInfo>
        ..........
        ..........
     </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
```

```
ID="_df3bdbcf-a225-4e97-b00a-a199bdda3d2c"
        IssueInstant="2017-08-10T13:20:26.556Z" Version="2.0">
        <Issuer>http://ADFSServer.cisco.com/adfs/services/trust</Issuer>
        ............

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

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

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

Hostname or IP Address Change

If you change the Hostname or IP Address of the Cisco IdS server, then perform the following:

- Re-generate the SAML certificate.
- Re-establish trust relationship between IdP and IdS.
- If the components are registered earlier, then
  - Re-register all the SSO components.
  - Perform the SSO Test to check if all the SSO components are registered. Verify that the test is successful for each component.



CHAPTER 3

Cisco Webex Experience Management Survey

Overview

Cisco Webex Experience Management is a Customer Experience Management (CEM) platform, enabling you to see your business from your customers' perspective and their experience with the brand. Experience Management powers customer journey mapping, text analytics, and predictive modeling using the feedback collected from customers via different channels such as email, SMS, and IVR.

Experience Management also allows handling of Personally Identifiable Information (PII) about a customer in a sensitive manner by avoiding storing PII data on the platform.

With Experience Management integrated with Unified CCX:

- Administrators can configure post-call surveys to collect feedback directly from customers.
- Administrators can configure and add gadgets that can be viewed on the Finesse desktop. The gadgets can display Customer Experience Journey of the customer calling in or aggregated feedback data about agent or supervisor performance.
- Agents and supervisors can view the pulse of the customers using industry standard metrics such as NPS, CSAT, and CES or any other custom KPIs.

Note Currently, you can have surveys only for inbound ICD calls.

For an overview about Experience Management, see Experience Management Overview.

For more information on the voice survey, see Experience Management Voice Survey.

For more information on the SMS or email survey, see Experience Management SMS or Email Survey.

For more information on PII data handling, see Experience Management PII .

Task Flow for Experience Management Post-Call Survey

Unified CCX is integrated with Experience Management to collect customer feedback through the various channels such as voice, SMS, or email post-call surveys.

The following table lists the tasks that are required to be performed to enable cross channel integration between Unified CCX and Experience Management:

Table 2: Tasks for Enabling Post-Call Survey

Task	Description
Experience Management account setup	Task Flow for Account Setup, on page 16
Onboarding and configuring Unified CCX to enable cross channel integration	Task flow to Integrate Experience Management and Unified CCX, on page 17
Configure voice (IVR) survey	Task Flow to Configure IVR Experience Management Post-Call Survey, on page 17
Configure SMS or email survey	Task Flow to Configure SMS/Email Experience Management Post-Call Survey, on page 19

Task Flow for Account Setup

The task flow to setup an account to enable Experience Management Post-Call Survey in Cisco Unified CCX solution is as follows:

Table 3: Tasks to Setup an Account

Sequence	Task
1	Contact your Cisco representative to purchase Experience Management licenses. After the purchase, you need to provide relevant information about your organization to the Experience Management Activation Team. To know more about the information that will be collected, see Prerequisites.
2	Experience Management Activation Team creates: **1.** Accounts and provisions the same. **2.** Default spaces and metric groups for your accounts. To know more about creating spaces, see Space Creation. **3.** Standard questionnaires for Experience Management Post Call Survey and publishes the same. To know more about creating questionnaires, see Questionnaires.
3	After successful account creation and provisioning, you will receive handover emails from the Experience Management Activation Team. The email contains credentials and other essential information for your account. To know more about provisioning details, see Handover.

Sequence	Task
4	Initially Spaces and Widgets are created by the Experience Management provisioning team. To know more about the different default Widgets, how to export and derive meaningful insights from them, see Experience Management Widgets. To know how to configure additional Widgets in Experience Management, see Configure Experience Management Widgets.

Task flow to Integrate Experience Management and Unified CCX

To onboard and configure Experience Management post-call survey in Cisco Unified CCX solution, the task flow is as follows:

Table 4: Configure Experience Management in Unified CCX

Sequence	Task
1	Use the details provided in the Handover emails and provision Experience Management in Unified CCX by using the **set cloudconnect cherrypoint config** command. For more information, see *Cloud Connect* topic in *Command Line Interface* chapter of *Cisco Unified Contact Center Express Admin and Operations Guide*.
2	Configure server settings in **Cloud Connect Server Settings** gadget of Finesse Administration, with hostname of Unified CCX nodes. Use the application user credentials. For more information, see *Cloud Connect Server Settings* topic in *Cisco Unified Contact Center Express Admin and Operations Guide*.
3	**Add Gadgets to Finesse desktop** The following Experience Management Widgets can be added as gadgets in Finesse desktop: • Customer Experience Journey • Customer Experience Analytics For example, you can add Customer Experience Journey in the **Home** page and Customer Experience Analytics in **My Statistics** page for agents and **Manage Team** page for supervisors. To know more about adding Gadgets to your Finesse desktop, see Experience Management Gadgets.

Task Flow to Configure IVR Experience Management Post-Call Survey

The task flow to enable IVR Experience Management post-call survey in Unified CCX solution is as follows:

Table 5: Tasks to Enable IVR Experience Management Post-Call Survey

Sequence	Task
1	Create and configure the questionnaires in Experience Management for sending IVR surveys to the customer. For more information about creating questionnaires, see Questionnaires.
2	In CUCM, configure Domain Routing based SIP Route Pattern, which is associated with SIP Trunk, so that the calls can be forwarded to the Survey URI (URI of the domain that has been provisioned, which is shared as part of the Handover). For more information, see *Cisco Unified Call Manager Admin Guide*.
3	Configure the Unified CCX Administration to provide an inline IVR survey to the customer. Select the required questionnaire for IVR survey from **Enable Cisco Webex Experience Management post-call survey** available in the **Cisco Script Application** page of Unified CCX Administration. For more information, see *Cisco Unified Contact Center Express Admin and Operations Guide*.

Note If you associate an application with both IVR Experience Management post-call survey and Unified CCX Post-Call Treatment, when an agent ends a call from Finesse desktop, the Unified CCX Post-Call Treatment takes precedence and the call is not transferred to Experience Management post-call survey.

Configure Scripts for IVR Survey

The following script variables can be configured for IVR survey:

Table 6: Script Variables for IVR Survey

Script Variable	Type	Description
POD.ID	ECC	In IVR script, populate the *POD.ID* ECC variable with customer ID because **Customer Experience Journey** gadget uses this variable to fetch and display all responses that are provided by the calling customer, across all channels. If the variable is not populated, it uses the calling number to fetch the relevant responses.
ccx_survey_opt_in	session	**Enabling and Disabling a Survey for a Customer** When an application is associated with a **Post-Call Survey**, by default the survey is presented to all customers, when agents end the calls from the Finesse desktop. If the *ccx_survey_opt_in* session variable in IVR script is set as **false** (for a customer, in a particular session), the survey is not presented to that customer after the agent ends the call from the Finesse desktop. The *ccx_survey_opt_in* session variable holds a Boolean value. **Note** The survey that is played to the customer, is the one that is associated with the first application that is triggered for the customer. However, the survey data is associated with the agent who ends the call on Finesse desktop.

Script Variable	Type	Description
ccx_survey_language	session	**Customers' Language Preference** When an Unified CCX application is associated with a survey, the script may use the *ccx_survey_language* session variable in IVR script to add the language preference of the customers. The format of the variable is **LanguageCode-CountryCode**. For example, **en-US**. If the *ccx_survey_language* session variable is not populated in IVR script, by default, the language associated with trigger will be used. To configure the survey to be played in multiple languages, see Questionnaires. To know the languages that are supported by Experience Management, see Languages. **Note** When a customer selects a language through Unified CCX application and if the same language is not configured for that survey in Experience Management, the language selection option is played to the customer.

Task Flow to Configure SMS/Email Experience Management Post-Call Survey

The task flow to enable SMS/Email Experience Management post-call survey in Unified CCX solution is as follows:

Table 7: Tasks to Configure SMS/Email Experience Management Post-Call Survey

Sequence	Task
1	The partner hosted module in the Experience Management Invitations solution is mandatory for the SMS/Email surveys to work. For information about partner hosted module, see https://xm.webex.com/docs/cxsetup/guides/partnerarchitecture/ For information about how to provision the infrastructure required to deploy the partner hosted components of the Experience Management Invitations module, see https://xm.webex.com/docs/cxsetup/guides/partnerinfra/. For information about how to provision the infrastructure required to deploy the partner hosted components, see https://xm.webex.com/docs/cxsetup/guides/partnerdeployment/
2	Configure the Experience Management Invitation module for sending SMS/Email surveys to the customer. Create dispatch templates on Experience Management. For information about setting up dispatch in Experience Management, see https://xm.webex.com/docs/cxsetup/guides/
3	Configure the Unified CCX Administration to provide an offline SMS/Email survey to the customer. Select the required dispatch template for SMS/Email survey from **Enable Cisco Webex Experience Management post-call survey** available in the **Cisco Script Application** page of Unified CCX Administration. For more information, see *Cisco Unified Contact Center Express Admin and Operations Guide*.

Note You can associate an application with both SMS/Email Experience Management post-call survey and Unified CCX Post-Call Treatment. Legacy Unified CCX post-call survey is triggered only if agent ends the call from Finesse desktop. SMS/Email survey is triggered irrespective of who ends the call. When both SMS/Email Experience Management post-call survey and Unified CCX Post-Call Treatment are enabled, Unified CCX Post-Call Treatment is triggered and the Experience Management post-call survey is sent.

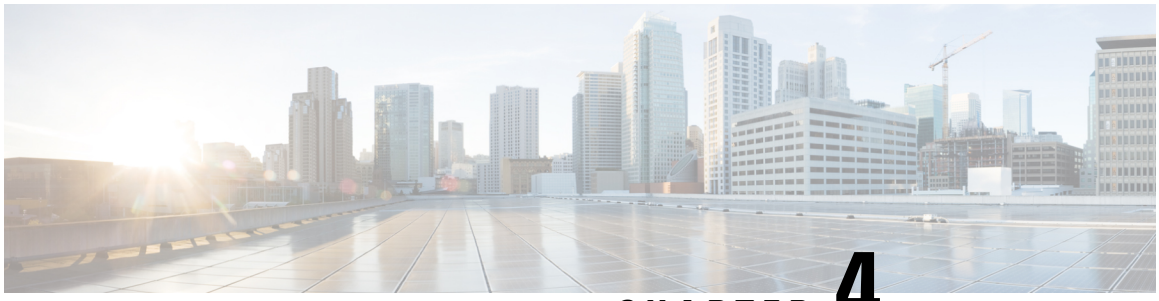
Configure Scripts for SMS/Email Survey

The following script variables can be configured for SMS/Email survey:

Table 8: Script Variables for SMS/Email Survey

Script Variable	Type	Description
POD.ID	ECC	In IVR script, populate the *POD.ID* ECC variable with customer ID because **Customer Experience Journey** gadget uses this variable to fetch and display all responses that are provided by the calling customer, across all channels. If the variable is not populated the SMS/Email survey may not work as expected.
ccx_survey_opt_in	session	**Enabling and Disabling a Survey for a Customer** When an application is associated with a **Post-Call Survey**, by default the survey is presented to all customers after the call ends. If the *ccx_survey_opt_in* session variable in IVR script is set as **false** (for a customer, in a particular session), the survey is not presented to that customer. The *ccx_survey_opt_in* session variable holds a Boolean value. **Note** The survey that is sent to the customer, is the one that is associated with the first application that is triggered for the customer after the call ends.
ccx_survey_language	session	**Customers' Language Preference** When an Unified CCX application is associated with a survey, the script may use the *ccx_survey_language* session variable in IVR script to add the language preference of the customers. The format of the variable is **LanguageCode-CountryCode**. For example, **en-US**. If the *ccx_survey_language* session variable is not populated in IVR script, by default, the language associated with trigger will be used. To configure the survey to be played in multiple languages, see Questionnaires. To know the languages that are supported by Experience Management, see Languages. **Note** When a customer selects a language through Unified CCX application and if the same language is not configured for that survey in Experience Management, the customer is asked to choose from the language selection options before accessing the survey.

Script Variable	Type	Description
ccx_customer_ani	session	**Customer's Phone Number** If the *ccx_customer_ani* session variable is configured with the phone number of the customer in the IVR script then an SMS is sent to this number when one of the channel associated is SMS. If the phone number is not configured then the phone number of the caller is obtained from JTAPI.
ccx_customer_email_id	session	**Customer's Email ID** When an Unified CCX application is associated with a survey, the script can use the *ccx_customer_email_id* session variable in IVR script to add the email address of the customer. This is a mandatory variable for the SMS/Email survey to work when one of the channel associated is email.



CHAPTER 4

Digital Channels

Task Flow to Enable Digital Channels

To enable digital channels in your contact center solution, follow this task flow:

License Requirements

The digital channel features of Cisco SocialMiner are available in the Premium license version of Cisco Unified Contact Center Express. The feature availability in Unified CCX is based on the type of license for Cisco Unified Contact Center Express.

Install Cisco SocialMiner

SocialMiner is installed as an appliance using the Cisco Unified Operating System (Unified OS). The operating system and the SocialMiner application are installed together using a similar installation process as other Unified OS products such as Cisco Unified Communications Manager and Cisco Unified Intelligence Center.

SocialMiner operates on a VMware Virtual Machine (VM) on hardware that is running a VMware Host Server. SocialMiner currently supports installation of only a single node (as opposed to a duplexed or redundant system).

Perform the following steps to install SocialMiner:

Procedure

Step 1 Create a virtual machine using a VMware Open Virtual Format template.

Step 2 Use the latest OVA template for the fresh installation of SocialMiner release. Go to https://software.cisco.com/download/home/270569179 and download this template.

Step 3 When deploying the template, select either a large or a small deployment from the drop-down list.

Step 4 Mount the SocialMiner DVD or ISO file to the virtual machine and set the virtual machine to boot from the SocialMiner DVD. The installation wizard opens. Use Tab to navigate between elements and then press the space bar or the Enter key to select the element and proceed.

Step 5 Perform the media check when prompted.

Step 6 Follow the instructions on the screen and select Yes or Continue.

Step 7 Use the arrow keys to highlight the correct time zone and then use **Tab** to navigate to the **OK** button. Press **Enter** to proceed.

Step 8 Provide the network information for SocialMiner . You must provide valid hostname with matching IP address. The system confirms that the hostname matches the IP address later in the installation process.

Step 9 Select **Yes** to provide DNS Client Settings for SocialMiner . Provide DNS servers and the domain. Select **OK**. DNS configuration is mandatory.

Step 10 Provide an Administrator ID and password. This credential is for platform (Unified OS) administration.

Step 11 Provide information about your organization. This information generates the security (SSL) certificates for this server.

Step 12 You must provide at least one NTP Server. Enter the NTP host address and select **OK**.

Step 13 Provide a security password.

Step 14 Provide a username and password for the SocialMiner administrator. You can import additional SocialMiner users from Active Directory after the SocialMiner installation is complete.

Step 15 The confirmation window opens. You can select **Back** to change settings or **OK** to complete the installation. Installation can take up to 2 hours. The server may reboot to complete the installation steps. If you install from an ISO file and see the virtual machine message, to "Disconnect anyway (and override the lock)?", select **Yes**. A sign-in prompt appears on the server console.

Step 16 After the installation is complete, perform the one-time setup tasks like:

a) If your system is installed behind a firewall, set up an HTTP proxy so that feeds can access sites on the Internet.

b) Configure Active Directory so that more users can sign in.

c) If you want to use Cisco Unified Intelligence Center, set up the reporting user so that the reporting tool can access the reporting database.

Configure SocialMiner in Unified CCX

SocialMiner Configuration

Use the **SocialMiner Configuration** web page to configure Cisco SocialMiner . You must configure information only on this web page to enable the chat and email features.

Cisco Unified CCX does not support custom configuration changes on the chat and email campaigns or feeds from the SocialMiner administration page.

This option is available only with the Unified CCX Premium license package. The email feature support for Unified CCX depends on the SocialMiner version. For information about feature compatibility, see the Unified

CCX Compatibility related information, located at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Any configuration change using SocialMiner Administration interface is not supported.

Note On a high availability setup, after the **Add to Cluster** operation is successful, the following message is displayed:

```
In case of HA, configure the SocialMiner on secondary node after adding
to cluster in the secondary node.
```

Every time you navigate to this page, the state of feeds, campaigns, and notifications rules are validated for chat and email, the connectivity to the email server is checked, and the web page shows the appropriate status. Icons are used as visual indicators to display the status of each service. Hover the cursor over the icon to display a tool tip that explains the reason for the current state. As part of validation, Unified CCX checks the following:

- **SocialMiner XMPP Service**

  Unified CCX checks the connectivity with the SocialMiner XMPP service. If the XMPP service is down, the following message is displayed:

  ```
  SocialMiner XMPP service is not accessible. Check the logs for more
  details.
  ```

- **SocialMiner Runtime Service**

  Unified CCX checks the connectivity with the SocialMiner runtime service. If the runtime service is down, the following message is displayed:

  ```
  SocialMiner runtime service is not accessible. Check the logs for more
  details.
  ```

- **SocialMiner Tomcat Service**

  Unified CCX checks the connectivity with the SocialMiner Tomcat service. If the Tomcat service is down, the following message is displayed:

  ```
  Unable to communicate to the SocialMiner on the IP address(Hostname)
  provided. Please verify whether SocialMiner is running on this IP
  address(Hostname) or check the network connection and make sure that
  SocialMiner is reachable from CCX.
  ```

- **SocialMiner Status**
  - **Feeds**

    Unified CCX validates the status of the intended chat and email feeds in SocialMiner .

    - —All the feeds are operating normally in SocialMiner .
    - —One or more feeds mismatches with SocialMiner .
    - —All the feeds are missing in SocialMiner .

  - **Campaigns**

Unified CCX validates the status of the intended chat and email campaigns in SocialMiner .

- —All the campaigns are operating normally in SocialMiner .
- —One or more campaigns mismatches with SocialMiner .
- —All the campaigns are missing in SocialMiner .

- **Notifications**

  Unified CCX validates the status of the intended chat and email notifications in SocialMiner .

  - —All the notifications are operating normally in SocialMiner .
  - —One or more notifications mismatches with SocialMiner . This status icon also appears after configuration, when no chat and email contact is injected yet. The status will change to normal after successful injection of chat and email contact.
  - —All the notifications are missing in SocialMiner .

- **Email Server**

  Unified CCX checks the connectivity with the email server.

  - —Email server is operating normally.
  - **Not Configured**—Channel provider is not configured.
  - **Not Applicable**—The following are the reasons for the current state:
    - Cisco Finesse is not active.
    - Email CSQ is not configured.
    - SocialMiner version is incompatible with the Email feature.
  - —Unable to reach the email server.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat > CCP Configuration** OR **Subsystems** > **Chat and Email > SocialMiner Configuration** as applicable.

The **Configuration** web page appears.

Note Ensure that SocialMiner certificate is uploaded to the Unified CCX Tomcat trust store using the Cisco Unified OS Administration interface. You can also use the `set cert import trust tomcat` CLI.

Unified CCX and SocialMiner servers must have DNS entries. SocialMiner must be accessible to Unified CCX by hostname. If the entries are not valid, an error is displayed.

Step 2 Complete or modify the following fields for SocialMiner :

Field	Description
IP Address / Host Name	IP address or fully qualified domain name of the SocialMiner server. For example, 192.168.1.5 or host.example.com.
User Name	Username of the SocialMiner administrator.
Password	Password of the SocialMiner administrator.

Note When the SocialMiner application password is reset, ensure that the new password is first updated in Unified CCX and then reset the password in SocialMiner . This prevents the account getting locked due to the authentication attempts from Unified CCX with old password.

Step 3 Click **Save** to save the changes.

Note

- If you see an error message, click **Save** to re-create feeds, campaigns, and notifications for chat and email in SocialMiner.
- When Unified CCX hostname is changed or when a new Unified CCX node is added, theSocialMiner Configurations must be saved again. This enables the change to take effect to re-create all the notifications for email and chat in SocialMiner .
- The Classic Chat Web Forms will not work if the feed is deleted from SocialMiner Administration interface. To revive this chat web form, save the SocialMiner configuration in the Unified CCX. A new Feed ID will then be created in the Unified CCX database. Download the Classic Chat Web Form code snippet again from the Chat Widget section of UCCX Administration and redeploy on the website to reflect the new feed ID.

Mail Server Configuration

Use the **Mail Server Configuration** web page to configure the mail server. This web page is available only when Cisco Finesse is enabled on the Unified CCX node with a premium license.

Before you begin

- Execute the commands **set-service msExchangeIMAP4 -startuptype automatic**, and **start-service msExchangeIMAP4** on Microsoft Exchange to set the Microsoft Exchange IMAP4 service to start automatically.
- Execute the command **set-service msExchangeIMAP4BE -startuptype automatic**, and execute **start-service msExchangeIMAP4BE** (for Microsoft Exchange 2013) on Microsoft Exchange to set the Microsoft Exchange IMAP4 Back End service to start automatically.

  These commands are specific to the local Exchange server.
- Create accounts and email addresses to be used for CSQ creation.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat and Email** > **Mail Server Configuration**.
The **Mail Server Configuration** web page opens.

Step 2 Complete or modify the following fields for the mail server:

Field	Description
Mail Server Settings	
Mail Server	Choose the mail server that is required to be configured from the listed options: • MS Exchange Server / Office 365 • Gmail
IMAP Folder Structure	
Drafts Folder Name	The name of the drafts folder of the respective mail server that is configured.
Outbox Folder Name	The name of the outbox folder of the MS Exchange Server / Office 365 email server that is configured. This folder is not available for the **Gmail** mail server.
Sent Items Folder Name	The name of the sent items folder of the respective mail server that is configured. **Note** All the listed mail servers have the default folder names prepopulated for all the IMAP folders in English locale. These folder names can be edited and can have custom values.
Incoming (Secure IMAP)	
Host Name	Fully qualified domain name (FQDN) of the incoming (IMAP) server. Do not enter the IP address.
Port Number	Port number that is used to connect to the IMAP server. The default port number is 993.
Outgoing (Secure SMTP)	
Host Name	FQDN of the outgoing (SMTP) server. Do not enter the IP address.
Port Number	Port number that is used to connect to the SMTP server. The default port number is 587.
Proxy Settings	
SOCKS	Choose the **Enable** or **Disable** radio button to use socks proxy for Mail Server connectivity. By default the **Disable** option is selected and **Enable** option is disabled. To enable **SOCKS**, configure **SOCKS Proxy** in **System Parameters** page.

Field	Description
Description	Description of the mail server.

Step 3 Click **Update** to save the changes.

Contact Service Queues

Before you begin

- You must create a skill before creating a CSQ. For information about creating a skill, see *Skill Configuration* section in the Cisco Unified Contact Center Express Administration and Operations Guide.
- Before creating an email CSQ, you must have configured the mail server.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat** > **Contact Service Queues** or **Subsystems** > **Chat and Email** > **Contact Service Queues** as applicable.

The Contact Service Queues (CSQs) web page opens and displays the information for existing chat and email CSQs if any.

Step 2 To add a new chat or email CSQ, click the **Add New** icon that appears in the toolbar in the upper left corner of the window or the **Add New** button that appears at the bottom of the window.

The Contact Service Queue Configuration web page opens.

Step 3 Specify the following fields:

Field Name	Description
CSQ Name	Name for the CSQ.

Field Name	Description
Resource Selection Criteria	Resource selection criteria chosen for the chat CSQ. • **Longest Available**—Selects the agent who has been in the Available state for the longest amount of time. • **Most Skilled**—Used for expert agent chat distribution. Selects the agent with the highest total competency level. The total competency level is determined by adding the agent's competency levels for each assigned skill that is also assigned to the CSQ. • Example 1: If Agent1 is assigned Skill1(5), Skill2(6), and Skill3(7) and CSQ1 specifies Skill1(min=1) and Skill3(min=1), the total competency level for Agent1 for CSQ1 is 12. • Example 2: If Agent1 is assigned Skill1(5) and Skill2(6), and Skill3(7) and CSQ1 specifies Skill1(min=1), only, the total competency level for Agent1 for CSQ1 is 5. **Note** • To change the competence level for an already configured agent, change the agent skill level and save the CSQ. • If two agents score equal in the primary selection criteria, the agent who was updated first will be assigned to the incoming chat until the maximum chats threshold is reached.

Table 9: CSQ Type—Chat

Field Name	Description
CSQ Type	Choose Chat.

Table 10: CSQ Type—Email

Field Name	Description
CSQ Type	Choose Email. **Note** You can create up to 100 email CSQs. If you exceed the limit, the following error is displayed: `Cisco Unified CCX supports a maximum of 100 Email CSQs. Exceeded maximum limit for Email CSQs.`
Mail Server	Fully Qualified Domain Name (FQDN) of email server. This field displays the mail server that you configured.
Email username	The email address to which emails are sent or retrieved.
Email password	Password for the email account.

Field Name	Description
Inbox Folder Name	The folder from which emails will be fetched and queued for the Contact Service Queue. Default value = Inbox folder of the selected mail server type
Drafts Folder Name	The folder to which SocialMiner will save the drafts of the emails when agent composes the response.
Outbox Folder Name	The folder to which SocialMiner will move the response email to, when it is being sent. This folder does not exist for **Gmail** mail server. The email response being sent will be moved to the drafts folder.
Sent Items Folder Name	The folder to which SocialMiner will move the response email to, when it is sent.
Test Configuration	This checks the following: • Connectivity from SocialMiner to the configured mail server by using the user credentials that is specified in the Contact Service Queue (CSQ) configuration. • Presence of and permissions to the Inbox, Drafts, Outbox, and Sent Items folder for the user, that is specified in the CSQ configuration.
Poll Interval (Seconds)	Frequency in seconds to fetch emails from the server. Default value = 600, Range = 10 to 86400
Snapshot Age (Minutes)	Specify the time in minutes from when the emails are to be fetched. Default value = 120, Range = 10 to 43200 For example, if you specify 120 minutes, this field fetches the emails from the last two hours.

Step 4 Click **Next**.

The Skill Association for CSQ area opens with the newly assigned CSQ name.

Note You can create up to 100 email CSQs. If you exceed the limit, the following error is displayed:

```
Cisco Unified CCX supports a maximum of 100 Email CSQs. Exceeded maximum
limit for Email CSQs.
```

Step 5 From the Available Skills list, choose the skill that you want to associate with the CSQ by clicking it. To choose more than one skill, press the **Ctrl** key and click the skills that you want to associate with the CSQ.

Step 6 Click **Add**.

The chosen skill and the minimum competence level for that skill are displayed in the right pane under the heading **Selected.**

Note To delete the skill from the Skills Required list, click the **Delete** icon next to **Minimum Competence**.

Step 7 Specify a minimum competence level for the skill assigned to the CSQ.

Step 8 To view the associated resources, click **Show Resources**.

Step 9 Click **Save** to save the changes for the CSQ.

The newly added CSQ appears in the **List of CSQs**.

Note You can create up to 100 email CSQs. If you exceed the limit, the following error is displayed:

```
Cisco Unified CCX supports a maximum of 100 Email CSQs. Exceeded maximum
limit for Email CSQs.
```

You can sort the CSQs by title by clicking the **CSQ Name** header and by type by clicking the **CSQ Type** header.

Step 10 To view the printable report and associated resources, click the CSQ for which you want to view the report and the associated resources and then click **Open Printable Report**.

Note To delete a CSQ, click the CSQ that you want to delete and then click **Delete**. A warning dialog box appears, asking you to confirm the deletion. To delete, click **OK**.

Caution Deletion of the chat CSQ affects the associated chat web forms. After deleting, modify the corresponding chat web form configurations and generate the HTML code.

Predefined Responses

You can add a maximum of ten chat predefined responses. These predefined responses are available to all the agents in the Manage Chats Gadget on the Finesse Agent Desktop. Use the **Predefined Responses** page to configure and manage chat predefined responses. To access the predefined responses, choose **Subsystems** > **Chat** > **Predefined Responses**.

Note Predefined responses are not available in the Cisco Agent Desktop. They are only available with the Finesse Agent Desktop.

Predefined Responses

Using this web page, you can add, modify, and delete predefined responses.

You can add a maximum of 500 chat and email predefined responses in total.

Note To modify an existing predefined response, click the Title header for the predefined response that you want to modify. To delete an existing predefined response, click the **Delete** icon for the predefined response that you want to delete.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat** > **Predefined Responses**.

The **Predefined Responses web page** opens, displaying the information for existing responses, if any.

Step 2 Click the **Add New** icon that is displayed in the toolbar in the upper left corner of the window or the **Add New** button that is displayed at the bottom of the window to create a new response.

The **Predefined Response Configuration web page** opens.

Step 3 Specify the following information:

Field	Description
Title	Unique identifier of the predefined response. **Note** The special characters angle brackets (< >), parentheses (( )), double quotation marks (" "), and pipe symbol (|) are not allowed.
Type	Types of media.
Response Description	Description for the predefined response. • Rich Text Editor is available to create an HTML-based email predefined response. Use the supported tags as provided in the Rich Text Editor for formatting purpose. • Plain Text Editor is available to create a chat predefined response. **Note** The special characters angle brackets (< >), parentheses (( )), double quotation marks (" "), and pipe symbol (|) are not allowed in Plain Text Editor for Chat Predefines Response. The maximum characters limit for predefined response for chat and email is 1500. In case of email, rich text is supported and includes the HTML tag characters for representing rich text.
Tags	Choose a tag for the predefined response. • **Global for all CSQs**: The predefined response is available to all the agents that are associated with all the CSQs. • **Customize (Maximum 10 CSQs)**: The predefined response is available only to the agents that are associated with the selected CSQs. If you choose this option, select the CSQs from the **Available CSQs** pane, and then click the left arrow to assign them. **Note** Predefined responses can be used only for emails sent in HTML format and not plain text.

Step 4 Click **Save**.

The newly added predefined response appears with the assigned tags in the **List of Predefined Responses**.

You can sort the predefined responses by title by clicking the Title header and by type by clicking the Type header.

Wrap-Up Reasons

To access the Wrap-Up Reasons, choose **Subsystems** > **Chat and Email** > **Wrap-Up Reasons**.

Use the **Wrap-Up Reasons** page to configure and manage Wrap-Up categories and reasons for chat and email Contact Service Queues (CSQs). Use the Ellipsis (...) to view all the Wrap-Up Reasons that are added for each Wrap-Up category.

Wrap-Up Reasons

Using this web page, you can add, modify, and delete the Wrap-Up Reasons.

You can add a maximum of 25 Wrap-Up categories. If you exceed the maximum number of categories, the **Add New** button is disabled.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat and Email** > **Wrap-Up Reasons**.
The **Wrap-Up Reasons** web page opens, displaying the information for existing Wrap-Up Reasons, if any.

Step 2 Click the **Add New** icon or the **Add New** button that is displayed in the toolbar in the upper left corner of the window.

The **Wrap-Up Reasons** web page opens.

Step 3 Specify the following information:

Field	Description
Category	Specify the name for the Wrap-Up category. Allows up to 40 characters.
Wrap-Up Reasons	Enter the Wrap-Up Reasons for the specified category. Allows up to 40 characters. Click the **Add** button to add up to 25 Wrap-Up Reasons for each category.

Field	Description
Tags	Choose a tag for the Wrap-Up category. • **Global for all CSQs**: The Wrap-Up reason is available to all the agents that are associated with all the CSQs. • **Customize** : The Wrap-Up reason is available only to the agents that are associated with the selected CSQs. If you choose this option, select the CSQs from the **Available CSQs** pane, and then click the left arrow to assign them. **Note** You can associate a maximum of 10 Wrap-Up categories to a CSQ.

Step 4 Click **Save**.

The newly added Wrap-Up category appears with the assigned tags in the **List of Wrap-Up Reasons**.

Note When you reskill or modify a category, the logged in agents can apply Wrap-Up Reasons from the updated list of categories for the new non-voice contacts only.

Email Signatures

To access the email signatures, choose **Subsystems** > **Chat and Email** > **Email Signatures**.

Email Signature Configuration

Using this web page, you can add, modify, and delete email signatures.

Note To modify an existing email signature, click the Title header for the email signature that you want to modify. To delete an existing email signature, click the **Delete** icon for the email signature that you want to delete.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat and Email** > **Email Signatures**.

The **Email Signature web page** opens, displaying the list of existing email signatures that are configured, if any.

Step 2 Click the **Add New** icon that is displayed in the toolbar in the upper left corner of the window or the **Add New** button that is displayed at the bottom of the window to create a new email signature.

The **Email Signature Configuration web page** opens.

Step 3 Specify the following information:

Field	Description
Name	Unique name of the email signature. **Note** The name can have a maximum of 100 characters.
Content	The email signature content. **Note** The email signature can have a maximum of 1500 characters. You may format the text of the email signature content, add images, add URL to the email signature, and add the Agent alias information. The Agent alias variable appears by default when any new email signature is created. If it is removed from the email signature it can be reinserted at the cursor location in the email signature by clicking on the Agent alias variable icon. When there is no alias configured for an agent, the Agent ID is presented in the email signature by default.
Tags	Choose a tag for the email signature. • **Global for all CSQs**: The email signature is available to all the agents that are associated with all the CSQs. • **Customize (Maximum 10 CSQs)**: The email signature is available only to the agents that are associated with the selected CSQs. If you choose this option, select the CSQs from the **Available CSQs** pane, and then click the left arrow to assign them. **Note** Only one (1) email signature can be tagged as Global for all CSQs. A CSQ can be tagged with only one (1) email signature. When an email is responded by an agent of a particular CSQ, the system will check if there is any email signature tagged for that CSQ. The different scenarios are: • If there is an email signature tagged to a CSQ, that will be appended in the email response. • If there is no CSQ specific email signature, the global signature is appended in the email response. • If there is no global email signature and no customized email signature tagged to the CSQ then there will be no email signature appended in the email response.

Step 4 Click **Save**.

The newly added email signature appears with the assigned tags in the **List of Email Signatures**.

You can sort the email signatures by title by clicking the Title header and by type by clicking the Type header.

Channel Parameters

Use the Channel Parameters web page to configure channel parameters.

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat** > **Channel Parameters** OR **Subsystems** > **Chat and Email** > **Channel Parameters** as applicable.

The Channel Parameters Configuration web page opens.

Step 2 Use this web page to specify or modify the following fields for channel parameters:

Field	Description
No Answer Timeout (Seconds)	The time for an agent to respond to the chat request after which, the chat request is routed back to the chat queue and for the chat toaster to fade out. This is applicable for the Group Chat request also. However when the chat is not accepted, the chat request is not routed back to the chat queue. **Note** When you use Chrome or Firefox, the browser overrides the chat toaster notification to fade out in 20 seconds, even if it is configured to a higher value.
Join Timeout (Minutes)	The time after which the customer initiates a chat and, if an agent is not joined, the customer gets a message as per the configuration in the **Chat Web Form Configuration** page. But an agent can still join the chat after this timeout. The default timeout is one minute and the maximum timeout value allowed is 60 minutes.
Inactivity Timeout (Minutes)	The customer inactivity time after which, the system ends the chat. This timeout is on the customer side only. The agent gets a message **"You are alone in the chat room. Click End to close the chat interface."**. The customer gets a message **"Warning: the server connection was lost due to an inactivity timeout or connection failure."**. Inactivity timeout may also apply to contacts in queue that have not yet been accepted by agents. This scenario occurs only when the Join Timeout value is greater than the Inactivity Timeout value. The customer then gets a message **"Sorry, the chat service is currently not available. Please try again later."**
Offer Chat Contact When On Voice Call	Click Yes if agents are allowed to handle a chat session during a voice call. **Note** This setting takes effect when the agent ends the current voice call. Chats are presented to agents even when they go off-hook or busy in a Non ICD call.

Field	Description
Offer Voice Call When On Chat	Click Yes if agents are allowed to handle a voice call during a chat session. **Note** This setting takes effect when the agent receives a new incoming chat. Direct/Consult Transfer to an IPCC extension is an exception. Even if agents are busy on a chat they would still get calls that are transferred to their extension directly.
Maximum Number Of Chat Sessions Per Agent	Number of chat sessions (ranging from 1 to 5) that an agent is allowed to handle. This includes the group chat sessions also. **Note** This option is available only if Finesse service is activated. For Cisco Agent Desktop, the value is set to 1.
Maximum Number Of Email Sessions Per Agent	Number of Email sessions (ranging from 1 to 5) that an agent is allowed to handle. **Note** This option is available only if Finesse service is activated.
Sticky Email Timeout (Hours)	Specify the amount of time for which an email message waits in a specific agent CSQ. Sticky email routing (Last-agent email routing) is a mechanism to route an email message to the agent who handled the last leg of the email conversation. When an email message, which is part of an ongoing conversation, comes in and the agent who handled the last leg of the conversation is not available, then the email does not wait indefinitely in that agent queue. After the configured time expires, the email message is placed on the intended CSQ to be handled by any available agent. **Note** Last-agent email routing is not available if the customer changes the subject line of the email message. Default = 4 hours, Range = 1 to 120 hours. **Note** This option is available only if Finesse service is activated.

Step 3 Click **Save** to save the changes for the channel parameters.

Note If any of the above parameters are changed during the call center operation, the updated values are not applied to the existing contacts in the system. The changed parameters will affect only the new contacts coming into the system.

Chat Widgets

Use the **Chat Widgets** section to configure chat widgets and generate HTML code that can be hosted on the customer website. You can configure and manage the following types of chat widgets:

- Classic Chat

- Bubble Chat

To access the **Chat Widgets** page, choose **Subsystems** > **Chat and Email** > **Chat Widgets**.

Chat Widgets Page

The **Chat Widgets** page lists the following information and options for each chat widget:

Field	Description
Name	Name of the chat widget.
Description	A brief description.
Widget Type	Configured as a Classic Chat or a Bubble Chat.
Post Chat Rating	Whether post chat rating is available for the chat. **Note** Post chat rating can be configured for only bubble chat.
Code	Option to generate the web form code for the configured chat widget.
Delete	Option to delete the chat widget.

Chat Widget Configuration

You can add, modify, and delete chat widgets. You can schedule business hours in the chat widget for week days, custom business days, and holidays. You can also configure an off hours message.

Note

- To modify an existing chat widget, click the chat widget name.
- To delete an existing chat widget, click the delete icon. Ensure that the widget is removed from the customer website before deleting the widget.
- The chat schedule is supported only for classic chat.

You can configure or modify Classic Chat and Bubble Chat widgets.

Bubble Chat Widget

To configure a Bubble Chat widget, complete the following steps:

Procedure

Step 1 From the Unified CCX Administration menu bar, choose **Subsystems** > **Chat and Email** > **Chat Widgets**.

The **Chat Widgets** web page opens, displaying the information for existing chat widgets.

Note During the widget configuration, live preview of the widget is possible.

Step 2 Click the **Add New** icon or the **Add New** button.

The **Bubble Chat Configuration** web page opens. The administrator can configure the messages and labels in any language.

Step 3 In the **Widget Details** area, specify the following information:

Field	Description
Name	Unique name of the chat widget.
Description	Chat widget description.

Step 4 Click **Next**.
The **Attributes - Branding and Identity** area appears.

Step 5 Specify the following information:

Section	Field	Description
Font Family	Typeface	Font family used for the text in the Chat Web Form and chat window. **Note** The default font family is Helvetica. You can change the font family by either selecting from the drop-down or entering a new name. If the selected font family is not available in the system where from the AppAdmin page is accessed, it will display an alert message. When you enter a new name, ensure that the correct spelling (case sensitive) is used. The system does not indicate if you enter an invalid name. Ensure that you use commonly available fonts so as to make it easy for the customers to view the information. Before proceeding, the administrator should ensure that the selected font family is applied on the Chat Web Form preview.
Chat Title	Text	Title text displayed on the Chat Web Form and Chat Bubble.
	Text Color	Color of the title text.
Button	Text	Text displayed on the button of the Chat Web Form.
	Color	Color of the button.
	Text Color	Color of the text displayed on the button.
Agent Message	Message Color	Background color of the agent message in the chat window.
	Text Color	Color of the agent message text.

Note As you specify the attributes, the **Preview** area dynamically displays the preview of the Chat Web Form and chat window based on your specifications.

Step 6 Click **Next**.
The **Attributes - Post Chat Rating** areas open.

Step 7 Specify the following information:

Field	Description
Enable Post Chat Rating	If this checkbox is checked, post-chat rating will be available for the chat. The **Post Chat Rating** column in the **Chat Widgets** page indicates whether post chat rating is available for a chat.
Label	Text asking the user to rate the chat experience.
Button Text	Text displayed on the button that is used to submit the rating.

Note The **Preview** area dynamically displays the preview of the rating window based on the information specified.

Step 8 Click **Next**.
The **User Form Fields** and **Problem Statements and CSQ Mapping** areas open.

Step 9 In the **User Form Fields** area, specify the following information:

a. In **Context Service Fieldsets**, enter valid fieldsets for configuring the chat widgets.

Note
- Fieldsets are comma separated strings in the format fieldset1, fieldset2 (for example: cisco.base.pod,cisco.ccx.pod). You can enter a maximum number of 10 fieldsets.
- All the selected User Form Fields except Name and Email must be part of the fieldsets specified, otherwise Context Service operations for chat would fail.
- To perform Context Service Lookup Customer for chat, the Email field is mandatory in the chat form.

b. From **Available Fields**, select the desired fields and move it to **Selected Fields**.

To create new fields in addition to the list of available fields, click **Add Custom Field**, enter the name of the new custom field in the pop-up window and click **OK**. The new custom field appears in the list of **Selected Fields**.

Step 10 In the **Add problem Statement CSQ mapping** area, specify the following information:

a. In **Problem Statement Caption**, enter the label for the problem statement field.

b. Enter the problem statement for the Chat Web Form and map the problem statement with an existing chat CSQ from the **CSQ List** drop-down list.

To add more problem statements and associate them with a chat CSQ, click **Add More**. Click the delete icon for a problem statement to delete that problem statement.

Step 11 Click **Next**. The **Chat Messages** area appears.

Step 12 Specify the following information:

Section	Field	Description
Initialization Messages	Widget Wait Message	Message displayed to the customer when the customer submits the chat form and waits for an agent to join.
	Join Time-out Message	Message displayed on the chat window to inform the customer that no agent is available currently.

Section	Field	Description
In Progress Messages	Text for Text Typing Box	Text directing the customer to enter a message. This text appears in the text box of the chat window where the customer enters messages to be sent.
	Agent Joined Message	Message displayed on the chat window to inform the customer that an agent has joined. This message has the Agent Alias or Agent ID. Two text boxes are available to enter text to be displayed before and after the Agent Alias or Agent ID.
	Agent Left Message	Message displayed on the chat window to inform the customer that the agent has left. This message will have the Agent Alias or Agent ID. Two text boxes are available to enter text to be displayed before and after the Agent Alias or Agent ID.
End Messages	Close Chat Confirmation Pop-up message	Message displayed on the pop-up window to confirm if the customer wants to close the chat. In the **Negative Response** and **Positive Response** text boxes, enter the text to be displayed on the pop-up window buttons that allows the user to either accept or reject the chat closure.
	Close Chat and Download Transcript Confirmation Pop-up Message	Message displayed on the pop-up window to inform the customer that the chat has ended and the chat transcript is ready for download. In the **Negative Response** and **Positive Response** text boxes, enter the text appears on the pop-up window buttons that allows the user to either accept or reject the transcript download.
Error Messages	System Error Message	Message displayed to the customer when the chat service is not available to handle chat requests.
	Connectivity Error Message	Message displayed to the customer when the chat is disconnected due to inactivity timeout or connection failure.

Step 13 Click **Next**. The **Service Hours** page appears.

Step 14 In **Service Hours** area, select one of the following options to configure the business hours.

- **Default (24 hours x 7 days)-** Select this option if the contact center works 24 hours and 7 days in a week.
- **Select Calendar-** Select this option to configure the business hours. Calendar drop-down is enabled for this selection.

Step 15 Select the desired calendar from the drop-down list and click the **View** link to preview the calendar details such as **Business Hours**, **Custom Business Days**, and **Holidays**.

Step 16 In the **Messages** area, specifiy the following:

Field	Description
Holiday	Message displayed on the bubble chat widget to inform the customer during a holiday.

Field	Description
Off Hours	Message displayed on the bubble chat widget to inform the customer during non-working hours.
Label	Heading text displayed on the bubble chat widget to inform the customer for the business hours details.

Step 17 In the **Label for Days of Week** area, specify a label for each day of the week.

Step 18 Click **Finish**.
The code for the Chat Web Form is generated and appears onscreen.

Note The Chat Web Form that is generated uses JavaScript. You must access this Chat Web Form from a JavaScript enabled browser.

Step 19 Click **Save Code to File** to save the generated code. Click **Back to Chat Widgets** to go to the main **Chat Widgets** page.

Note You can also generate the code from the main **Chat Widgets** page by clicking on the **Code** icon against the chat widget name. The generated code appears on a pop-up window. To save this code, click **Save Code to File**.

Teams

Choose **Subsystems > Chat > Teams** from the Unified CCXAdministration menu bar to access this configuration area.

Note The team configuration for chat is the same as it is for voice.

Change the Desktop Layout

The default desktop layout xml must be modified to enable the digital channel gadgets on the Finesse desktop. You must contact the contact center Administrator to make changes to the desktop layout xml.

Procedure

Step 1 Sign in to **Cisco Finesse Administration Console**.

Step 2 In the **Desktop Layout** tab, you can define the layout of the Finesse desktop .

Step 3 In the Finesse Layout XML area, make changes to the XML as required to include the new gadgets.

Step 4 Click **Save**. Finesse validates the XML file to ensure that it is a valid XML syntax and confirms to the Finesse schema.

Note For more details on managing the Finesse desktop layout see, **Manage Desktop Layout** section in Cisco Unified Contact Center Express Administration and Operations Guide.

Configuration of Proxy Based on Deployment of SocialMiner

Proxy settings must be configured for Cisco SocialMiner based on the deployment type.

Procedure

Step 1 Sign in to **Cisco Unified Contact Center Express Administration**.

Step 2 Navigate to **System Menu** > **System Parameters** to modify the fields in Proxy Parameters.

Note For more details on the System Parameters see, **System Parameters** section in Cisco Unified Contact Center Express Administration and Operations Guide.

Certificate Management

The digital channel gadgets to load on the web browsers in the Unified CCX system must have the self-signed and certificate authority (CA) signed certificates. The same signing authority must sign the certificates of SocialMiner and Unified CCX. For more information on how to trust the self-signed certificates and to obtain and upload CA certificates see, Cisco Unified Contact Center Express Administration and Operations Guide.

Procedure

Step 1 Sign in to **Cisco Unified OS Administration** using your administrator password.

Step 2 Navigate to **Security** > **Certificate Management** menu.

Step 3 You can use the Find controls to filter the certificate list.

Step 4 Click the file name of the certificate. The **Certificate Configuration** window appears and perform the necessary actions.

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 SocialMiner to handle the email and relay the contact requests from a mail server. One SocialMiner 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 2010, 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, SocialMiner uses secure IMAP (for message retrieval) and secure SMTP (for message sending). On the Exchange Server, enable IMAP (SMTP is enabled by default).

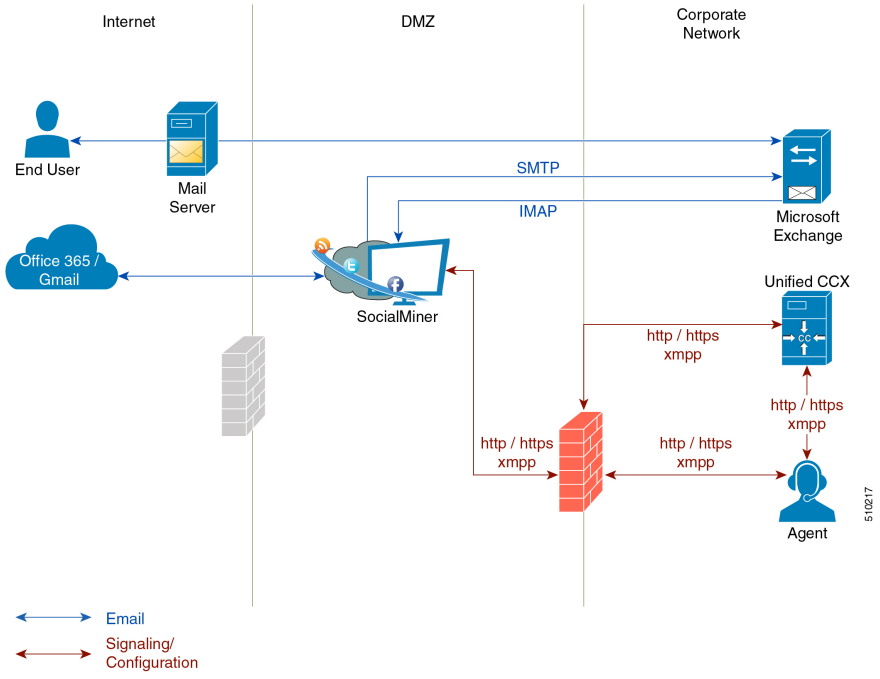
For more information about enabling IMAP, see section “Mail Server Configuration” in *Cisco Unified Contact Center Express Administration and Operations Guide* at:

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 SocialMiner 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 SocialMiner see, https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/211530-Unsupported-configurations-for-UCCX-and.html.

Figure 2: 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 the customer's email, the reply 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 on 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 SocialMiner configured within Unified CCX.

Table 11: Agent Email Features Available with Premium Package

Feature
Fully integrated with Cisco Finesse agent desktop.
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.

Feature
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 has been increased to 20MB. The size limit of a single file attachment has been increased to 10 MB. The total size limit of attachments in the incoming email from the customer has been increased to 20 MB.
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.
Microsoft Exchange. Supported email service. This must be purchased separately by customer.
Context Service Integration for Chat and Email. Integrates the Context Service with chat and email to store Cisco Contact Center customer data with rich contextual information about interactions, thus resulting in a seamless omni channel experience.
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 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.

Feature
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.

Email Enhancements

Few of the email enhancements that are available with the Cisco Finesse Email feature:

- The agent can add and modify the To, Cc, and Bcc recipients in the email reply and forward.
- The agent has an option to click Reply All to send the email response to all the recipients that were initially included in the email
- The agent has an option to forward the email to any other recipient.
- The agent can send and receive email messages with attachments of maximum size upto 20 MB.
- An administrator can create, modify, delete and view email signatures.

  The email signature gets automatically appended to the email response that is sent by the agent.

  In the email signature, the agent details are automatically inserted based on the Agent Alias system variable value. If the Agent Alias value is available, the alias name is inserted. If the alias name is not available, then the Agent ID is inserted in the signature.

  The email signatures are configured and tagged as Global for all CSQs or Customize for selected CSQs. Following are the important criteria while tagging an email signature to CSQs:

  - A CSQ can be tagged with only one email signature.
  - Only one email signature can be tagged as Global for all CSQs.
  - If there are no email signatures configured for a CSQ, there will not be any email signature that gets appended to the email sent by the contact center agent.

Unified CCX Web Chat

As part of the Premium offering, Unified CCX agents can service customer chat requests using the Agent Web Chat Application from the Cisco Agent Desktop or through a standalone browser.

As stated in the overview section, this feature requires a Cisco SocialMiner deployment to accept and relay the contact requests from a customer website. One SocialMiner deployment can serve only one Unified CCX deployment (single node or high availability deployment).

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 12: 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.
Auto chat reject. If no agent is available, the chat request is rejected.
Chat Timeouts. Session timeouts for chat inactivity and maximum wait period.
Typing Indicator. The agent or customer can see when the customer or agent is typing a message.
Audible Alert. An alert is played when the agent receives a new chat request or when there is a new message on an inactive chat session tab.
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.
Chat Transcript. Chat transcripts can be downloaded by the customer after the chat session. Administrators can login to SocialMiner to retrieve chat transcripts.
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.
Integrated Web Chat General System Features with Cisco Finesse Agent Desktop.
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.
Visual Customization of the Chat Form. A customizable customer chat form.

Feature
Business Hours Setting. The Administrator can configure a schedule for the chat web form based on the business days, working hours, and holidays.
Web 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. Web 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, SocialMiner is not supported in HA.
Plain text. Only plaintext chat and predefined responses are supported.

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:

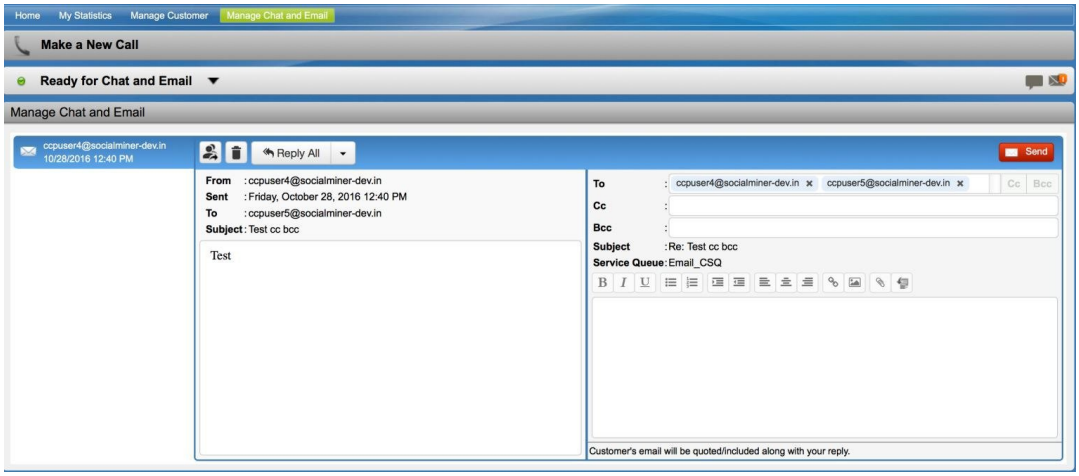
- The Historical reports, **Chat Agent Details Report** and **Chat Agent Summary Report** reflect the chat session information handled by the agents only after the contact is ended.
- In Chat Agent Details Historical report (in the case of group chat):
  - **Chat Routed CSQ** column will show the name 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.

Manage Digital Channels

Manage Chat and Email Gadget

The following figure shows the Cisco Finesse Manage Chat and Email gadget for agents.



The Manage Chat and Email gadget allows you to manage chat and email contacts. Chat and email contacts that are assigned to you appear in tabs on the left. You can click each individual tab to view and reply to the contact.

Chat contacts are denoted by a chat icon. The following information appears on each chat contact tab:

- Customer name
- Total chat time: Indicates the duration of the chat session.
- New message indicator: If you receive a message on a chat contact that is not your current contact, the tab flashes for a few seconds. A number appears on the tab that indicates how many messages the customer sent since you last replied.

Email contacts are denoted by an envelope icon. When you begin typing a reply to the email contact, a pencil icon appears on the envelope icon.

The following information appears on each email contact tab:

- Customer information: Customer email address, customer name (if available).
- Email timestamp: Indicates the time that the system received the email contact.
- Email subject: Hovering the mouse over the email tab, displays the subject of the email in a tool tip.

Note When you accept a chat request, Finesse automatically switches to the Manage Chat and Email tab and the chat becomes the active contact. When you are assigned an email contact, Finesse does not switch tabs and the contact does not become the active contact. An orange icon appears on the envelope icon in the Chat and Email Control gadget.

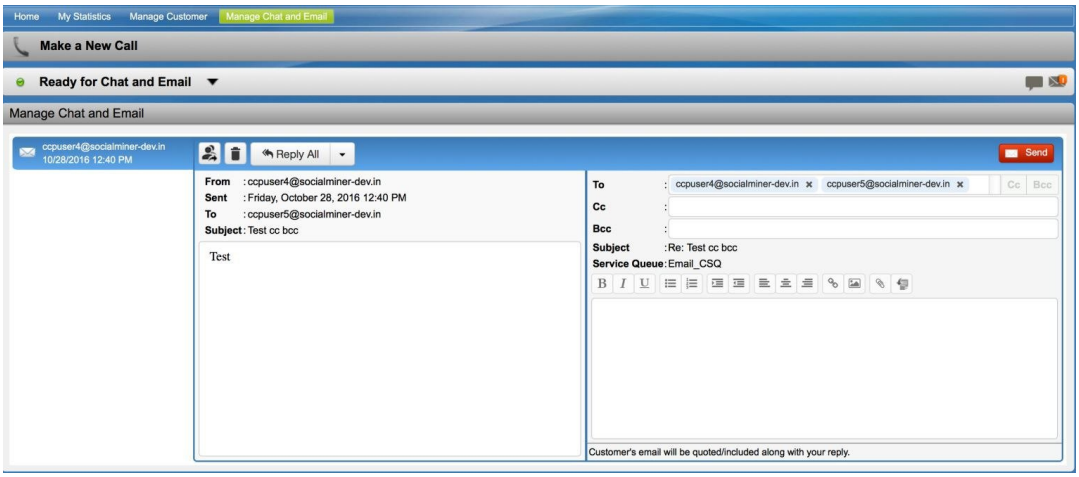
Email Features

Let us see how we can now use the available email features. You can also see the Cisco Finesse Agent and Supervisor Desktop User Guide for Cisco Unified Contact Center Express for more information.

Email Reply Panel

The following figure shows the Email Reply panel of the Manage Chat and Email gadget.

Figure 3: Email Reply panel



The customer email appears on the left. The area where you type the response appears on the right. After you begin your reply, Finesse automatically saves a draft of your message every 3 minutes.

Note Do not close or reload the browser when you reply to an email or when the email loads on the desktop.

The Email Reply panel provides the following functionality:

Button	Name	Description
	Requeue	Requeues an email contact to a new CSQ.
	Discard	Discards an email.

Button	Name	Description
Reply	Reply	Sends a reply to the email address of the customer.
Reply All	Reply All	Sends a reply to the customer and to all other email addresses that the customer had included in the original email.
Cc	Cc	Allows to include other email addresses to send a copy of the email to them.
Bcc	Bcc	Allows to include other email addresses to send a blind copy of the email to them.
Forward	Forward	Forwards an email to other email addresses.
	Bold	Applies bold to the selected text.
	Italic	Applies italics to the selected text.
	Underline	Underlines the selected text.
	Bulleted List	Inserts a bulleted list.
	Numbered List	Inserts a numbered list.
	Increase Indent	Increases the space between the left margin and the content.
	Decrease Indent	Decreases the space between the left margin and the content.
	Align Left	Aligns the content to the left margin.
	Align Center	Aligns the content to the center.
	Align Right	Aligns the content to the right margin.
	Add/Edit Link	Creates or modifies a hyperlink of the selected text to the specified URL.
	Add Image	Adds a specified image to your reply.
	Attach a file	Attaches a specified file to the email reply.

Button	Name	Description
	Predefined Response	Inserts a predefined response into your reply. **Note** If a Predefined Response is not configured, this button is disabled. If the email is in Plain text format, this button is disabled.
	Send	Sends your reply to the customer.

Accept an Email

You must be in Ready state to receive an email contact. When an email contact arrives on your desktop, it is automatically accepted and an orange icon appears on the envelope on the Chat and Email Control gadget.

To view the contact, you must click the **Manage Chat and Email** tab to go to the Manage Chat and Email gadget. If you have more than one contact assigned to you, in the left panel, click the tab for the email contact that you want to view.

Reply to an Email Contact

Procedure

Step 1 On the Manage Chat and Email gadget, click the email contact that you want to reply to.

Step 2 Click **Reply/Reply All** to reply to the email address of the customer or to any other email addresses copied by the customer. You may modify or add email addresses in the **To** field. You may also include **Cc** and **Bcc** to include more email addresses by clicking the respective fields.

The maximum number of recipients allowed per field (**To**, **Cc**, and **Bcc**) is 20.

Step 3 In the Email Response area, enter your response to the customer.

You can use a predefined response or type your own response.

Note If you select a predefined response, the existing content of the reply is overwritten by the predefined response text.

If **Email Signature** is configured, it gets appended at the end of the email before sending. The Email Signature is not visible to the sender.

Step 4 When you are finished, click **Send**.

Forward an Email

Procedure

Step 1 On the Manage Chat and Email gadget, click the email contact that you want to reply to.

Step 2 Click **Forward** to forward an email to add any other email addresses that you may want to send the email to. You may modify or add email addresses in the **To** field. You may also include **Cc** and **Bcc** to include more email addresses by clicking the respective fields.

Note
- The maximum number of recipients allowed per field (**To**, **Cc**, and **Bcc**) is 20.
- No further attachments can be attached to the outgoing emails.
- The **Reply To** field is modified appropriately such that the recipient of the forwarded email can reply to the original sender of the email directly and not send it back to the Contact Center.
- The **Requeue** is disabled if you have initiated to forward the email. You must cancel **Forward** and click **Reply/Reply All** to requeue the email.

Step 3 In the Email Response area, enter your response.

You can use a predefined response or type your own response.

Note If you select a predefined response, the existing content of the reply is overwritten by the predefined response text.

If **Email Signature** is configured, it gets appended at the end of the email before sending. The Email Signature is not visible to the sender.

Step 4 When you are finished, click **Send**.

Download Customer Attachments

If a customer includes attachments in an email, the attachment file names appear under the subject of the email. Finesse imposes the following limitations on customer email attachments:

- The total number of attachments cannot exceed 10.

Note Images within the body of the email are counted as attachments.

- The size of a single attachment cannot exceed 2 MB.
- The total size of all attachments cannot exceed 5 MB.

Procedure

Step 1 Click the filename of the attachment you want to open or download.
You are prompted to open or save the file.

Step 2 Choose whether to open the file or save the file to your computer.

Step 3 Repeat Step 1 and Step 2 for each attachment that you want to open or download.

Add a Hyperlink to an Email

Procedure

Step 1 In your email reply, select the text that you want to turn into a hyperlink.

Step 2 Click the **Add/Edit Link** button.
A dialog box opens where you can enter the URL for the link.

Step 3 In the **Please enter a URL to insert** box, enter the URL for the link.

Step 4 Click **OK**.

Add an Image to an Email

Procedure

Step 1 Place your cursor where you want the image to appear.

Step 2 Click the **Add Image** button.
A dialog box opens where you can enter a URL for the image.

Step 3 In the **Please enter a URL for the image** box, enter the URL.

Step 4 Click **OK**.
The image appears inline in the email response.

You can also copy and paste an image into the email response.

Add an Attachment to an Email

You can add up to 10 attachments to an email reply to a customer. The following limitations apply:

- The size of a single attachment must not exceed 2 MB.
- The total size of all attachments must not exceed 5 MB.

Procedure

Step 1 Click the **Attach a file** button.

Step 2 Navigate to the file that you want to send attach to the email.

Step 3 Click **Open**.
The file appears below the reply panel.

Step 4 Repeat Step 1 and Step 2 for each file that you want to attach (up to 10).

If you want to remove an attachment, click the **X** to the right of the attachment filename.

Requeue an Email Contact

You can transfer an email contact either to the same Contact Service Queue (CSQ) or to any other CSQ. After you initiate the transfer from the agent desktop, the contacts are requeued to a CSQ.

Last-agent email routing is a mechanism to route an email message to the agent who handled the last leg of the email conversation. When you requeue an email, the email will be routed to the intended CSQ to be handled by any available agent, and last-agent email routing is not considered.

Note The requeued contact is not requeued to the same agent even if the agent is part of the requeued CSQ and is available to handle more contacts.

When you sign out or refresh your browser, any contacts that you were handling are disassociated from you and requeued to the same CSQ.

Procedure

Step 1 Select the email that you want to requeue.

Step 2 Click the **Requeue** button.
The list of CSQs is displayed with a search option.

Step 3 Type the CSQ name into the **Search** box to bring up the desired CSQ or select the CSQ from the list.
A confirmation dialog appears.

Step 4 Click **Yes** to confirm.

The email is removed from the multiple email sessions panel and requeued to the selected CSQ.

Discard an Email Message

Procedure

Step 1 On the **Manage Chat and Email** gadget, select the email message that you want to discard.

Step 2 Click the **Discard** button on the Email Reply panel.

You are prompted to discard the selected email message.

Step 3 Click **Yes** to confirm.

The email message is discarded.

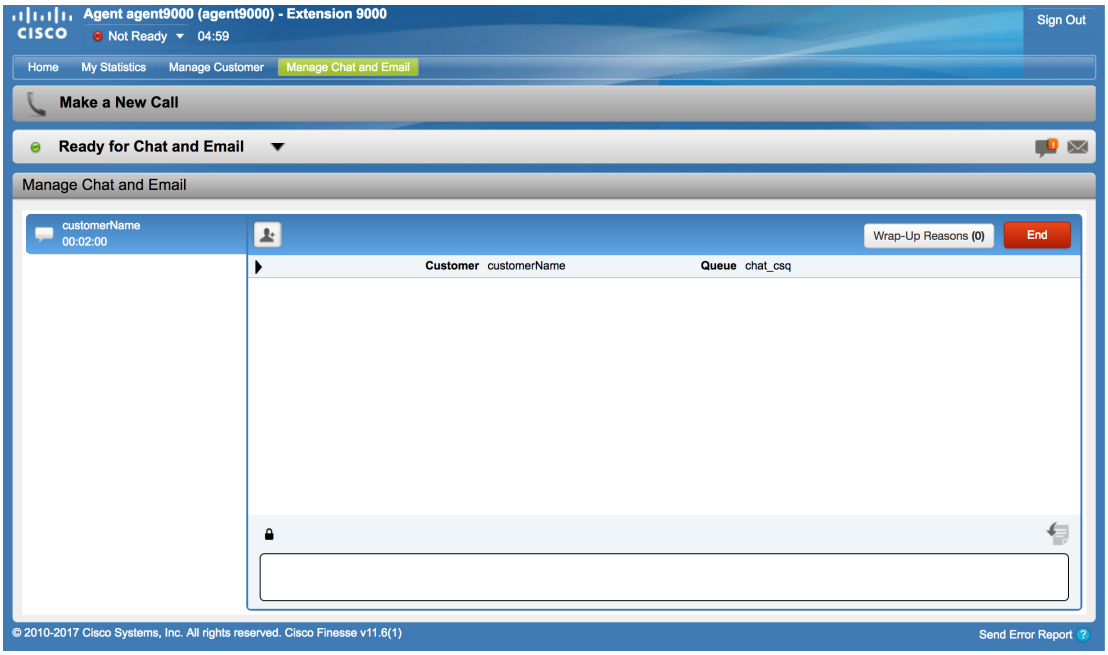
When you discard an unsent reply that has attachments, the draft of the reply from the agent and the attachments are deleted. The original email message sent by the email contact remains in the Exchange mailbox.

Chat Features

Chat Interaction Panel

The following figure shows the Chat Interaction panel of the Manage Chat and Email gadget.

Figure 4: Chat Interaction Panel



The Chat Interaction panel provides the following functionality:

- Typing area: Type your message in the typing area. Right-click to perform basic clipboard operations, and to check spelling.
- The typing awareness indicator shows when the other participant is typing.
- Group Chat icon: Allow you to initiate a group chat with another agent or supervisor.
- Group Chat invite appears for the agent to accept or decline the invite.

- In Group Chat, an agent can click **Leave** to leave the group chat whenever required.
- Predefined responses: Click to select a predefined response from the list. When you insert a predefined response, it is placed at the position of your cursor.
- End chat session: Click **End** to end a chat session.
- Customer details area: Click the drop-down arrow next to the customer details to minimize or maximize this area.

Accept a Chat

When a customer initiates a chat session from a website, Unified CCX Web Chat:

- Sends incoming chat to an available agent.
- Plays an audio alert (For a, new chat request and new message on an inactive chat).

Note With multiple chat session tabs, the selected chat session tab is considered as active. All other chat session tabs are considered as inactive.

- Displays contact details of the customer.

When a customer initiates a chat from Facebook Messenger, Unified CCX Web Chat:

- Prompts agent to accept chat before the time counter expires.

You are presented with incoming chats until you reach the maximum active chat sessions that are set by administrator.

Procedure

Step 1 Click **Accept** in the incoming chat bar within the specified time to accept the chat.

If this is the first chat, the Manage Chats gadget opens, the chat session starts, and you are connected to the customer.

Note Repeat Step 1 when you are presented with a new incoming chat.

A new tab opens for the chat session and new chat session becomes the current session.

Step 2 To end the chat session, click **End**.

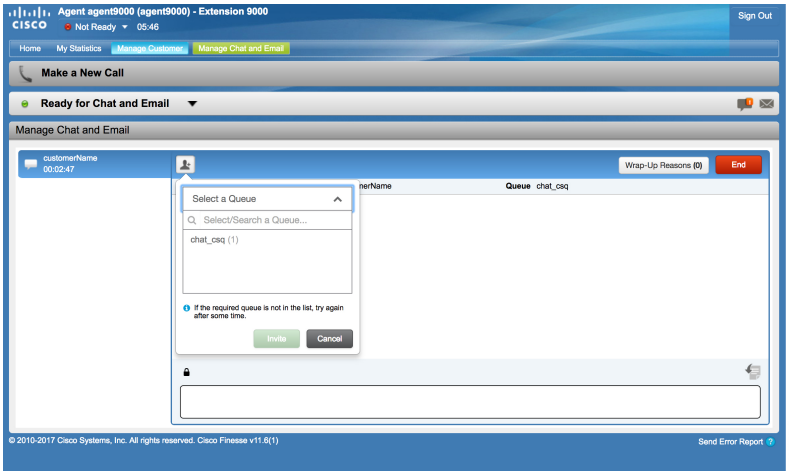
Initiate a Group Chat

You can initiate a Group Chat when you wish 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 you to:

- Send a chat invite to an available agent of the selected CSQ.

  The CSQ names are displayed with the number of available agents in that CSQ.
- Enter the summary of the ongoing chat for the invited agent. This helps the invited agent to understand the context of the ongoing chat.

Figure 5: Initiate Group Chat Invite Interface



Procedure

Step 1 Click **Group Chat** icon to initiate a group chat with another agent or supervisor.

Step 2 **Select a Queue** from the list to invite any available agent to join the chat session.

Step 3 You may enter a summary of the chat in the **Enter Notes** text box. This helps the invited agent to know the context of the chat. This is optional.

Note The summary notes are visible only when the first agent enters the notes when the chat session was initiated.

The notes entered by the invitee is displayed only to the invited agent.

Step 4 Click **Invite**.
The available agent gets a notification to **Accept** or **Decline** the chat. When an available agent accepts the group chat, the three participants (the two agents and the customer) may exchange information in the chat window.

Step 5 To leave the chat session, click **Leave**.

When there is only one agent and the customer in the chat session, the chat can be ended by the Customer or the Agent by clicking **End**.

Accept a Group Chat

You will receive an incoming group chat notification on the Finesse desktop. You may see the notes of the ongoing chat along with the invite. This helps you to understand the issue for which the group chat was initiated by the inviting agent.

Procedure

Step 1 Click **Accept** when you see the new group chat notification to join the chat session.

The agent can see chat history upto 100 messages after joining the group chat.

Step 2 You may now exchange information with the other two participants (inviting agent and the customer).

Note

- The **Group Chat** icon is disabled till the time there are two agents in the ongoing chat. Only when one agent chooses to leave the chat session, the **Group Chat** icon will be enabled again. The agent who wishes to leave the chat session may choose to click **Leave**. The agent who is still active in the group chat session can initiate another group chat by following the steps detailed in the **Initiate a Group Chat** section.
- The maximum number of participants in a Group Chat including the customer is three (3).
- The notes are not persisted for any subsequent chat sessions with the same customer.

Decline a Group Chat

You will receive an incoming group chat notification on the Finesse desktop. You may also see a summary of the ongoing chat along with the invite. This will help you to know the issue for which the group chat was initiated by the inviting agent.

Procedure

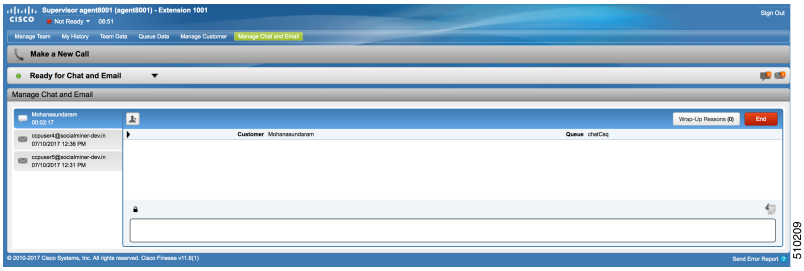
Click **Decline** when you see the new group chat notification to decline the chat invite.

Note The agent who declined the group chat invite is not offered any successive group chat invites for the same chat session till another agent accepts a group chat invite for the same chat session.

Apply Wrap-Up Reasons for Chat and Email

Wrap-Up Reasons are the logical explanations that you can apply when you wrap up the chats and emails handled by you. If your administrator has assigned Wrap-Up Reasons for you, the Wrap-Up Reasons appear in the drop-down list that can be selected. If there are no Wrap-Up Reasons configured by the administrator, it appears blank.

Wrap-Up Reasons that your administrator modifies is available only to the new contacts and not for the contacts that you are currently handling.



Procedure

Step 1 Click **Wrap-Up Reasons(0)**.

In a chat interaction panel you see the **Wrap-Up Reasons(0)** beside the **End** and in a group chat interaction panel beside the **Leave**. In an email reply panel, this is found beside the **Send**. The number in brackets indicates the count of Wrap-Up Reasons selected. This dynamically changes based on your selection.

Step 2 Select the appropriate Wrap-Up Reasons from the drop-down list.

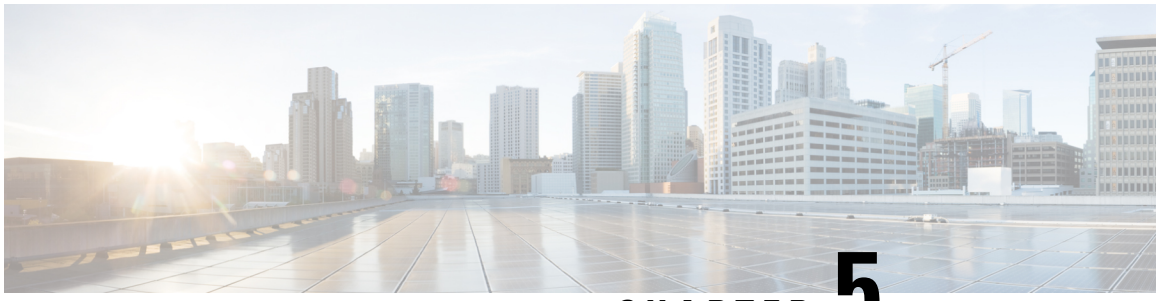
Step 3 Click **OK** to close the Wrap-Up Reasons selection pane.

You can change your selection at any time. Click **Wrap-Up Reasons(0)**; to open the Wrap-Up Reasons selection pane. You can select a maximum number of five (5) Wrap-Up Reasons.

Digital Channel Reports

There are multiple historical and live data reports that provide information on the digital channels. The reports provide agent detail, agent summary, CSQ activity, CSQ agent summary in context to the digital channels.

All the historical and live data reports are available at the following location, https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html.



CHAPTER 5

Desktop Chat

Desktop Chat

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

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

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

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

Cisco Instant Messaging and Presence (IM&P)

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

Cisco IM&P supports multiple forms of clustered deployment to provide high availability.

Identity, Presence, Jabber

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

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

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

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

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

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

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

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

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

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

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

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

Example for Desktop Chat availability:

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

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

Cisco IM&P Deployment Considerations

Finesse is configured to the primary and secondary IM&P chat servers through the Cisco Finesse Administration interface.

Desktop Chat automatically discovers the appropriate IM&P node, configured for the user, by connecting to the configured servers and connects to the appropriate nodes in IM&P. This resolution is only performed for the first time chat is loaded and subsequently uses the same nodes, until the browser cache is cleared by the user.

Note Desktop Chat does not use DNS_SRV* records unlike Jabber and cannot automatically configure itself based on the network configurations. The explicit chat URI configuration from Administrative pages is required for chat server discovery.

For details on Cisco IM&P deployment, see Unified CM Solution Reference Network Design guide at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12/presence.html.

See Configuration and Administration of the IM and Presence Service on Cisco Unified Communications Manager guide for details about the following:

- How to install and configure IM&P services.
- How to configure IM&P to enable chat services for end users.
- How to configure clusters and high availability deployment.
- How to configure IM&P Federation.

Cisco IM&P Design Considerations

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

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

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

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

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

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

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

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

Bandwidth and Latency Considerations for Cisco IM&P

Cisco IM&P service is closely integrated with Unified CM and it depends on Unified CM for user management and service enabling and authentication.

Cisco IM&P can be deployed as a cluster to guarantee availability and the users must be pre-configured to specific node pairs within the cluster. Details of Cisco IM&P installation and cluster deployment can be found here https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

For more details on the latency requirements for IM&P server refer, Unified CM SRND at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.

The maximum latency supported between Finesse and IM&P nodes is 200 ms.

Cisco IM&P High Availability Considerations

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

Desktop Chat Failover

The following table lists the desktop chat failover scenarios:

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

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

Desktop Chat Server Settings

Desktop Chat is an XMPP browser based chat, which is powered by Cisco Instant Messaging and Presence (IM&P) service. It provides presence and chat capabilities within the Unified CM platform. For more details, see *Configuration and Administration of the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Desktop Chat connects to Cisco IM&P servers over port 5280 from the browser hosting the agent desktop. IM&P server visibility and port accessibility needs to be ensured if clients intend to use this feature. The Desktop Chat gadget configures the IM&P host BOSH URL's used by the desktop to communicate with the IM&P server over BOSH HTTP.

IM&P has a clustered design, where users are distributed across multiple nodes in the cluster. The Desktop Chat initially discovers the IM&P nodes that a user has configured, caches this information and communicates with the actual server for subsequent login, until the browser cache is cleared. To spread the initial discovery load, it is advisable to configure the nodes in a round robin fashion if the deployment has more than one Finesse cluster. For example, if there are 5 IM&P nodes configure Finesse cluster A with node 1 & 2, Finesse cluster B with nodes 3 & 4, and so on.

Node availability should be considered while configuring the IM&P URL. The secondary node will be available for discovery in scenarios where the first node is not reachable. The secondary node will be connected for discovery only if the primary node is unreachable.

For the URL to be configured, refer Cisco Unified Presence Administration service, in *System, Service Parameters*. Choose the required IM&P server, select Cisco XCP Web Connection Manager. The URL binding path is listed against the field *HTTP Binding Path*. The full URL to be configured in Finesse is `https://<hostname>:5280/URL-binding-path`.

Use the Desktop Chat Server Settings to configure chat settings for the Finesse desktop. The following table describes the fields on the Desktop Chat Server Settings gadget.

Field	Explanation
Primary Chat Server	Enter the IM&P primary server URL of Desktop Chat.
Secondary Chat Server	Enter the IM&P secondary server URL of Desktop Chat.

Actions on the Desktop Chat Server gadget:

- **Save:** Saves your configuration changes
- **Revert:** Retrieves the most recently saved server settings

Important For Desktop Chat to work without any issues, ensure the following services are running on IM&P:

- Cisco Presence Engine
- Cisco XCP Text Conference Manager
- Cisco XCP Web Connection Manager
- Cisco XCP Connection Manager
- Cisco XCP Directory Service
- Cisco XCP Authentication Service
- Cisco XCP File Transfer Manager

Note Desktop Chat requires the Cisco IM and Presence certificates to be trusted. To start the Desktop Chat without experiencing an exception, you must add the certificate to the browser trust store, or configure IM and Presence with CA-signed certificate, or push self-signed certificate through group policies in supported browsers. For more information on accepting certificates, see the *Accept Security Certificates* section, in the *Common Tasks* chapter of *Cisco Finesse Agent and Supervisor Desktop User Guide for Cisco Unified Contact Center Express* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html.

For more information on adding certificates to the browser trust store, see Certificate Management.

Use Desktop Chat

The Desktop Chat allows agents or supervisors to chat internally with other users on the Finesse desktop and with users outside the contact center. The agent state on the Desktop Chat is different from the Voice or Digital Channels state.

For more details on how to sign in to Desktop Chat, managing contacts, groups, the chat window, how to change state for Desktop Chat, and how to sign out of Desktop Chat see, .

Sign In to Desktop Chat

Procedure

Step 1 In the Finesse desktop, click the Desktop Chat icon ( ).

Step 2 Enter your username and password in the appropriate fields and click **Sign In**.

Step 3 **Note** If you are using self-signed certificates, you get the certificate acceptance window.

Click the certificate link. A new browser tab opens for the certificate that you must accept. A certificate error appears in the address bar.

- To accept the certificates in Internet Explorer, refer to the section *Accept Security Certificates* > *Step 2* > *Substep d* onward.
- To accept the certificates in Edge, refer to the section *Accept Security Certificates* > *Step 3* > *Substep d* onwards.
- To accept the certificates in Firefox, refer to the section *Accept Security Certificates* > *Step 4* onwards.
- To accept the certificates in Chrome, refer to the section *Accept Security Certificates* > *Step 5* onwards.

Note The **Accept Security Certificates** topic is in the *Cisco Finesse Agent and Supervisor Desktop User Guide for Cisco Unified Contact Center Express*.

Add Contact

If you have Cisco Jabber on your desktop, then the first time you sign in to Desktop Chat, you will see your Cisco Jabber contact list in the Desktop Chat window. If you do not have Cisco Jabber, your contact list will be empty.

Procedure

Step 1 To add a contact:

- In the empty contact list, enter the agent name or ID in the **Search** field.

  Note When you enter the text to search, the Search field pre populates relevant results in a drop-down. From the results list, hover over the required contact and click the icon.

- In the existing contact list, click the icon at the end of the group and click **Add**.
- From the **Recent Chats** group, click the icon at the end of the required chat and click **Add**.

Step 2 In the **Add Contact** window, you can choose to change the display name.

Step 3 From the **Add to Group** drop-down, either choose an existing group or create a new group to add the contact.

Step 4 Click **Add**.
The contact is added to your existing or newly created group.

Edit Contact

Use this option to change the contact name or contact group.

Procedure

Step 1 In the Contact list, click the ••• icon at the end of the required contact.

Step 2 From the drop-down, click **Edit**.

Step 3 In the **Edit Contact** window, modify the display name or the group.

While modifying the group for the contact, you can either add the contact to existing groups or create a new group.

Step 4 Click **Save**.

Move Contact

Use this option to move a contact to a different group.

Procedure

Step 1 To move a single Contact:

a) Click the ••• icon at the end of the required contact.
b) From the drop-down, click **Move**.
c) In the **Select Destination** window, select an existing group or create a new group.
d) Click **Move**.

Step 2 To move multiple contacts:

a) Press and hold the **Ctrl** key and select the required contacts.
b) On the Contact list header, click **Move**.
c) In the **Select Destination** window, select existing groups or create a new group.
d) Click **Move**.

Delete Contact

Use this option to delete a contact. If the contact is part of multiple groups, it is removed only from that group and not from the other groups.

Procedure

Step 1 To delete a single contact:

a) In the Contact list, click the ••• icon at the end of the required contact.
b) From the drop-down, click **Delete**.
c) In the confirmation prompt, click **Delete** to remove the contact from that group.

Step 2 To delete multiple contacts:

a) Press and hold the **Ctrl** key and select the required contacts.
b) On the Contact list header, click **Delete**.
c) In the confirmation prompt, click **Delete** to remove the contact from that group.

Edit Group

Use this option to change the group name.

Procedure

Step 1 In the contact list, click the ••• icon at the end of the required group.
Step 2 From the drop-down list, click **Edit**.
Step 3 In the **Group** window, modify the group name.
Step 4 Click **Save**.

Delete Group

Use this option to delete a group.

Procedure

Step 1 In the Contact list, click the ••• icon at the end of the required group.
Step 2 From the drop-down, click **Delete**.
Step 3 In the confirmation prompt, click **Delete**.
The group is removed with all the contacts in it.

Chat Window

When you receive an incoming chat request, a chat window pops up with the display name of the agent in the chat window header. If the Cisco Finesse desktop window or tab is inactive, Finesse displays a notification with the chat details. Click the toaster notification to restore the Cisco Finesse desktop.

You can move the chat window to any location on the screen but cannot maximize it to the full screen.

Note You can chat with agents logged in to the Desktop Chat. You cannot send messages to the signed out agents.

The Desktop Chat window provides the following functionalities:

- Typing area: Type your message in the typing area. Right-click to perform basic clipboard operations.

- The typing awareness indicator shows when the other participant is typing.
- Multiple chats:
  - All agents are displayed in the chat tabs at the bottom of the chat window.
  - The chat tab area displays up to three active chats. To view more than three active chats, click the » icon.
  - For each chat tab, the unread chat notification is shown in a badge next to the display name. The badge disappears when that chat tab is active.
  - When you hover over the status on any chat tab next to the display name, you get the option to close that chat tab.
- Click the chat window header to minimize or maximize the chat window.
  - When minimized, the chat window header shows the total number of chats that have unread messages.
  - Click **X** on the chat window header and confirm to close all chats.
- Chat history: The Desktop Chat window stores the chat history only for a particular session. If you sign out or the browser is refreshed or closed, the chat history is lost.
- Resize chat window: Click the  button on the chat window header to increase the chat window frame size and the  button to restore the frame size.
- Attachments:

Note The administrator should have enabled attachment support for you to send and receive attachments.

  - To send an attachment:
    1. Click the **Send a file** button and navigate to the file you want to send.
    2. Click **OK**.
  - When you receive an attachment, you are prompted to Accept and Decline the attachment. Click **Accept** to download the attachment or click **Decline** to reject it.
    - The file name and file size are displayed in the attachment header.
    - The attachments are downloaded in the downloads folder of the browser.
    - You cannot open the attachment from the chat window.
    - The supported file types and maximum attachment size are configured by your administrator.

Note You can send or receive attachments only from the users using Desktop Chat.

Change Your Desktop Chat State

When you sign in to the Desktop Chat, your state is set to Available by default. To change your state:

Procedure

Step 1 Click the drop-down arrow beside your current state in the Desktop Chat window.

Step 2 Choose the appropriate state from the list.

Note If your status in set to Do Not Disturb and you receive a chat message, the message is displayed only if your chat window is active. If the chat window is closed or minimized, the Desktop Chat icon blinks and you will only see the minimized chat window header with the number of chat tabs that have unread messages.

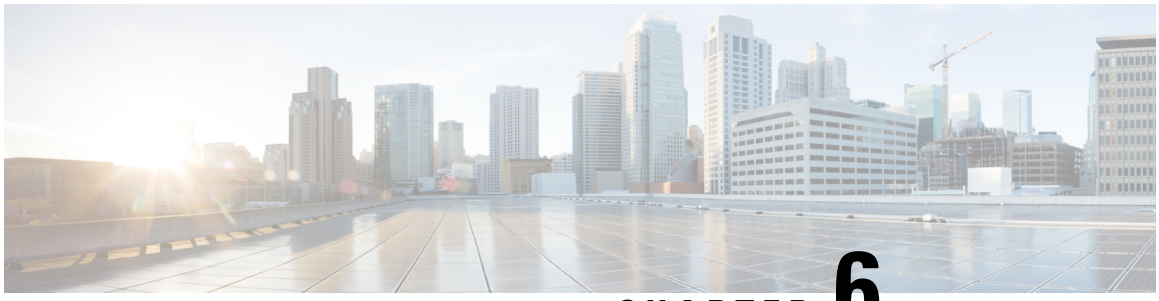
Sign Out of Desktop Chat

When you sign out of the Desktop Chat, you will only be signed out from the Desktop Chat and not the Voice or Digital channels. Your Voice and Digital Channels state remains the same. To sign out:

Procedure

Step 1 Click the drop-down arrow beside your current state in the Desktop Chat window

Step 2 From the displayed list, click **Sign Out**.



CHAPTER 6

Team Message

Overview

Team Message is introduced in Finesse for enabling quick communication within the organization. It enables supervisors to broadcast short messages, which are displayed on agents desktop.

Note Customers who upgrade with existing layouts, need to add this component manually from the Default Desktop Layout.

Key Features

Key features of Team Message are as follows:

Role	Features
Administrator	Enable/Disable Team Message on supervisor desktop.
Supervisor	• Send messages to a single team, multiple teams or all the teams that they manage. • View and delete broadcasted messages. • Set a time frame for a message to be displayed. After expiry of the set time, the message is not displayed.
Agent	• View Team Message banner in real time to stay up-to-date with the latest broadcasts. • Scroll through the list of broadcasted messages.

Note During failover, team message and failover banners are displayed together.

Use Team Message

Send Team Message

The Team Message feature allows you to create and send a broadcast message to one or multiple teams. The message appears as a banner across the Finesse desktop and agents can view these messages in real-time. Team Message will be available on your Finesse desktop only if the administrator has configured this feature for you.

Procedure

Step 1 In the Finesse desktop, click the **Team Message** icon.

Step 2 In the **Compose Message** box, enter the broadcast message (maximum number of characters allowed is 255).

Step 3 Select the team or teams to send the message by checking the check box next to the team name.

Note You can send multiple messages to a single team, multiple teams, or all teams.

Step 4 From the drop-down, you can set an expiry time for the composed messages: starting at 5 minutes and ending at 23:55 hours. The time is displayed in hours and minutes. However, this time frame can be edited.

Step 5 Click **Send**.

You can view the latest messages sent by clicking **Show recent messages**. If you wish to delete any or all messages, check the check box next to the message. Click **Delete** and confirm the deletion.

The message is removed from active display and the previous non-expired team message will become the active message for the agent.

Note Administrator or supervisor who creates a Team Message can delete the created Team Message through `TeamMessage` API. For more information on deleting a TeamMessage, see https://developer.cisco.com/docs/finesse/#teammessagedelete-a-team-message.

Note The rate at which messages (create/delete) are published to the teams involved, is capped at per hour and the maximum number of active messages allowed is . If the limit of active messages is reached, supervisors will not be able to broadcast new messages until an existing team message is deleted or it expires.

As there are no individual limitations on supervisors, either one or all supervisors can broadcast messages up to the maximum active messages limit.

View Team Message

On logging in to the Finesse desktop, you can view the Team Message banner which broadcasts the active team updates sent by your supervisor in real-time. The total number of active messages sent by your supervisor is displayed in the banner. By clicking the number, you can view the latest message with the name of the supervisor and the timestamp being displayed against each message.

You can toggle between the active messages (note that messages expire after a time frame, as set by the Supervisor).

If the Finesse desktop is inactive, a toaster notification appears when a new team message is sent by the Supervisor. You can click the notification to view the message.

Note During failover, the team message banner and the failover banner will be displayed together.