Common Tasks

Change Your State

When you sign in to Cisco Finesse desktop, by default your state is set to Not Ready. This is applicable to both voice and digital channels.

You can set your state to Ready or you can choose from one of the configured Not Ready reasons.

While you are on a call, chat or replying to an email, you can select and apply a state when you complete the task.

Change Your State for Voice Channels

When you sign in to Cisco Finesse desktop, by default your state is set to Not Ready. To accept incoming call, you must set your state to Ready.

When you answer a call, you can change your state after you complete the call. If Wrap-Up is required, when a call ends you transition to Wrap-Up state. While in Wrap-Up state, you can complete any after call work. If Wrap-Up is optional, you can select Wrap-Up while on call to transition to Wrap-Up state when the call ends.

To end the Wrap-Up state, you must select your new state from the drop-down or wait for the preconfigured timer to expire.

Procedure

Step 1 Click the drop-down besides your current state.

Step 2 Select the appropriate state from the list.

Your agent state changes to reflect your new selected state. If you select change of state while you are still on call, the state change will reflect after you complete the call.

Change Your State for Digital Channels

When you sign in to the Finesse desktop, your state is set to **Not Ready** by default.

If you are in Ready state, you can set your state to Not Ready.

To accept incoming chat and email contacts, you must set your state to Ready.

Procedure

Step 1 Click the drop-down arrow beside your current state.

Step 2 Select the appropriate state from the list.

Browser Settings for Internet Explorer

To ensure all features of Finesse work properly on the Internet Explorer, you must:

1. Disable pop-up blockers.
2. Configure the following privacy and advanced settings:
    1. From the browser menu, select **Tools** > **Internet Options**.
    2. In the **Privacy** tab, click **Sites**.
    3. In the Address of website box, enter the domain name for the Side A Finesse server.
    4. Click **Allow**.
    5. In the Address of website box, enter the domain name for the Side B Finesse server.
    6. Click **Allow** > **OK**.
3. Enable the following security settings to allow users to sign in:
    - Run ActiveX controls and plug-ins
    - Script ActiveX controls marked as safe for scripting
    - Active scripting

To enable these settings:

1. From the Internet Explorer browser menu, click **Tools** > **Internet Options**.
2. In the **Security** tab, click **Custom level**.
3. Under ActiveX controls and plug-ins, select **Enable** for **Run ActiveX controls and plug-ins** and **Script ActiveX controls marked safe for scripting**.
4. Under Scripting, select **Enable** for **Active Scripting**.

Note If the customer is using self-signed CA (Certificate Authority) and their agents use the server's FQDN, there should not be any certificate errors or warnings when connecting to Finesse over HTTPS.

Browser Settings for Firefox

Complete the following steps to ensure Finesse responds as expected when it is not the active window:

Procedure

Step 1 Open Firefox and enter **`about:config`** in the address bar.

Step 2 On the warranty page, click **I accept the risk!**.

Step 3 In the **Search** field, enter `dom.disable_window_flip`.

Step 4 Double-click **dom.disable_window_flip** to set the value to *false*.

Step 5 Restart Firefox.

Sign In to Cisco Finesse Desktop

Note Extension Mobility brings a user-specific phone profile (including configured extensions for that user) to the phone being logged in from. After logging in to Cisco Unified Communications Manager with Extension Mobility, agents can log in to Unified CCX using Finesse.

If you log in to any other Extension Mobility device when you are still logged in to one Extension Mobility device and Finesse Desktop, you are automatically logged off from the first Extension Mobility device. However, you have to log out and log in again to Finesse Desktop.

Procedure

Step 1 Enter the following URL in the address bar of your browser:

https://*FQDN of Finesse Server:8445*/desktop

/

Where *FQDN of Finesse Server* is the fully qualified domain name of your primary server.

Step 2 If your contact center has installed a language pack for Cisco Finesse, on first login, a language selector screen appears on the desktop. From the language selector drop-down, choose the language that you want to appear on the desktop. Click **Next**.

Note You can also select a language by passing the locale as part of the URL (for example, https://*FQDN of Finesse server*/desktop?locale=fr_FR) or by changing your browser preferred language. The default language is English (en_US).

If your contact center does not have a language pack installed for Cisco Finesse, the desktop locale is English only.

Step 3 In the **Username** field, enter your agent ID or username.

Note Agent IDs are case-sensitive and can contain letters, numbers, hyphens (-), underscores (_), and periods (.). Agent IDs are assigned to you by your administrator. Agent IDs cannot begin or end with a period or contain two periods in a row.

Cisco Finesse agent usernames are restricted to 7-bit printable ASCII characters (any of the 94 characters with the numeric values from 33 to 126). The supported characters are: **A-Z and 0-9**,**,**,**-**,**!**, ~,`,**$**,^,**&**,**(**,**)**,**"**,**'**,**{**,**}**,**@**,**.**.They do not support the following characters, /, \, **[**,**]**,**:**,**;**,|, =,**,**+, ***,**?**, <, >.

Step 4 In the **Password** field, enter your password.

Step 5 In the **Extension** field, enter the extension of your phone.

Step 6 Click **Sign In**.

Note The **Sign In** button is enabled once the username, password, and extension fields are entered. If any field is incomplete, the **Sign In** button remains disabled.

Step 7 To change the language that appears on your desktop, use the **Change the Language** link to return to the language selector screen and choose the language.

You are signed into the Cisco Finesse desktop and your status is set to Not Ready. On clicking the user options on the top right corner, your role (agent or supervisor), agent name, agent ID, extension, and mobile number appear in the drop-down.

Note When you log in to the Finesse desktop for the first time, you are prompted to set your preference for notifications. Choose the option to always receive or allow toaster notifications. Toaster notifications will not appear if your browser is set to private mode that is **New incognito window** in Chrome or **New private window** in Firefox.

Sign In to Cisco Finesse Desktop Single Sign-On Mode

Procedure

Step 1 Enter the following URL in the address bar of your browser:

https://*FQDN of Finesse Server: 8445*/desktop

Where *FQDN* is the fully qualified domain name of your primary server.

Step 2 If your contact center has installed a language pack for Cisco Finesse, on first sign-in, a **Language Selector** screen appears on the desktop. From the language selector drop-down, choose the language that you want to appear on the desktop. Click **Next**.

Note You can also select a language by passing the locale as part of the URL (for example, https://*FQDN of Finesse server*/desktop?locale=fr_FR) or by changing your browser preferred language. The default language is English (en_US).

If your contact center does not have a language pack installed for Cisco Finesse, the desktop locale is English only.

Step 3 In the next page, enter your **Username** and **Password** and click **Sign In**.

Step 4 In the **Extension** field, enter your extension and click **Submit**.

Step 5 To change the language that appears on your desktop, click the **Change the Language** link to return to the language selector screen and choose the language.

You are signed into the Cisco Finesse desktop and your status is set to Not Ready. On clicking the user options on the top right corner, your role (agent or supervisor), agent name, agent ID, extension, and mobile number appear in the drop-down.

Note On first sign-in, you are prompted to set your preference for notifications. On the sign-in page, Username field is auto populated and disabled. Choose the option to always receive or allow toaster notifications. Toaster notifications will not appear if your browser is set to private mode that is **New incognito window** in Chrome or **New private window** in Firefox.

Account Locked After Five Failed Sign In Attempts

If you try to sign in to Finesse with the wrong password for five times in a row, Finesse blocks access to your account for five minutes. For security reasons, if you try to sign in again during that time, Finesse does not alert you that your account is locked. You must wait five minutes and try again. Do not attempt to sign in again when your account is locked, otherwise the lockout timer resets, and you must wait an additional five minutes.

This restriction applies to all the sign in methods.

Accept Security Certificates

The first time you sign in to the Finesse desktop, you may be prompted to accept security certificates before you can continue. Unless the certificates are deleted, you have to accept them only once. These certificates allow the Finesse desktop to communicate over a secure connection to the Finesse server.

Ensure the pop-ups are enabled for the Finesse desktop.

Note If you are using a Windows client, signed in as a Windows user and using Internet Explorer, you must run Internet Explorer as an administrator to install these security certificates. In your **Start** menu, right-click Internet Explorer and select **Run as administrator**.

Contact your administrator if you do not have the required permissions to install the security certificates.

Procedure

Step 1 In your browser, enter the URL for the Finesse desktop.

Step 2 If you use Internet Explorer:

a) A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)** to open the Finesse sign in page.

b) Enter your agent ID or username, password, and extension, and click **Sign In**.

c) In the **SSL Certificate Not Accepted** dialog box, click the certificate link.

A new browser tab opens for the certificate you need to accept. A certificate error appears in the address bar.

d) To open the Certificate dialog box, click **Certificate error** > **View Certificates**.

e) In the Certificate dialog box, click **Install Certificate** to open the Certificate Import Wizard.

If you are using Internet Explorer 11, the Install Certificate option does not appear until you add Finesse to your trusted sites.

1. From the browser menu, select **Internet Options**.
2. On the **Security** tab, click **Trusted Sites** > **Sites**.
3. In the **Add this website to the zone** field, enter the URL for the Finesse desktop, and click **Add**.
4. After you click **Install Certificate**, under **Store Location**, select **Current User** to install the certificate for the current user only, or select **Local Machine** to install the certificate for all Windows users on that computer.

   If you select **Local Machine**, a dialog box appears asking if you want to allow Windows host process to make changes to this computer. Select **Yes**.

f) On the Certificate Import Wizard, click **Next**.

g) Select **Place all certificates in the following store** and click **Browse**.

h) Select **Trusted Root Certification Authorities** and click **OK**.

i) Click **Next**.

j) Click **Finish**.
k) In the Security Warning dialog box, click **Yes** to install the certificate.
l) In the Certificate Import dialog box, click **OK**.
m) Click **OK** to close Certificate dialog box.
n) Close the browser tab. The accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process completes.

Note To remove the certificate error from the desktop, you must close and reopen your browser.

Step 3 If you use Edge:

a) A page appears stating that the site is not secure. Click **Details** > **Go on to the website (not recommended)** to open the Finesse sign in page.
b) Enter your agent ID or username, password, and extension, and click **Sign In**.
c) In the **SSL Certificate Not Accepted** dialog box, click the certificate link.

A new browser tab opens for the certificate you need to accept. A certificate error appears in the address bar.

d) To open the certificate information, click **Certificate error** > **View Certificates**.
e) In the **Certificate Information** column, click **Export to file**, browser to any location on your computer and save the certificate.
f) From **Start**, search and open the **Manage user certificates** tool.
g) In **Manage user certificates**, under **Certificates - Local Computer**, right-click **Trusted Root Certification Authorities** and click **All Tasks** > **Import**.
h) In the **Certificate Import Wizard**, click **Next**.
i) Click **Browse**, navigate to the location where you exported the certificate, select the certificate, and click **Open**.
j) In the **Certificate Import Wizard**, click **Next** > **Next** > **Finish**.
k) In the **Certificate Import Wizard** dialog box, click **OK**.
l) Close the browser tab. The accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process completes. To remove the certificate error from the desktop, you must close and reopen your browser.

Note If you want to add Finesse FQDN to the Trusted Sites of Edge:

1. Open the **Control Panel**.
2. Search and open **Internet Options**.
3. Follow **Step e** of **Accepting certificates in Internet Explorer**.

Step 4 If you use Firefox:

a) On **Your connection is not secure** page, click **Advanced** > **Add Exception**.

Important Ensure the **Permanently store this exception** box is checked.

b) Click **Confirm Security Exception**.

c) On the Finesse sign in page, enter your agent ID or username, password, and extension, and click **Sign In**.
d) In the **SSL Certificate Not Accepted** dialog box, click the certificate link.

A browser tab opens for the certificate that you need to accept.

e) On browser tab, click **I Understand the Risks** > **Add Exception**.
f) Ensure the **Permanently store this exception** box is checked.
g) Click **Confirm Security Exception**.

The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process completes.

Step 5 If you use Chrome:

a) A page appears that states your connection is nor private. Click **Advanced** > **Proceed to** *Finesse FQDN* to open the Finesse Sign-in page.
b) Enter your agent ID or username, password, and extension, and then click **Sign In**.
c) In the **SSL Certificate Not Accepted** dialog box, click the certificate link.

A browser tab opens for the certificate that you need to accept.

d) On the browser tab, click **Advanced** > **Proceed to** *Finesse FQDN*.

The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process completes.

Note If you click the certificate link and do not accept it, the certificate link stays enabled in the **SSL Certificate Not Accepted** dialog box.

Accept Certificates for Live Data Gadget

The Cisco Unified Intelligence Center Live Data gadget provides reports that you can view in the Finesse desktop. If your desktop contains these reports, the first time you sign in, you may be prompted to accept security certificates.

Procedure

Step 1 Sign in to the Finesse desktop.

The Cisco Unified Intelligence Center Live Data gadget displays a message that states Finesse is checking for connectivity. If Finesse detects any security certificates that must be accepted, a message appears that lists the certificates that you must accept to use Cisco Unified Intelligence Center.

Note Each Cisco Unified Intelligence Center report displays this message.

Step 2 Click **OK**.

A new browser tab (or window, depending on your browser settings) opens for each certificate that you need to accept. The message in the gadget changes to state that to continue, accept the certificates in the opened tabs.

Step 3 If you use Internet Explorer:

a) Click **Certificate error** > **View Certificates** to open the Certificate dialog box.
b) On the Certificate dialog box, click **Install Certificate** to open the Certificate Import Wizard.

If you are using Internet Explorer 11 with Windows 8.1, the Install Certificate option does not appear until you add Finesse to your trusted sites.

1. From the browser menu, select **Internet Options**.
2. On the **Security** tab, click **Trusted Sites** > **Sites**.
3. In the **Add this website to the zone** field, enter the URL for the Finesse desktop and click **Add**.
4. After you click **Install Certificate**, under **Store Location**, select **Current User** to install the certificate for the current user only, or select **Local Machine** to install the certificate for all Windows users on that computer.

   If you select **Local Machine**, a dialog box appears that asks if you want to allow Windows host process to make changes to this computer. Select **Yes**.

c) On the Certificate Import Wizard, click **Next**.
d) Select **Place all certificates in the following store** and click **Browse**.
e) Select **Trusted Root Certification Authorities** and click **OK**.
f) Click **Next**.
g) Click **Finish**.
h) On the Security Warning dialog box, click **Yes** to install the certificate.
i) On the Certificate Import dialog box, click **OK**.
j) Click **OK** on the Certificate dialog box.
k) Close the browser tab. Repeat the preceding steps until all certificates are accepted.

After the browser tabs are closed, the Cisco Unified Intelligence Center Live Data gadget reloads.

Step 4 To accept the certificates in Edge:

a) In certificate error browser tab, click **Certificate error** > **View Certificates** to open the certificate information.
b) In the **Certificate Information** column, click **Export to file**, browser to any location on your computer and save the certificate.
c) From **Start**, search and open the **Manage user certificates** tool.
d) In **Manage user certificates**, under **Certificates - Local Computer**, right-click **Trusted Root Certification Authorities** and click **All Tasks** > **Import**.
e) In the **Certificate Import Wizard**, click **Next**.

f) Click **Browse**, navigate to the location where you exported the certificate, select the certificate, and click **Open**.
g) In the **Certificate Import Wizard**, click **Next** > **Next** > **Finish**.
h) In the **Certificate Import Wizard** dialog box, click **OK**.
i) After the browser tabs are closed, the Cisco Unified Intelligence Center Live Data gadget reloads.

Step 5 If you use Firefox:

a) In each tab, click **I Understand the Risks** and click **Add Exception**.
b) Ensure the **Permanently store this exception** box is checked.
c) Click **Confirm Security Exception**.
After the browser tabs are closed, the Cisco Unified Intelligence Center Live Data gadget reloads.

Step 6 To accept the certificates in Chrome:

a) In **Your connection is not private** page, click **Advanced** > **Proceed to** *CUIC FQDN*.

After the browser tabs are closed, the Cisco Unified Intelligence Center Live Data gadget reloads.

Accept Certificates for Multi-session Chat and Email

Before you can join a chat room or handle email contacts, you may be required to accept certificates in the Manage Chat and Email gadget on the Finesse desktop. When you sign in to Finesse, select Manage Chat and Email gadget from the left pane to check whether you must accept any certificates and ensure that the gadget loads properly.

Procedure

Step 1 Sign in to the Finesse desktop.

The Manage Chat and Email gadget displays a message that states that it is checking for connectivity. If Finesse detects that security certificates must be accepted, a message appears that lists the certificates that you must accept to use the gadget.

Step 2 Click **OK**.

A new browser tab (or window, depending on your browser settings) opens for each certificate that you need to accept.

Step 3 The steps to accept the certificates in your browser are the same as the steps you followed to accept the Live Data certificates. Follow the instructions for your browser type that are outlined in *Accept Certificates for Live Data Gadget* section.

Related Topics

Accept Certificates for Live Data Gadget, on page 8

Sign Out of the Finesse Desktop

Important Do not close your browser to sign out of the Finesse desktop. Finesse can take up to 120 seconds to detect that your browser is closed and an additional 60 seconds to sign you out. Finesse may continue to route contacts to you during this time.

You cannot sign out of the Finesse desktop when your Voice or Digital Channels are in the Ready state.

Procedure

Step 1 Ensure your state is set to Not Ready. Click the user options icon on the top-right corner of your screen. The Sign Out option is displayed with a drop-down list of Sign Out reason .

Note If you handle chat and email contacts, you must ensure that your status is set to Not Ready in both the Call Control gadget and the Chat and Email Control gadget.

Step 2 Select the appropriate Sign Out reason code to sign out.

Note If no Sign Out reason are configured for your team, Finesse signs you out when you click **Sign Out**.

Step 3 On the **Sign Out** screen, you can choose to exit the browser or click the **Sign In** link to be redirected to the Finesse login screen.

Desktop Chat

Desktop Chat interface is hosted by the Finesse browser desktop and requires a separate login. This feature provides chat functionalities required for agents and supervisors to chat with each other or with other Subject Matter Experts in the organization. Desktop Chat will be available on your Finesse desktop only if the administrator has configured this feature for you.

Note Desktop Chat does not support Single Sign-On. It requires an explicit login for both SSO and non SSO platforms.

Desktop Chat users are identified with a unique identity which is in the form of username@FQDN.com.

The agent state in the Desktop Chat is seperate from the Voice or Digital Channels state and can be controlled by the user.

The Desktop Chat state is reflected in the user's combined presence. For example, If you are logging into Desktop Chat, you are seen as available in Jabber or other connected chat tools.

While accepting the Desktop Chat certificates, if you accept one certificate and skip the rest, you will lose your Desktop Chat status during a failover. Ensure to accept all certificates to preserve the Desktop Chat login

and status after a failover. Depending on the failover type, you may either lose or retain all your Desktop chat sessions.

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 you need to 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* onwards.

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.

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 Finesse desktop window or tab is inactive, Finesse displays a notification with the chat details. Click the toaster notification to restore the 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 who are logged into 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**.

Live Data Reports

Access Live Data

Cisco Finesse agent and supervisor desktops provide Live Data gadget.

Live Data gadget displays information about the current state of the contact center. This gadget receives data from the real-time data source at frequent intervals.

This feature provides the following access:

- Agents can access the Live Data agent reports.
- Supervisors can access the Live Data agent and supervisor reports.

To access reports, the administrator must add and configure them in the Cisco Finesse administration console.

In Cisco Finesse agent desktop, click the **My Statistics** tab to access the reports.

In Cisco Finesse supervisor desktop, click the **Team Data** tab and **Queue Data** tab to access the reports.

View Multiple Live Data Report Views

Cisco Finesse allows you to view multiple Live Data reports or views on a single gadget. You can select the desired view to display from a drop-down list on the gadget toolbar, which lists up to five report views in **Report Name - View Name** format. Your administrator determines which views are available for you to select.

Note When you upgrade from an earlier version of Unified CCX 10.x to Unified CCX 11.0 version you can view the multiple live data reports on a single gadget only.

From the Live Data report toolbar, you can also do the following:

- Pause and resume event updates in the Live Data gadget using the pause and play button. (If the button is paused when there are updates available on the gadget, a notification appears over the button.)
- Hide and restore the toolbar using the arrow in the center of the toolbar.
- Access help for the relevant reporting gadgets by clicking the help button.

View My History

Use the **My History** tab on the Agent or Supervisor desktop to view your recent call history and state history.

Recent Call History

On clicking the **My History** tab on the desktop, you can view the following details of the your calls since midnight:

- **Type**: Indicates if the call was an Inbound or Outbound call.
- **Number**: Indicates the phone number of the Inbound or Outbound call.
- **Disposition**: Indicates the action taken for the call.
- **Wrap-Up Reason**: Indicates the call reason category for the call.
- **Queue**: Indicates the queue associated with the call.
- **Start-Time**: Indicates the start time of the call.

- **Duration**: Indicates the duration of the call.
  - For Inbound calls it includes the ring time, talk time and hold time.
  - For Outbound calls it includes dial tone, ring back, talk time, and hold time.
- **Make Call**: Click on the call icon to initiate an outgoing call when in Ready or Not Ready state.

Recent State History

On clicking the **My History** tab on the desktop, you can view the following details of your call state history since midnight:

- **Start Time**: Indicates the time when agent state was initiated.
- **State**: Indicates the ACD agent state.
- **Reason**: Indicates the reason for the current agent state.
- **Duration**: Indicates the duration of the agent state.

View Context Service Data

Cisco Context Service is a cloud-based omnichannel solution for Cisco Unified Contact Center Express. It enables you to capture your customer's interaction history by providing flexible storage of customer-interaction data across any channel.

For more information about Context Service and to check service availability, see https://help.webex.com/community/context-service.

Procedure

Step 1 To view the Context Service gadget, click the **Manage Customer** tab.

Step 2 For information about how to use the Context Service, see the instructions provided in the gadget.

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.