Common Tasks

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:
   a. From the browser menu, select **Tools** > **Internet Options**.
   b. In the **Privacy** tab, click **Sites**.
   c. In the Address of website box, enter the domain name for the Side A Finesse server.
   d. Click **Allow**.
   e. In the Address of website box, enter the domain name for the Side B Finesse server.
   f. 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:

a. From the Internet Explorer browser menu, click **Tools** > **Internet Options**.

b. In the **Security** tab, click **Custom level**.

c. Under ActiveX controls and plug-ins, select **Enable** for **Run ActiveX controls and plug-ins** and **Script ActiveX controls marked safe for scripting**.

d. Under Scripting, select **Enable** for **Active Scripting**.

Note If you are using self-signed or CA-signed certificates and the server's FQDN, there should not be any certificate errors or warnings when connecting to Cisco 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.

Browser Settings for Chrome

Ensure that you disable the **Automatic tab discarding** feature in Chrome (version 74 and earlier) to avoid exiting the Finesse desktop tab when the system memory is low.

Procedure

Step 1 Open Chrome and enter **`chrome://flags/#automatic-tab-discarding`** in the address bar.

Step 2 Press **Enter**.

Step 3 Select **Disabled** from the drop-down list.

Step 4 Click **Relaunch Now**.

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.

Sign In to Cisco Finesse Desktop

The administrator can set up custom security banner message and custom logon message for Finesse Desktop users. Both the message types can be configured at the same time. The custom logon message can be used to configure the logon banner commonly across all processes that support the feature.

Note This feature custom logon message is available only for CCX deployment.

If your administrator has defined a custom security banner message, the message is displayed at the bottom of the Finesse desktop **Sign In** page. If your administrator has defined a custom logon message, the message is displayed in a pop-up dialog box after you click **Sign In**. You must acknowledge the custom logon message to sign in.

Note Custom logon message is not displayed for SSO users.

Note This feature custom logon message is available only for CCX deployment.

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 Sign in to the administration console on the primary UCCX server using the URL: https://FQDN of Unified CCX 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 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 Primary Server:8445*/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 user ID.

Note

- User IDs are case-sensitive and can contain numbers (0-9), hyphens (-), underscores (_), and periods (.). User IDs are assigned to you by your administrator and cannot begin or end with a period or contain two periods in a row.

  To make user IDs case-insensitive, you must install 12.5(1) SU1 ES02.

- 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,,,-,!,** ~,`,**$,^,&,(,),",',{,},@,.**. The following characters are not supported: /, \, **[,],:,;,|**, =,,,+, ***,?**, <, >.

- The Username (desktop Sign In page) in Unified CCX deployment refers to the AgentID.

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.

- For non-SSO users, a dialog with the message appears when you (agent, supervisor, administrator) click the **Sign In** button.

- If sign in fails due to device errors the desktop attempts to automatically sign in again. An alert is displayed detailing the number of remaining retries and the time left for the next retry attempt.

- If your administrator has enabled the device selection feature for you, the devices associated to your extension are displayed in **Select Your Preferred Device** screen. For more information see Agent Device Selection, on page 5. Even if an agent has signed into only one device, this screen is displayed. Therefore, this screen offers a chance to determine if an agent has missed logging into the selected device and thereby retrying the login.

- To change the language that appears on your desktop, use the **Change the Language** link. On the language selector screen, choose the language.

You are signed in to 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.

Agent Device Selection

When you (agents and supervisors) need to use different devices that are configured with the same extension, the administrator must enable the Agent Device Selection feature for you. You can select one of the endpoints (Desk Phone with Extension Mobility, Desk Phone without Extension Mobility, Jabber, and so on) on the shared Automatic Call Distribution (ACD) lines as your active device while signing in to the Finesse desktop. This informs the solution to ignore the other devices and use the indicated device as the only source for call interaction. This allows effective control of the call irrespective of from where you connect to the system. You can switch the active device based on where you are working—across shifts, moving from one office to another across various locations, or working from home.

When you sign in with the desired extension, the **Select Your Preferred Device** screen displays a list of devices that share the same extension. You can refresh the list of devices (if the required device is not listed) and select the device that you want to use as the active device for the current desktop session.

Note When the Agent Device Selection feature is enabled, both primary and secondary extensions can be shared with multiple devices. However, ensure that the devices using the shared extensions are not used at the same time.

Procedure

Step 1 Sign in to the Finesse desktop.
If your administrator has enabled the Agent Device Selection feature, the devices sharing your extension are displayed in **Select Your Preferred Device** screen.

Select Your Preferred Device screen displays the shared devices in your extension in the following format: Device Type (Device Name). For example, Cisco 6940 (SEP0000BCCER9876).

Step 2 Click the device name to select your preferred device.

- To access the Finesse desktop Sign In page, click **Back**. When you click the **Back** button on the browser, the page refreshes and you are retained on the same **Select Your Preferred Device** screen. However, if you had selected any device, the selection is lost.

  Note Finesse desktop retains your selection only when you click **Continue**.

  When the Finesse desktop fails over, the reconnection banner shows the active device that is selected for the new session, which is the same as the device selected before the failover.

Note If the required device is not listed, check whether the extension used to sign in (displayed in the **Select Your Preferred Device** screen) is valid and if you have signed in to the device. After you have signed in to the required device, click **Refresh**.

- When you place the pointer on the truncated (because of space constraints) device name, a tool tip appears to detail the complete information of the device like device type and device name.
- The supported resolution for the Finesse desktop is 1366 x 768 or higher for the optimal viewing of the **Select Your Preferred Device** screen.
- The maximum number of devices that are listed in **Select Your Preferred Device** screen is five.
  - If you have signed into more than five devices, and your preferred device is not listed, sign out from devices that are not required. Click **Refresh** in **Select Your Preferred Device** screen to update the displayed list of devices.

- When you sign in, the browser saves the device that is selected for that agent and the extension used. On subsequent sign-in of the same agent with the same extension, on the same machine, through the same browser, that device will be displayed as the first in the preferred device selection screen.

Step 3 Click **Continue**.

The selected device is listed under the user options icon on the top-right corner of your screen.

Note To change the device selection, sign out from Finesse desktop and sign in again.

Note Enabling automatic device selection is supported when a single active device is available for the extension at the time of sign in. For more information, see *Enable Automatic Device Selection for Single Active Device* in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/series.html#MaintainandOperate

Sign In to Cisco Finesse Desktop Single Sign-On Mode

Cisco Finesse supports custom security banner message for Finesse desktop users. If your administrator has defined the security banner message, then it is displayed in the desktop **Sign In** page.

Procedure

Step 1 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 Primary Server:8445*/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 2 On the IdP page, enter your operating system **Username** and **Password**, and click **Sign in**.

Step 3 In the **Extension** field, enter your extension and click **Submit**.

Note

- If your administrator has enabled the device selection feature for you, the devices associated to your extension are displayed in **Select Your Preferred Device** screen. For more information see Agent Device Selection, on page 5. Even if an agent has signed into only one device, this screen is displayed. Therefore, this screen offers a chance to determine if an agent has missed logging into the selected device and thereby retrying the login.
- If sign in fails due to device errors the desktop attempts to automatically sign in again. An alert is displayed detailing the number of remaining retries and the time left for the next retry attempt.
- To change the language that appears on your desktop, use the **Change the Language** link. On the language selector screen, choose the language.

You are signed in to 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

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

After you enter the Finesse desktop URL in your browser, the procedure to add a certificate is as follows:

Install certificates on Windows operating system:

The procedure to add a certificate varies for each browser. The procedure for each browser is as follows:

Internet Explorer

Note If you are using a Windows client, signed in as a Windows user, you must run Internet Explorer as an administrator to install the 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.

1. A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)** link to open the Finesse sign in page. The Finesse sign in screen appears with a certificate error in the address bar.
2. Click on the certificate error that appears in the address bar and then click **View Certificates**.
3. In the **Certificate** dialog box, click **Install Certificate** to open the **Certificate Import Wizard**.
4. Select **Current User** to install the certificate for the current user only, or select **Local Machine** to install the certificate for all Windows users.
5. On the **Certificate Import Wizard**, click **Next**.

6. Select **Place all certificates in the following store** and click **Browse**.
7. Select **Trusted Root Certification Authorities** and click **OK**.
8. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears.
9. Click **Yes** to install the certificate. The **Certificate Import** dialog box appears.
10. Click **OK** and close the **Certificate Import** dialog box.
11. 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 is complete.

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

Firefox

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

Note Ensure that the **Permanently store this exception** box is checked.

2. Click **Confirm Security Exception**.
3. On the Finesse sign in page, enter your agent ID or username, password, and extension, and click **Sign In**.
4. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.
5. On the browser tab, click **I Understand the Risks** > **Add Exception**. Ensure that the **Permanently store this exception** box is checked.
6. 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 is complete.

Chrome and Edge Chromium (Microsoft Edge)

1. A page appears that states your connection is not private. To open the Finesse sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

2. Enter your agent ID or username, password, and extension, and then click **Sign In**.
3. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.

4. On the browser tab,

    In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

    In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

    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.

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. The certificate error appears every time you sign in. The procedure to permanently accept the certificate is as follows.

5. Click on the certificate error that appears in the address bar and then,

    In Chrome, select **Certificate (Invalid)**.

    In Microsoft Edge, select **Certificate (not valid)**.

    The **Certificate** dialog box appears.

6. In the **Details** tab, click **Copy to File**. The **Certificate Export Wizard** appears.
7. Click **Next**.
8. Keep the default selection **DER encoded binary X.509 (.CER)** and click **Next**.
9. Click **Browse** and select the folder in which you want to save the certificate, enter a recognizable file name and click **Save**.
10. Browse to the folder where you have saved the certificate (**.cer** file), right-click on the file, and click **Install Certificate**. The **Certificate Import Wizard** appears.
11. Keep the default selection **Current User** and click **Next**.
12. Select **Place all certificates in the following store** and click **Browse**. The **Select Certificate Store** dialog box appears.
13. Select **Trusted Root Certification Authorities** and click **OK**.
14. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears that asks if you want to install the certificate.
15. Click **Yes**. A **Certificate Import** dialog box that states the import was successful appears.

Close the browser and sign in to Finesse. The security error does not appear in the address bar.

Install certificates on macOS:

The procedure to download a certificate varies for each browser. The procedure for each browser is as follows:

Chrome and Edge Chromium (Microsoft Edge)

1. A warning page appears which states that your connection is not private. To open the Finesse sign in page,

    In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

    In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

2. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (Not Valid)**.

   A certificate dialog box appears with the certificate details.

3. Drag the **Certificate** icon to the desktop.
4. Double-click the certificate. The **Keychain Access** application opens.
5. In the right pane of Keychains dialog, browse to the certificate, right-click on the certificate, and select **Get Info** from the options that are listed. A dialog appears with more information about the certificate.
6. Expand **Trust**. From the **When using this certificate** drop-down, select **Always Trust**.
7. Close the dialog box that has more information about the certificate. A confirmation dialog box appears.
8. Authenticate the modification of Keychains by providing a password.
9. The certificate is now trusted, and the certificate error does not appear on the address bar.

Firefox

1. In your Firefox browser, enter the Finesse desktop URL. A warning page appears which states that there is a security risk.
2. Click **Advanced** and then click **View Certificate** link. The **Certificate Viewer** dialog box appears.
3. Click **Details** and then click **Export**. Save the certificate (**.crt** file) in a local folder.

Note If **.crt** file option is not available, select **.der** option to save the certificate.

4. From the menu, select **Firefox** > **Preferences**. The **Preferences** page is displayed.
5. In the left pane, select **Privacy & Security**.
6. Scroll to the **Certificates** section and click **View Certificates ...**. The **Certificate Manager** window is displayed.
7. Click **Import** and select the certificate.
8. The certificate is now authorized, and the certificate error does not appear on the address bar.

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.

After you log in to Finesse and click **Manage Chat and Email** a warning page **Click Launch Certificate and accept certificate to use Chat and Email** appears.

Click **Launch Certificate**.

Procedure

Step 1 **In Internet Explorer:**

a) A warning page appears that states the site is not secure.

b) Click **More Information** and then click **Go on to the webpage (Not recommended)** link.
The page that states this site is not secure automatically closes and the multi-session gadget loads.

Step 2 **In Firefox:**

a) A warning page appears that states your connection is not private.

b) Click **Advanced** and then click **Accept the Risk and Continue**.
The page that states this connection is not private automatically closes and the multi-session gadget loads.

Step 3 **In Chrome and Edge Chromium (Microsoft Edge):**

a) A warning page appears that states your connection is not private.

b) In Chrome, click **Advanced** and then click **Proceed to <Hostname> (unsafe)** link.

c) In Microsoft Edge, click **Advanced** and then click **Continue to <Hostname> (unsafe)** link.

The page that states this connection is not private automatically closes and the multi-session gadget loads.

The Launch Certificate error may appear multiple times. Follow the same procedure to load the multi-session gadget.

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 is available on your Finesse desktop only if the administrator has configured this feature for you.

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 *Accept Security Certificates*.

Note The supported format for Cisco IM and Presence EC certificate is imphostname-EC.domain.com.

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 separate 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.

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

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 Firefox, refer to the section *Accept Security Certificates* > *Step 4* onwards.
- To accept the certificates in Chrome and Edge Chromium, 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**.

Edit Call Variables

You can edit the call variable values if the administrator has configured the call variable as editable. You can edit the values during an active call or in the wrap-up state.

Note Call variables edit operation updates the values of the variables within the particular call. All entities listening to dialog events receive the updated call variables through the Cisco Finesse notifications. If any CTI clients are connected to the same CTI server, they also receive notifications of the changed call data though CTI call events. However, application scripts or databases that are used to populate the call variables are not directly affected by this edit.

Procedure

Step 1 In the Finesse desktop, expand the call control gadget to display the call variables.

Step 2 Click in the text box to edit the values as required.

Note In the following scenarios the changes made to the call variable by a user is overwritten:

- When multiple users edit the same field at the same time. For example, when two users (User A and User B) are editing the same field at the same time and if User A saves the edited values. Then, the changes that are made by User B are overwritten and User B is notified with a message.
- When there is a script change in the CTI server and during this period a user is editing the values. Then, the changes that are made by the user are overwritten and the user is notified with a message.

Step 3 Click **Save**.

To retrieve the previously saved values, click **Revert**.

Note The unsaved field values are overwritten during conflict.

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 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.

Drag-and-Drop and Resize Gadget or Component

The administrator can configure the drag-and-drop and resize gadget or component features for agents and supervisors to customize their Finesse desktop.

- The drag-and-drop feature allows agents and supervisors to drag (and drop) the gadget or the component to the required position on the desktop layout.
- The resize feature allows the agents and supervisors to shrink or expand the gadget or the component to a custom size on the desktop layout.

The Finesse desktop retains your choices when you access the browser again. For more information on resetting to default layout, see *Reset Layout*.

Note These features are also applicable for third-party gadgets.

Restrictions and Limitations

Following are the restrictions and limitations for drag and drop or resize feature:

- Rearranging and resizing action that is performed on a gadget or component is specific to the logged in user, the browser used, to the respective tab, and the device used.
- Rearranging and resizing actions are not applicable for header and page-level gadgets and components. For example, Agent State for Voice and Dialer Component.

Note If the administrator modifies the default layout, then the changes that are made by you are overwritten with default settings. The changes are reflected when you refresh or sign in again.

Drag-and-Drop a Gadget or Component

Before you begin

This feature is available on your Finesse desktop only if the administrator has configured this feature for you.

Procedure

Step 1 Sign in to the Cisco Finesse desktop.

Step 2 Place the pointer on the gadget or component title header. When the pointer changes to ✥ , click and drag the gadget or component to the required position on the desktop layout.

The drag-and-drop action that is performed on a gadget or component is specific to the logged in user, the browser used, to the respective tab, and the device used.

Note You can arrange a maximum of 12 gadgets or components side by side in a specific tab.

Resize a Gadget or Component

Before you begin

This feature is available on your Finesse desktop only if the administrator has configured this feature for you.

Procedure

Step 1 Sign in to the Cisco Finesse desktop.

Step 2 Place the pointer on the gadget or component border. When the pointer changes to ↕, then click and drag the ↕ to resize the gadget or component on the desktop layout.

The resize action that is performed on a gadget or component is specific to the logged in user, the browser used, to the respective tab, and the device used.

Note

- ↕ indicates vertical resizing and ↔ indicates horizontal resizing.
- The maximum length of the gadget is restricted to the screen length. The minimum length of the gadget is restricted to a 12th of the screen length.

Reset Layout

If you have modified the desktop layout using the drag-and-drop and resize features, then the layout can be reset to the default view using **Reset Layout** option. The **Reset Layout** option is available in the user options icon drop-down list.

Note You can also clear your browser cache to reset the layout to the default view.

Procedure

Step 1 Click the user options icon on the top-right corner of the screen.

Step 2 Click **Reset Layout**.

Step 3 Click **Ok** in the confirmation dialog box.

Restores the default view across all tabs.