Common Tasks

This chapter describes common tasks that agents and supervisors perform. These tasks include signing in and signing out of the desktop, changing your state, selecting reason codes and wrap-up reasons, and call control tasks.

Browser Settings for Agent and Supervisor Desktop

To ensure that all features of the Cisco Finesse agent and supervisor desktop work properly, you must disable popup blockers from the following supported browsers:

- Chrome (version 60 or higher)

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

- Firefox (version 52 and higher ESR)
- Edge Chromium (Microsoft Edge v79 and later)
- Internet Explorer 11.0 (Native Mode)

  Apart from disabling popup blockers, to configure the privacy and advanced settings in Internet Explorer, go to **Tools** > **Internet Options** > **Privacy**. Enter the domain name of Side A and B Finesse servers, and click **Allow**.

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.

Procedure

Step 1 In the address bar of your browser, enter https://FQDN of Finesse Server: 8445/desktop, where FQDN of Finesse Server is the fully qualified domain name of the Cisco Finesse 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.
- 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 CCE deployment refers to the AgentID (Peripheral number).

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.
- 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.

Sign In to Cisco Finesse Desktop Single Sign-On Mode

Cisco Finesse supports custom logon message for Finesse desktop users. For more information on custom messages see the .

Procedure

Step 1 In the address bar of your browser, enter https://FQDN of Finesse Server: 8445/desktop, where FQDN of Finesse Server is the fully qualified domain name of the Cisco Finesse 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 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 On the IdP page, enter **Username** and **Password**, and click **Sign in**.

Note You must enter the AWDB username.

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

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.

Sign In to Finesse Desktop Hybrid Mode

Procedure

Step 1 In the address bar of your browser, enter http://*FQDN of Finesse Server:8445*/finext-desktop.

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

Step 2 If your contact center has installed a language pack for 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 and click **Next**.

Note You can also select a language by passing the locale as part of the URL (for example, http://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 Finesse, the desktop locale is English only.

Step 3 On the login page, enter your **Username** and click **Next**.

Step 4 If the agent is in SSO Mode, the Finesse login page is displayed. Enter your **Extension** and click **Submit**.

If the agent is in Non SSO Mode, enter your **Password** and **Extension**. Click **Sign In**.

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 Non SSO users in Hybrid Mode can log in with a different username by clicking the **Sign in as a different user** link. This will direct you to the login page to enter your credentials.

Note On first login, you are prompted to set your preference for notifications. Choose the option to always receive or allow toaster notifications. Notifications may 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 Using IPv6

If directed by your administrator, you can sign in to Finesse using an IPv6-only client. In this case, include the appropriate HTTP or HTTPS port in the sign-in URL in Step 1 of the preceding procedure.

- For secure access using HTTPS, enter:

  https://<*FQDN*>:8445/desktop

- For HTTP access, enter:

  http://<*FQDN*>:8082/desktop

The remaining steps of the sign-in procedure remain the same for IPv6.

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 regardless of how you sign in, be it on the desktop, as a mobile agent, or using the Finesse IP Phone Agent (IPPA).

Sign In as Mobile Agent

When you sign in as a mobile agent, you can use any phone (home phone or mobile phone) that is accessible to the contact center phone system to receive calls.

For more information about using the mobile agent feature, see the *Unified Contact Center Enterprise Features Guide*.

Procedure

Step 1 In the address bar of your browser, enter http://FQDN of Finesse Server: 8445/desktop, where FQDN of Finesse Server is the fully qualified domain name of the Cisco Finesse server.

Step 2 In the **ID**, **password**, and **Extension** fields enter your username or agent ID, password, and extension.

For a mobile agent, the extension represents your virtual extension, also known as the local CTI port (LPC).

Step 3 Check the **Sign in as a Mobile Agent** box.

Step 4 The Mode and Dial Number fields appear. From the Mode drop-down, choose the mode you want to use.

Example:

In Call by Call mode, your phone is dialed for each incoming call and disconnected when the call ends.

In Nailed Connection mode, your phone is called when you sign in and the line stays connected through multiple customer calls.

Step 5 In the Dial Number field, enter your phone number and click **Sign In**.

In Nailed Connection mode, the desktop must receive and answer a setup call before sign-in is complete.

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.

When you select the **Sign in as a Mobile Agent** check box and choose a mode (Call by Call or Nailed Connection), Finesse stores a cookie in your browser that allows the browser to remember these selections. When you access the sign-in page again, the **Sign in as a Mobile Agent** check box and Mode are already selected. These selections persist across sign-ins, browser restarts, and failover scenarios.

However, if you access the alternate Finesse server directly and you have not signed in to this server as a mobile agent before, you must make these selections again.

Accept Security Certificates

Ensure that the pop-ups are enabled for .

After you enter 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 sign in page. 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 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 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 . 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 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 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 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 10, 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 Microsoft 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.

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 codes.

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

Note If no Sign Out reason codes 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.

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 All Digital Channels

When you sign in to Cisco Finesse desktop, the default state will be Not Ready for all digital channels. However, for individual digital channels, the default state reflected is as per registration for that particular channel.

Note You can register and configure upto four digital channels for Unified CCE deployment.

To change state for all digital channels:

Procedure

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

Step 2 Select Ready state from the list.

For all the digital channels, your selected state change is displayed as Ready.

What to do next

Proceed to change the state for your individual registered digital channels.

Change Your State for Individual Digital Channels

You can change the state for individual digital channels that you have configured and registered.

Procedure

Step 1 Click on the drop-down beside the configured channel.

Step 2 Select the required state from the list.

The change of state for the individual digital channels is reflected as a color change on the icon. For example, to indicate the state change, if you have registered Available and Not Available as the terminologies for **Chat** channel, and you select Available as your state, the **Chat** icon changes to green and if you select Non Available the **Chat** icon changes to Red.

Popover Notifications for Digital Channels

When you receive a request for chat, email, or any digital channels that you have registered and configured, a popover notification is displayed on the Finesse desktop. Click **Accept** to accept the request or **Reject** to reject the request.

Note If you do not accept the request, the popover notification fades away. The duration of the notification is configured by the administrator.

Make a Call

Your status must be Ready or Not Ready to make an outgoing call.

Note Finesse supports the use of any ASCII character when you make a call. Finesse converts letters typed into the dial pad into numbers. It does not remove non-numeric characters (including parentheses and hyphens) from phone numbers. All alphabetical and special characters from the phone numbers including **#**, *****, **+**, and **:** is supported.

Procedure

Step 1 Click the dialpad icon on the Cisco Finesse desktop.

The dialer dialog containing the keypad and a list of phone contacts is displayed. Your administrator assigns the phone contacts.

Step 2 Click the contact from the list or manually enter the number into the dialpad to make a call.

Note Enter text in the search field to search the list of contacts. To edit the number before making a call, click the edit icon next to the contact to populate the dialpad with the phone number.

Step 3 To end the call, click **End**.

Answer a Call

You must be in Ready state to be available for customer calls. When a call arrives at the desktop, your state automatically changes to Reserved. A popover notification with configured customer details is displayed with the **Answer** button.

Note You can receive a direct call from another agent while you are in Not Ready or Ready state.

Procedure

Step 1 Sign in to the Finesse desktop using the URL: `https://FQDN of Finesse Server:8445/desktop`.

Step 2 Click **Answer** in the notification popover.

Your state changes to Talking. You are connected to the caller. The configured call variables are displayed in the call control area and can be maximized or minimized, if required. This can be done by toggling the maximize/minimize arrow or clicking on call control. If a second call arrives on the desktop, the original call's call variables display is minimized.

Step 3 To end the call, click **End**.

Your state changes to Ready and you are available for the next incoming call.

To be in Not Ready state when the call ends, click the drop-down arrow beside your state while you are on the call and choose Not Ready or Not Ready with the appropriate reason code. Your state changes to Talking->Not Ready (Pending). After the call ends, your state changes to Not Ready.

Answer an Outbound Option Preview Call

An Outbound Option Preview call allows you to view a customer's contact information before you choose to accept or decline the call.

Procedure

Step 1 Ensure your state is set to Ready to receive a call.

The Outbound Option Preview call arrives at the desktop as a popover with the **Accept** and **Decline** buttons.Your state changes to Reserved (Outbound). The Call Control gadget expands to show customer information.

Step 2 After you review the information, click **Accept** to accept the call or click **Decline** to decline the call.

If you accept the call, the system places the call to the customer. If the attempt succeeds, you are connected to the customer. If the attempt fails, the reservation call disappears and Finesse places you in the Ready state.

If you decline the call, you must choose to reject or close the contact. If you click **Reject**, the contact remains in the campaign to be retried at a later time. If you click **Close**, the contact is closed for the duration of the campaign.

Answer a Direct Preview Outbound Call

A Direct Preview Outbound call allows you to view a customer's contact information before you choose to accept or decline the call.

Procedure

Step 1 Ensure your state is set to Ready to receive a call.

A Direct Preview Outbound call arrives at the desktop as a popover which has **Accept** and **Decline** buttons. Your state changes to Reserved (Outbound). The Call Control gadget expands to show customer information.

Step 2 After you review the information, click **Accept** to accept the call or click **Decline** to decline the call.

If you accept the call, the system places the call to the customer directly from your phone. If the attempt succeeds, you are connected to the customer. If the attempt fails, Finesse places you in Ready state.

If you decline the call, you must choose to reject or close the contact. If you click **Reject**, the contact remains in the campaign to be retried at a later time. If you click **Close**, the contact is closed for the duration of the campaign.

Reclassify a Direct Preview Outbound Call

The Reclassify button allows you to reclassify a Direct Preview Outbound call as Answering Machine, Fax, Invalid Number, or Voice. By default, a call is classified as Voice. This button is available after you accept the Direct Preview call and remains for the life of the call. This also available while you are in the Wrap-Up state. You can reclassify a call multiple times.

Procedure

Step 1 Answer a Direct Preview Outbound call.

Step 2 Listen to the call. If you determine the number called is busy, an answering machine, a fax, or an invalid number, click **Reclassify**.

Step 3 Choose the appropriate option from the resulting drop-down.

Step 4 To end the call, click **End**.

Schedule a Callback

If you are on an Outbound Dialer call and the customer wants to be called back at a later time, you can schedule a callback.

Procedure

Step 1 While you are on the call, click **Callback**.

The Callback dialog box appears. The Current Time field contains the current time in the customer's time zone (this field is read-only). The Phone Number field contains the phone number that was dialed for this call.

Step 2 If the customer prefers to be called back at a different phone number, enter the new phone number in the Phone Number field.

Step 3 In the Date and Time fields, enter the date and time to call the customer. Type the date and time in to the respective fields or choose the date and time from the displayed calendar.

You must enter the time in the customer's location (not the time in your location).

You can toggle between AM or PM and click **Enter**.

Note The time corresponds to the customer's time zone. Finesse uses the customer's area code to determine the time zone. A customer using a mobile phone may not be in the time zone that matches the area code of the phone. Therefore, you should confirm the time zone with the customer.

Step 4 Click **Schedule**.

Step 5 If you need to update the information after you schedule a callback, click **Callback** to re-open the Callback dialog box.

Step 6 Update the necessary fields and click **Update**.

Step 7 If you need to cancel the callback after you schedule it, click **Callback** to re-open the Callback dialog box.

Step 8 Click **Cancel**.

A message is displayed confirming that the callback has been canceled.

Answer an Outbound Option Personal Callback Call

When you are on an Outbound Option call, you can schedule a customer callback at a more convenient time. Scheduled callbacks can be personal or regular, depending on the configuration of your contact center. Regular callbacks appear on your desktop in the same Outbound Option mode as the original call (for example, if the original call was a Preview call, the callback call is a Preview call).

Personal callbacks are similar to Outbound Option Preview calls but the buttons on the desktop are slightly different.

Procedure

Step 1 Ensure your state is set to Ready to receive a call.

When an Outbound Option Personal Callback call arrives at the desktop, your state changes to Reserved (Outbound). The Call Control gadget expands to show customer information.

Step 2 After you review the information, click **Accept** to accept the call or click **Decline**, and then click **Close**.

If you accept the call, the system places the call to the customer. If the attempt succeeds, you are connected to the customer. If the attempt fails, the reservation call disappears and Finesse places you in Ready state.

If you decline the call, the contact is closed for the duration of the campaign.

Initiate a Consult Call

You must be on an active call to initiate a consult call.

Procedure

Step 1 Click **Consult**.

The dialer dialog containing the keypad and a list of phone contacts is displayed.

Step 2 Choose the contact you want to consult from the list of contacts or enter the number into the dialpad.

Step 3 On the dialpad, click **Call**.

The customer call is placed on hold and you are connected to the contact that you called.

Step 4 After you consult with the contact that you called, you can choose to end the consult call and retrieve the customer call, conference the customer into the consult call, or transfer the customer to the agent or supervisor that you consulted.

Option	Description
To end the consult call and retrieve the customer call	Click **End** on the consult call and click **Retrieve** on the customer call.
To place the other agent or supervisor on hold and go back to the customer	Click **Retrieve** on the customer call. Click **Retrieve** on the consult call to place the customer on hold and go back to the other agent or supervisor.
To conference the customer into the consult call	Click **Conference**. If you want to leave the conference, click **End**.
To transfer the customer to the agent or supervisor you are consulting with	Click **Transfer**.

Transfer a Call (Single-Step Transfer)

This feature allows you to transfer a call without first initiating a consult call.

Note You must be in Talking state to initiate a transfer. If you put the call on hold, the Transfer button disappears.

Procedure

Step 1 Click **Direct Transfer**.

The dialer dialog containing the keypad and a list of phone contacts is displayed.

Note Your administrator assigns your phone contacts.

Step 2 Choose a contact from the list or enter the number you want to call into the dialpad.

Note Enter text in the search field to search the list of contacts or select a contact to populate the dialpad with the phone number.

Step 3 On the dialer dialog, click **Direct Transfer**.

The call disappears from your desktop. You are now ready for the next call.

Send DTMF

Use this feature to send a string of dual-tone multifrequency (DTMF) digits during a call. For example, you can use this feature to interact with an interactive voice response (IVR) system to enter an account number or a password.

Note You must be on an active call to use this feature.

Procedure

Step 1 Click **Keypad**.

The dialer dialog containing the keypad and a list of phone contacts are displayed.

Step 2 Click the appropriate buttons on the dialpad to enter the DTMF digits.

You can send the following characters as part of a DTMF string:

- 0-9
- pound sign (#)
- asterisk (*)

The characters appear in the text field above the dialpad (this text field is read-only).

Note You can use the dialpad to enter the DTMF digits. You cannot type the DTMF digits using your keyboard.

Step 3 Click **Keypad** again or click anywhere outside to close the dialpad.

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.

If Cisco IM and Presence is configured with certificate which are not automatically trusted by browsers, user will be prompted to accept security certificate during sign in to the Finesse desktop. To avoid the prompts to accept certificate appearing every time, user 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, 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**.

Apply Wrap-Up Reason

Wrap-up reasons can be applied on all Inbound calls routed to the Contact Center and on all the Contact Center triggered outbound campaign calls only. If your administrator has assigned wrap-up reasons to you, the Wrap-Up Reason button appears when you are on a call or when you are in Wrap-Up state after a call (if you are configured for Wrap-Up).

If you do not have any Wrap-Up Reasons assigned to you, you will not have this feature on your desktop. Your administrator creates and assigns Wrap-Up Reasons.

Note Wrap-Up Reasons are set on per call basis. This means if you apply a wrap-up reason for a call, the same will be reflected on desktops of all other participants (agents) of the call.

You can enter a Wrap-Up Reason during a call or while you are in Wrap-Up state after the call ends (this includes call termination as well as transfer and conference drop scenarios). If Wrap-Up is required, you automatically transition to Wrap-Up state when the call ends. If wrap-up is optional, you can select Wrap-Up from the agent state drop-down during the call. Your state then appears as Talking -> Wrap-Up (Pending) for the duration of the call. When the call ends, you transition to Wrap-Up state and can complete any after call work.

If you want to specify what state to enter when the wrap-up timer expires, you can select the state from the drop-down before you select Wrap-Up. For example, while on a call, select Not Ready from the drop-down. Then select Wrap-Up.

To end Wrap-Up state, select your new state (Ready or Not Ready) from the drop-down or wait for the preconfigured timer to expire.

Note Once you enter a Wrap-Up state no further call updates will be made in the call control gadget. However, if you enter a wrap-up reason for the call while in wrap-up state, the call control gadget will be updated with the new wrap-up reason only; all other call information will remain as they were prior to entering the wrap-up state.

Procedure

Step 1 Click **Wrap-Up**.

Step 2 You can either select the appropriate reason by scrolling through the drop-down or use the provided search field in the Wrap-Up drop-down.

Step 3 Click **Apply**.

A check icon appears on top of the **Wrap-Up** button to indicate that Finesse successfully applied the Wrap-Up reason. The Wrap-Up reason that is applied is displayed as a tag just below the search field in the Wrap-Up popover.

Note You can change the Wrap-Up reason during the call. If you decide you want to use a different Wrap-Up reason, click the **Wrap-Up** button again, select a new Wrap-Up reason, and click **Apply**.

If you want to cancel the Wrap-Up reason, click **Cancel** to close the Wrap-Up popover.

Force Wrap-Up

If your administrator has assigned wrap-up reasons and you wish to change your state from wrap-up to any other state, a tooltip with the message **Select Wrap-Up Reason** is displayed. You cannot change your state unless the wrap-up reason is applied, or your timer expires and your state is changed automatically.

The wrap-up timer is applicable when administrator has set the wrap-up time for the CSQ. When agents end a call, the wrap-up timer starts the countdown and agents are required to wrap-up before the timer reaches zero.

For Example, if the timer is set to 30 seconds, the timer starts from 30 and ends on zero.

The wrap-up timer is displayed below the state.

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

Click the **My History** tab on the desktop, you can view the following details of your calls since the last time you logged in:

- **Type**: Indicates if the call was an Inbound or Outbound call.
- **Number**: Indicates the phone number of the call.
- **Disposition**: Indicates the action taken for the call.
- **Wrap-Up Reason**: Indicates the call reason category.
- **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

Click the **My History** tab on the desktop, you can view the following details of your call state history since the last time you logged in:

- **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 Multiple Live Data Report Views

Cisco Unified Intelligence Center 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 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.

From the Live Data report toolbar, you can:

- 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 Context Service Data

Cisco Context Service is a cloud-based omnichannel solution for Cisco Unified CCE. It enables you to capture the 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.

Send Error Report

If you experience problems with the Finesse desktop, you can send a set of desktop logs to your administrator.

Procedure

Step 1 To send desktop logs to the administrator, click the user options on the top-right corner of your screen.

Step 2 Select the **Send Error Report** option from the drop-down.

After Finesse desktop submits the logs, the Send Error Report option changes to display the **Successfully Sent** confirmation message.

The Send Error Report option reappears after the Finesse desktop submits the logs.

Note If your browser freezes or crashes before you can click the Send Error Report option and you need to restart your browser, do not click the Send Error Report option right away. After a browser restart, the logs are no longer available. You must wait until the desktop starts to exhibit the problem again and then select the option.