Common Tasks

Browser Settings for Internet Explorer

If Internet Explorer is used to access the Finesse desktop, certain settings must be configured in the browser to ensure all features of Finesse work properly.

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

- Active scripting

To enable these settings:

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

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

Browser Settings for Firefox

Complete the following steps to ensure Finesse behaves as expected when it is not the active window.

Procedure

Step 1 Open Firefox and enter `about:config` in the address bar.
A warning page appears that states, `This might void your warranty!`.

Step 2 Click **I'll be careful, I promise!**.

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

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

Step 5 Restart Firefox.

Sign In to Finesse Desktop

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

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

Procedure

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

https://*FQDN:portnumber*/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 Finesse, a language selector appears on the desktop. From the language selector drop-down list, select the language that you want to appear on the desktop.

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

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

Finesse agent usernames are restricted to 7-bit printable ASCII characters (any of the 94 characters with the numeric values from 33 to 126).They do not support double quotes ("").

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**.

You are signed in to the Finesse desktop. Your role (agent or supervisor), agent name, agent ID, and extension appear in the header. Your status is set to Not Ready.

Note On first login, you are prompted to set your preference for notifications. Choose the option to always receive or allow toaster notifications. Note that toaster notifications will not appear if your browser is set to private mode i.e **New incognito window** in Chrome or **New private window** in Firefox.

Sign In to Finesse Desktop Single Sign-On Mode

Procedure

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

https://*FQDN:portnumber*/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 Finesse, a language selector appears on the desktop. From the language selector drop-down list, select the language that you want to appear on the desktop.

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**.

Step 4 In the **Password** field, enter your password and click **Sign-In**.

Step 5 The Finesse landing page is displayed, In the **Extension** field, enter the extension of your phone.

Step 6 Click **Submit**.

You are signed in to the Finesse desktop. Your role (agent or supervisor), agent name, agent ID, and extension appear in the header. Your status is set to Not Ready.

Note On first login, you are prompted to set your preference for notifications. Choose the option to always receive or allow toaster notifications. Note that toaster notifications will not appear if your browser is set to private mode i.e **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 five times in a row, Finesse blocks access to your account for 5 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 5 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 5 minutes.

This restriction applies regardless of how you sign in, be it on the desktop or using the Finesse IP Phone Agent (IPPA).

Accept Security Certificates

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

You must make sure pop-ups are enabled for the Finesse desktop.

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

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

Procedure

Step 1 Enter the URL for the Finesse desktop in your browser.

Step 2 If you use Internet Explorer:

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

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

   The following message appears:

   Establishing encrypted connection...

   A dialog box appears that lists the certificates to accept.

c) Click **OK** on the dialog box.

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

   Note Depending on your browser settings, a window may open for each certificate you need to accept instead of a browser tab.

d) Click **Certificate error** and then click **View Certificates** to open the Certificate dialog box.

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

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

   1. From the browser menu, select **Internet Options**.
   2. On the **Security** tab, click **Trusted Sites**, and then click **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 who use this 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**.

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

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

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

i) Click **Next**.

j) Click **Finish**.

   A Security Warning dialog box appears that asks if you want to install the certificate.

k) Click **Yes**.

   A Certificate Import dialog box that states the import was successful appears.

l) Click **OK**.

m) Click **OK** on the Certificate dialog box.

n) Close the browser tab. You are asked to accept another certificate. Repeat the preceding steps until all certificates are accepted.

After you accept all required certificates, the sign-in process completes.

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

Step 3 If you use Firefox:

a) A page appears that states this connection is untrusted. Click **I Understand the Risks**, and then click **Add Exception**.
b) Ensure the **Permanently store this exception** check box is checked.
c) Click **Confirm Security Exception**.

The Finesse sign-in page appears.

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

The following message appears:

Establishing encrypted connection...

A dialog box appears that lists the certificates to accept.

e) Click **OK**.

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

f) On each tab, click **I Understand the Risks**, and then click **Add Exception**.
g) Ensure the **Permanently store this exception** check box is checked.
h) Click **Confirm Security Exception**.

Each tab closes after you accept the certificate.

After you accept all required certificates, the sign-in process completes.

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 that security certificates 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** and then click **View Certificates** to open the Certificate dialog box.

b) On the Certificate dialog box, click **Install Certificate** to open the Certificate Import Wizard.

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

1. From the browser menu, select **Internet Options**.
2. On the **Security** tab, click **Trusted Sites**, and then click **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 who use this 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 then click **Browse**.

e) Select **Trusted Root Certification Authorities**, and then click **OK**.

f) Click **Next**.

g) Click **Finish**.

A Security Warning dialog box appears that asks if you want to install the certificate.

h) Click **Yes**.

A Certificate Import dialog box that states the import was successful appears.

i) Click **OK**.

j) Click **OK** on the Certificate dialog box.

k) Close the browser tab. You are asked to accept another certificate. 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 If you use Firefox:

a) In each tab, click **I Understand the Risks**, and then click **Add Exception**.

b) Ensure the **Permanently store this exception** check box is checked.

c) Click **Confirm Security Exception**.
After the browser tabs are closed, the Cisco Unified Intelligence Center Live Data gadget reloads.

Accept Certificates for Multi-session Chat and Email

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

Procedure

Step 1 Sign in to the Finesse desktop.

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

Step 2 Click **OK**.

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

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

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 closed and an additional 60 seconds to sign you out. Finesse may continue to route contacts to you during this time.

Sign out of the desktop as described in the following procedure.

Procedure

Step 1 Ensure your status is set to Not Ready. Click the status drop-down list and select Not Ready (or Not Ready with the appropriate reason code).

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 Click **Sign Out**.

A drop-down list appears that contains the Sign Out reason code.

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

Step 3 Select the appropriate Sign Out reason code from this list.

Step 4 On the sign out confirmation screen, you can choose to exit the browser or be redirected to the Finesse Desktop by clicking the **Click here** link. This will take you to any one of the following sign out scenarios:

- The Finesse Landing page. To log in to the Finesse Desktop again, enter your **Username**, **Password** and **Extension**.
- The Finesse Landing page. To log in to the Finesse Desktop again, enter your **Extension**.
- The Log In page. To log in to the Finesse Desktop again, enter your **Password** and **Extension**.

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.

Live Data Reports

For more information about the Live Data reports that are supported by Cisco Finesse, see Live Data Reference.

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 Context Service Data

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

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

Procedure

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

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