



# Cisco Finesse

---

- [Introduction, on page 1](#)
- [Cisco Finesse Administration Console, on page 1](#)
- [Cisco Finesse Agent and Supervisor Desktop , on page 117](#)

## Introduction

Cisco Finesse is a next-generation agent and supervisor desktop designed to provide a collaborative experience for the various communities that interact with your customer service organization. It helps improve the customer experience while offering a user-centric design to enhance customer care representative satisfaction as well.

Cisco Finesse provides:

- A browser-based administration console and a browser-based desktop for agents and supervisors; no client-side installations required.
- A single, customizable "cockpit", or interface, that gives customer care providers quick and easy access to multiple assets and information sources.
- REST APIs that simplify the development and integration of value-added applications and minimize the need for detailed desktop development expertise.

Finesse configuration changes are permitted on only the primary server. Access to Finesse administration console on the secondary server is read-only.

When you attempt to save the changes in Finesse administration console on the secondary node, you receive a message that administration on the secondary node is read-only.

## Cisco Finesse Administration Console

### Getting Started

This chapter describes the interfaces that you use to configure, administer, and maintain Cisco Finesse and describes how to access them.

## Administration Tools

### Cisco Finesse Administration Console

The Cisco Finesse administration console is a web-based interface used to configure system settings in Cisco Finesse. The administration console contains tabs to click and access the various administration features. The tab names and the associated tasks are:

- **Settings:** IP Phone Agent Settings.
- **Call Variables Layout:** Manage the call and ECC variables that appear on the agent desktop call control gadget, team performance gadget, and call popover.
- **Desktop Layout:** Make changes to the default desktop layout for agents and supervisors.
- **Phone Books:** Add, edit, or delete phone books or phone book contacts.
- **Reasons:** Add, edit, or delete Not Ready reason codes, Sign Out reason codes, or Wrap-Up reasons (Reason Codes are disabled for Packaged CCE deployments).
- **Team Resources:** Assign desktop layouts, phone books, reason codes, and wrap-up reasons to specific teams.
- **Workflows:** Create and manage workflows and workflow actions.

The features you configure in the administration console are case-sensitive. For example, you can create two workflows named WORKFLOW and workflow; or two phone books named BOOK and book.

### Response Caching

To reflect the changes made to system settings in Finesse desktop, the administrator must clear server cache using the CLI **utils webproxy cache clear rest**. Ensure that the agent browser is refreshed for the system settings changes to take effect.

For more information of REST API Response Caching, see *Cisco Finesse Web Services Developer Guide* at <https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide>.

### Sign In to Cisco Finesse Administration Console

You can access the Cisco Finesse administration console only through HTTPS.

When you sign in to Cisco Finesse, always use the fully qualified domain name (FQDN) of the Cisco Finesse server in the URL.

### Procedure

- 
- Step 1** Direct your browser to `https://<FQDN>:8445/cfadmin`, where *FQDN* is the fully qualified domain name of your primary Finesse server.
- Step 2** The first time when you access the administration console using HTTPS, you are prompted to trust the self-signed certificate provided with Finesse. The following table describes the steps for each supported browser.

**Note** If you are using HTTPS but have installed a CA Certificate, you can skip this step. For more information about installing a CA Certificate, see *Cisco Finesse Installation and Upgrade Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html>.

Option	Description
Internet Explorer:	<ol style="list-style-type: none"> <li>a. A page appears that states this site is untrusted.</li> <li>b. Click <b>More information &gt; Go on to the webpage</b>.</li> </ol>
Microsoft Edge:	<ol style="list-style-type: none"> <li>a. A page appears that states this site is untrusted.</li> <li>b. Click <b>Details</b> and click <b>Go on to the webpage</b>.</li> </ol>
Firefox:	<ol style="list-style-type: none"> <li>a. A page appears that states this connection is untrusted.</li> <li>b. Click <b>I Understand the Risks</b>, and then click <b>Add Exception</b>.</li> <li>c. In the Add Security Exception dialog box, ensure that the check box is <b>Permanently store this exception</b> checked.</li> <li>d. Click <b>Confirm Security Exception</b>.</li> </ol>
Chrome:	<ol style="list-style-type: none"> <li>a. A page appears that states this connection is not private.</li> <li>b. Click <b>Advanced &gt; Proceed to &lt;Hostname&gt; (unsafe)</b></li> </ol>

**Step 3** On the Sign In page, in the ID field, enter the Application User ID that was used during the installation.

**Step 4** In the Password field, enter the Application User password that was used during the installation.

**Step 5** Click **Sign In**.

A successful sign-in launches an interface with defined administration gadgets and a Sign Out link.



- Note**
- After 30 minutes of inactivity, Cisco Finesse automatically signs you out of the administration console and you must sign in again.
  - When your administrator privileges are revoked by another Unified CCX administrator, you are automatically signed out (within 5 minutes) from the Cisco Finesse administration console. For more information on administrators privileges, see [Administrator Capability View Menu](#).

## Sign In Using IPv6

If you sign in to the Finesse Administration Console using an IPv6-only client, include the HTTPS port in the sign in URL in Step 1 of the preceding procedure.

`https://<FQDN>:8445/cfadmin`

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

If you sign in to the Finesse Administration Console using an IPv6-only client, include HTTPS port in the sign in URL in Step 1 of the preceding procedure.

- For HTTPS access, enter:

```
https://<FQDN>:8445/cfadmin
```

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

### Account Locked after Five Failed Sign in Attempts

If an administrator tries to sign in to the Finesse administrator console (or diagnostic portal) with the wrong password five times consecutively, Finesse blocks access to that user account for 30 minutes. For security reasons, Finesse does not alert the user that their account is locked. They must wait 30 minutes and try again.

Similarly, if agents or supervisors sign in to the desktop five times consecutively with the wrong password, Finesse blocks access to that user account. However, in this case, the lockout period is 5 minutes. This restriction also applies when agents and supervisors sign in using the mobile agent or Finesse IP Phone Agent (IPPA).




---

**Note** When an agent or supervisor account is locked, subsequent attempts to sign in, even with correct credentials, reset the lockout period to 5 minutes again. For example, if a locked user tries to sign in again after only 4 minutes, the lockout period is reset and the user must wait another 5 minutes. This reset does not apply to the administrator account.

---

To view if a user account is locked, enter the **file get activelog desktop recurs compress** CLI command.

Extract the zipped output and search the catalina.out logs (/opt/cisco/desktop/finesse/logs/catalina.out) for the following message referring to the locked username:

```
An attempt was made to authenticate the locked user "<username>"
```

### Cisco Unified Operating System Administration

This interface is web-based and is used to perform the following system administration functions:

- **Show:** View information on cluster nodes, hardware status, network configuration, installed software, system status, and IP preferences.
- **Settings:** Display and change IP settings, network time protocol (NTP) settings, SMTP settings, time, and version.
- **Security:** Manage certificates and set up and manage IPSec policies.
- **Software Upgrades:** Perform and upgrade or revert to a previous version.
- **Services:** Use the Ping and Remote Support features.



## Sign In to Cisco Unified Operating System Administration

### Procedure

---

- Step 1** Direct your browser to `http://host or IP address/cmplatform`, where *host or IP address* is the hostname or IP address of your server.
- Step 2** Sign in with the username and password for the Administrator User account.
- Note** After you sign in, you can access other Unified Communications Solutions tools from the Navigation drop-down list.
- 

## Certificate Management

Finesse provides a self-signed certificate that use or provide a CA certificate. You can obtain a CA certificate from a third-party vendor or produce one internal to your organization.

Finesse does not support wildcard certificates. After you upload a root certificate signed by a certificate authority (CA), the self-signed certificates are overwritten.

If you use the Finesse self-signed certificate, agents must accept the security certificates the first time they sign in to the desktop. If you use a CA certificate, you can accept it for the browser on each client or deploy a root certificate using group policies.



- 
- Note** If there is a mismatch between the server hostname and the certificate hostname, a certificate address mismatch warning message is displayed in IE. The certificate must be regenerated so that the hostname matches the server hostname before importing to Finesse. If there is a valid reason for the mismatch, uncheck the **Warn about certificate address mismatch** checkbox from **Tools > Internet Options > Advanced > Security** to allow the certificate to be accepted.
- 

## Obtain and Upload CA Certificate



- 
- Note** This procedure only applies if you are using HTTPS and is optional. If you are using HTTPS, you can choose to either obtain and upload a CA certificate or use the self-signed certificate provided with Finesse.
- 

To eliminate browser security warnings each time you sign in, obtain an application and root certificate signed by a CA. Use the Certificate Management utility from Cisco Unified Operating System Administration.

To open Cisco Unified Operating System Administration in your browser, enter:

`https://hostname of primary UCCX server/cmplatform`

Sign in using the username and password for the Application User account created during Finesse installation.




---

**Note** You can find detailed explanations in the Security topics of the *Cisco Unified Operating System Administration Online Help*.

---

### Procedure

---

- Step 1** Generate a CSR.
- Click **Security > Certificate Management > Generate CSR**.
  - From the Certificate Name drop-down list, choose **tomcat** and click **Generate CSR**.
- Step 2** Download the CSR.
- Select **Security > Certificate Management > Download CSR**.
  - From the Certificate Name drop-down list, choose **tomcat** and click **Generate CSR**.
- Step 3** Generate and download a CSR for the secondary Unified CCX server.
- To open Cisco Unified Operating System Administration for the secondary server in your browser, enter:  
<https://hostname of secondary UCCX server/cmplatform>
- Step 4** Use the CSRs to obtain the CA root certificate, intermediate certificate, and signed application certificate from the Certificate Authority.
- Note** To set up the certificate chain, you must upload the certificates in the order described in the following steps.
- Step 5** When you receive the certificates, click **Security > Certificate Management > Upload Certificate**.
- Step 6** Upload the root certificate.
- From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
  - In the **Upload File** field, click **Browse** and browse to the root certificate file.
  - Click **Upload File**.
- Step 7** Upload the intermediate certificate.
- From the **Certificate Purpose** drop-down list, choose **tomcat-trust**.
  - In the **Upload File** field, click **Browse** and browse to the intermediate certificate file.
  - Click **Upload File**.
- Step 8** Upload the application certificate.
- From the **Certificate Purpose** drop-down list, choose **tomcat**.
  - In the **Upload File** field, click **Browse** and browse to the application certificate file.
  - Click **Upload File**.
- Step 9** Restart both the Unified CCX nodes in the cluster.
- 

## Client-Side Certificate Acceptance

There are procedures that agents must perform to accept certificates the first time they sign in. The procedure type depends on the method you choose to manage certificates and the browser used by the agents.

### Deploy Root Certificate for Internet Explorer

In environments where group policies are enforced via the Active Directory domain, the root certificate can be added automatically to each user's Internet Explorer. Adding the certificate automatically simplifies user configuration requirements.



---

**Note** To avoid certificate warnings, each user must use the FQDN of the Finesse server to access the desktop.

---

#### Procedure

---

- Step 1** On the Windows domain controller, navigate to **Administrative Tools > Group Policy Management**.
- Note** Users who have strict Group Policy defined on the Finesse Agent Desktop have to disable **Cross Document Messaging** from **Group Policy Management** to ensure proper functioning of Finesse on Internet Explorer 11.
- Step 2** Right-click Default Domain Policy and select **Edit**.
- Step 3** In the Group Policy Management Console, click **Computer Configuration > Policies > Window Settings > Security Settings > Public Key Policies**.
- Step 4** Right-click Trusted Root Certification Authorities and select **Import**.
- Step 5** Import the *ca\_name.cer* file.
- Step 6** Go to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Certificate Services Client - Auto-Enrollment**.
- Step 7** From the Configuration Model list, select **Enabled**.
- Step 8** Sign in as a user on a computer that is part of the domain and open Internet Explorer.
- Step 9** If the user does not have the certificate, run the command **gpupdate.exe /target:computer /force** on the user's computer.
- 

### Set Up CA Certificate for Internet Explorer and Edge Browsers

After obtaining and uploading the CA certificates, the certificate must be automatically installed via group policy or all the users must accept the certificate.

In environments where users do not log in directly to a domain or where group policies are not utilized, every Internet Explorer user in the system must perform the following steps one time to accept the certificate:

#### Procedure

---

- Step 1** In Windows Explorer, double-click the *ca\_name.cer* file and then click **Open**.
- Note** Here the *ca\_name* is the name of your certificate.
- Step 2** In the **Certificate Import Wizard**, select **Current User**.
- Step 3** Click **Install Certificate > Next > Place all certificates in the following store**.
- Step 4** Click **Browse** and choose **Trusted Root Certification Authorities**.

- Step 5** Click **OK > Next > Finish**.
- Step 6** Click **Yes** on the install a certificate from a CA prompt.
- Step 7** To verify that the certificate was installed, from the browser menu on IE, choose **Tools > Internet Options**.
- Step 8** In the **Content** tab, click **Certificates**.
- Step 9** In the **Trusted Root Certification Authorities** tab, ensure that the new certificate appears in the list.
- Step 10** Restart the browser for the certificate installation to take effect.
- Note** If you are using Internet Explorer 11, you may receive a prompt to accept the certificate even if it is signed by a private CA.

---

### Set Up CA Certificate for Firefox Browser

Every Firefox user in the system must perform the following steps once to accept the certificate:



- 
- Note** To avoid certificate warnings, each user must use the FQDN of the Unified CCX server to access the desktop.
- 

#### Procedure

---

- Step 1** From the Firefox browser menu, choose **Options**.
- Step 2** Go to **Privacy and Security** tab.
- Step 3** Under Certificates section, click **View Certificates**.
- Step 4** Select **Authorities**.
- Step 5** Click **Import** and browse to the *ca\_name.cer* file.
- Note** Here the *ca\_name* is the name of your certificate.
- Step 6** Check the **Validate Identical Certificates** check box.
- Step 7** Restart the browser for the certificate to install.
- 

### Set Up CA Certificate for Chrome Browser

#### Procedure

---

- Step 1** In the browser, go to **Settings**.
- Step 2** In the Chrome browser, select **Advanced Settings > Privacy and Security**, click **Manage Certificates**.
- Step 3** Click **Trusted Root Certification Authorities** tab.
- Step 4** Click **Import** and browse to the *ca\_name.cer* file.  
In the **Trusted Root Certification Authorities** tab, ensure that the new certificate appears in the list.

**Step 5** Restart the browser for the certificate to install.

### Trust Self-Signed Certificate

Trust the self-signed certificate provided by Finesse to eliminate browser warnings each time you sign in to the administration console or agent desktop.

If you have uploaded a CA certificate, you can skip this procedure.

### Procedure

In your browser, enter the URL for the administration console (<https://FQDN of primary server:portnumber/cfadmin>) or the agent desktop (<https://FQDN of primary server>).

Option	Description
If you use Internet Explorer:	<ol style="list-style-type: none"> <li>a. A page appears that states there is a problem with the website's security certificate. Click <b>Continue to this website (not recommended)</b>. The sign in page for the administration console (or agent desktop) appears with a certificate error in the address bar if the browser.</li> <li>b. Click <b>Certificate Error &gt; View Certificates</b> to open the Certificate dialog box.</li> <li>c. In the Certificate dialog box, click <b>Install Certificate</b> to open the Certificate Import Wizard.</li> <li>d. Click <b>Next</b>.</li> <li>e. Choose <b>Place all certificates in the following store</b> and click <b>Browse</b>.</li> <li>f. Choose <b>Trusted Root Certification Authorities</b> and click <b>OK</b>.</li> <li>g. Click <b>Next &gt; Finish</b></li> <li>h. If a Security Warning dialog box appears asking if you want to install the certificate, click <b>Yes</b>.</li> <li>i. In the Successful Certificate Import dialog box, click <b>OK</b>.</li> <li>j. Enter your credentials and click <b>Sign In</b>.</li> </ol>
If you use Firefox:	<ol style="list-style-type: none"> <li>a. A page appears that states this connection is untrusted.</li> <li>b. Click <b>I Understand the Risks Add Exception</b>.</li> <li>c. In the Add Security Exception dialog box, ensure the <b>Permanently store this exception</b> check box is checked.</li> <li>d. Click <b>Confirm Security Exception</b>.  The page that states this connection is untrusted automatically closes and the administration console (or agent desktop) loads.</li> <li>e. Enter your credentials and click <b>Sign In</b>.</li> </ol>

Option	Description
	<p><b>f.</b> For the agent desktop only, an error appears that states Finesse cannot connect to the Cisco Finesse Notification Service and prompts you to add a security exception for the certificates issued by the Finesse server.</p> <p>Click <b>OK</b>.</p>

## Add Certificate for HTTPS Gadget

Add a certificate for a secure HTTP (HTTPS) gadget to load the gadget on the Finesse desktop and successfully perform HTTPS requests to the Finesse server.

This process allows HTTPS communication between the Finesse gadget container and the third-party gadget site for loading the gadget and performing any API calls the gadget makes to the third-party server.



**Note** A gadget that loads using HTTPS may still use HTTP communication between that gadget and the application server where it resides. If all traffic must be secure, the gadget developer must ensure that HTTPS is used to make API calls to the application server.

The certificate must be signed with a common name. The gadget URL in the desktop layout must use the same name (whether it uses an IP address or a FQDN) as the name with which the certificate is signed. If the certificate name and the name in the gadget URL do not match, the connection is not trusted and the gadget does not load.

To find the certificate name, enter the gadget URL in your browser. Click the lock icon in the address bar and then click View Details. Look for the common name field.

The Finesse host must be able to resolve this name using the DNS host entered during the installation. To verify that Finesse can resolve the name, run the CLI command **utils network ping <hostname>**.

## Procedure

- Step 1** Download the certificate from the third-party gadget host.
- Step 2** Upload the certificate to the designated Finesse system.
  - a) Sign in to Cisco Unified Operating System Administration on the primary Unified CCX node (<https://FQDN/cmplatform>, where *FQDN* is the fully qualified domain name of the Unified CCX node).
  - b) Click **Security > Certificate Management**.
  - c) Click **Upload Certificate/Certificate Chain**.
  - d) From the Certificate Name drop-down list, select **tomcat-trust**.
  - e) Click **Browse** and navigate to the tomcat.pem file that you downloaded in the previous step.
  - f) Click **Upload File**.
- Step 3** Restart Cisco Tomcat on the primary Unified CCX node.
- Step 4** Restart Cisco Finesse Tomcat on the primary Unified CCX node.
- Step 5** After synchronization is complete, restart Cisco Tomcat on the secondary Unified CCX node.

**Step 6** Restart Cisco Finesse Tomcat on the secondary Unified CCX node.

---

### Add Certificate for Multi-session Chat and Email

Add the Customer Collaboration Platform certificate to the Unified CCX servers to allow communication between Customer Collaboration Platform and Finesse. After you complete this procedure, agents must accept certificates in the Finesse desktop before they can use this gadget.

If Customer Collaboration Platform is deployed with private certificates, agents cannot join chat rooms or reply to email messages until they accept the Customer Collaboration Platform certificates. If the Manage Chat and Email gadget is deployed on the Manage Chat and Email tab of the Finesse desktop, agents may not realize that they need to accept the certificates. Have agents check the tab where the gadget appears when they sign in to Finesse to make sure that certificates are all accepted and the gadget loads correctly.

The steps to add a certificate for the Manage Chat and Email gadget are the same as the steps outlined in the procedure **Add Certificate for HTTPS Gadget**.



---

**Note** The procedure to add a certificate for an HTTPS gadget refers to the third-party gadget host. To add a certificate for chat and email, perform the applicable steps on the Customer Collaboration Platform server.

---

#### Related Topics

[Add Certificate for HTTPS Gadget](#), on page 10

## Manage System Settings



---

**Note** For information about Finesse IP Phone Agent Settings, see **Manage Finesse IP Phone Agent**.

---

#### Related Topics

[Manage Finesse IP Phone Agent](#), on page 98

## Desktop Chat Server Settings

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

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

IM&P has a clustered design, where users are distributed across multiple nodes in the cluster. The Desktop Chat initially discovers the IM&P nodes that a user has configured, caches this information and communicates with the actual server for subsequent login, until the browser cache is cleared. To spread the initial discovery

load, it is advisable to configure the nodes in a round robin fashion if the deployment has more than one Finesse cluster. For example, if there are 5 IM&P nodes configure Finesse cluster A with node 1 & 2, Finesse cluster B with nodes 3 & 4, and so on.

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

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

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

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

**Actions on the Desktop Chat Server gadget:**

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




---

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

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





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

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



**Note** Desktop Chat is not supported with the unrestricted versions of IM&P.

## Configure Desktop Chat Server Settings

### Procedure

- Step 1** Sign in to the administration console with the Application User credentials.
- Step 2** In the **Desktop Chat Server Settings** area, enter the IM&P primary and secondary server URL of the Desktop Chat.
- Step 3** Click **Save**.

**Note** Desktop Chat requires Cisco Unified Presence 12.5 and higher versions.

## Cloud Connect Server Settings

Cloud Connect is a component that hosts services that allow customers to use cloud capabilities such as Cisco Webex Experience Management. The administrator can configure the Cloud Connect server settings in the Finesse administration console to contact the Cisco cloud services.

For more information, see the Cisco Webex Experience Management Survey section in *Cisco Unified Contact Center Express Features Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-feature-guides-list.html>.

The following table describes the fields on the Cloud Connect server settings gadget:

Field	Explanation
Username	(mandatory) The Cloud Connect administrator username required to sign in to Cloud Connect.
Password	(mandatory) The Cloud Connect administrator password required to sign in to Cloud Connect.
Publisher Address	(mandatory) The hostname of the Cloud Connect publisher.

Field	Explanation
Subscriber Address	(optional) The hostname of the Cloud Connect subscriber.

#### Actions on the Cloud Connect Server Settings gadget:

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

## Configure Cloud Connect Server Settings

### Procedure

- 
- Step 1** Sign in to the administration console on the primary UCCX server using the URL: `https://FQDN of Unified CCX server:8445/cfadmin`.
- Step 2** Select **Settings > Cloud Connect Server Settings**.
- Step 3** Enter the **Username**, **Password**, and **Publisher Address** of the Cloud Connect server.  
(optional) Enter the **Subscriber Address** for multinode deployment.
- Step 4** Click **Save**.
- 

## Keyboard Shortcuts

Keyboard shortcuts provide an alternate way to perform a specific action on the Finesse agent and supervisor desktop. For more information, see *Access Keyboard Shortcuts* section in the *Cisco Finesse Agent and Supervisor Desktop User Guide*.

### Keyboard Shortcut Conflicts

Keyboard shortcut conflicts occur if multiple gadgets use the same keyboard shortcut. This causes a particular key combination to be disabled until the conflict is resolved.

Keyboard shortcut conflicts at the page level can be resolved only by modifying the keyboard shortcuts at the gadget level. To modify the keyboard shortcuts at the gadget level, contact developer support services.

Keyboard shortcut conflict can occur in the following scenarios:

Conflict Scenario	Resolution
Conflicts can occur between keyboard shortcuts at the page level and gadget level.	This conflict cannot be resolved by the Finesse administrator.
Conflicts can occur when two gadgets have the same keyboard shortcut, and both are in the same tab.	Move one of the gadgets to another tab.
Conflicts can occur when there are multiple instances of the same gadget and focus is on the active tab*.	Move one of the gadgets to another tab.

\* - Active tab refers to the tab that is currently being used.

The administrator can use the CLI command to disable the keyboard shortcuts for the Finesse agent and supervisor desktop. For more information on CLI commands, see *Desktop Properties*.

**Note**

- After deploying the third-party gadgets, the administrator must sign in as an agent and a supervisor to check if there are any keyboard shortcut conflicts and resolve them.
- The third-party gadget providers can use the keyboard shortcuts JavaScript library as a guideline to provide a consistent desktop user experience.

## Manage Call Variables Layouts

### Call Variables Layouts

You can use the Call Variables Layouts gadget to define how call variables appear on the Finesse agent desktop. You can configure up to 200 unique Call Variables Layouts (one default and 199 custom layouts). As part of this functionality:

- Each layout has a name (required) and description (optional).
- You can change the name and description of the default Call Variables Layout.
- You cannot delete the default Call Variables Layout.
- Finesse appends (*Default*) to the name of the default Call Variables Layout.
- To display a custom Call Variables Layout, in the Unified CCX routing script, set the user.layout ECC variable to the name of a configured Call Variables Layout. In this case, if no custom layouts match the user.layout value (or no custom layouts are configured), Finesse displays the default layout.
- Finesse retains the custom layout as specified by the user.Layout ECC variable on CTI server failover. During PG failover, Finesse changes the active call layout to the default layout while retaining the call variables and time indicators.

### Call Variables

Each Call Variables Layout supports one variable in the header of the call control gadget and up to a total of 20 variables in two columns below the header (up to 10 in each column). You can use call variables, Extended Call Context (ECC) variables, or the following Outbound Option ECC variables:

- BACampaign
- BAAccountNumber
- BAResponse
- BASTatus
- BADialedListID
- BATimeZone
- BABuddyName

Columns can be empty.

The administrator can include the following additional fields in the Call Variables Layout. These variables appear as a drop-down list in the call variable gadget which the admin can assign to a layout.

- queueNumber
- queueName
- callKeyCallId
- callKeyPrefix
- callKeySequenceNum
- wrapUpReason




---

**Note** The callKeyPrefix indicates the day when the call was routed.

The callKeyCallId indicates the unique number for the call routed on that day.

To uniquely locate the call in Unified CCE database records, concatenate the two variables callKeyPrefix and callKeyCallId.

---

To enable Outbound Option data to appear in Cisco Finesse, the administrator must edit the Default Layout to include some or all Outbound Option variables.

## Edit Call Variables

Administrator can set call variables (callVariable1 to callVariable10) values and ECC variable values as editable. Amongst BA (campaign-based outbound calls) variables, only BAResponse can be edited. The agent and the supervisor can edit the call variable values during an active call or in the wrap-up state.




---

**Note**

- Cisco Finesse refers to the ECC variable length from the AWDB and this length is validated while you edit the ECC variable. Cisco Finesse server takes about 15 minutes to update these changes from AWDB. Agents must sign in again for the ECC variable configuration changes to reflect in the Cisco Finesse desktop.

- 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 Agent PG, 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.
- 




---

**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 Agent PG, 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.

---

## Configure Call Variables Layouts

### Procedure

---

- Step 1** From the Manage Call Variables Layouts gadget:
- Click **New** to create a new Call Variables Layout.
  - Choose a layout from the list and click **Edit** to modify an existing Call Variables Layout (or click **Delete** to remove it).
- Step 2** Under **Create New Layout** (or under Edit <layout name> when editing an existing layout):
- Enter a name for the Call Variables Layout (maximum 40 characters).
  - Enter a description of the Call Variables Layout (maximum 128 characters).
- Step 3** Under Call Header Layout:
- Enter the display name that you want to appear in the header of the Call Control gadget on the Finesse desktop. For example, Customer Name (maximum 50 characters).
  - From the drop-down list, choose the call variable or Outbound Option ECC variable that you want to appear in the header. For example, callVariable3 (maximum 32 characters).
- Step 4** In the Call Body Left-Hand Layout and Call Body Right-Hand Layout areas:
- a) Click **Add Row** to add a new row (or click the “X” to delete a row).
  - b) For each row:
    - Enter the display name that you want to appear on the desktop. For example, Customer Name (maximum 50 characters).
    - Enter the corresponding call variable or Outbound Option ECC variable from the drop-down list (maximum 32 characters).
- Step 5** Select up to five call variables using the check box. The selected call variables are displayed in agent call popover and supervisor active call details.
- Note** If you do not select any call variables, the first two call variables from the Call Body Left-Hand layout area will be displayed in the agent call popover and supervisor active call details. If there are no call variables in the Left-hand layout area, then the call variables in the Right-Hand Layout will be selected.
- Step 6** Turn on the toggle switch to enable the edit option for a specific call variable. By default, this option is turned off.
- Note**
- Call variable (callVariable1 to callVariable10) values are editable.
  - ECC variable values are editable.
  - Amongst BA variables (campaign-based outbound calls), only BAResponse value is editable.
- Step 7** Click **Save** to save the changes, or **Cancel** to discard the changes.

**Note** When you modify the Call Variables Layout of the agent desktop, the changes you make take effect after three seconds. However, agents or supervisors who are signed in when the changes are made must sign out and sign back in to see those changes reflected on their desktops.

**Step 8** To view the latest configured Call Variables Layout, click **Refresh** from the Manage Call Variables Layouts gadget.

---

## Add ECC Variables to Call Variables Layout

### Procedure

---

**Step 1** In the header or the row where you want the ECC variable to appear, from the Variable drop-down list, choose **Custom**.

**Step 2** In the Custom/ECC Variable Name field, enter the name of the ECC variable you want to appear on the agent desktop.

**Step 3** Click **Set**.

The ECC variable now appears in the Variable drop-down list for selection.

---

## Assign Call Variables Layouts

### Procedure

---

**Step 1** In Cisco Unified CCX Editor, open the script for which you want to assign ECC call variables.

**Step 2** Select **Expanded Call Variables** from **Settings**.

**Step 3** Click **New Variable** icon.

**Step 4** Create a variable with "user" as prefix.

For example: userSSN

**Step 5** In **Set Enterprise Call Info** step of the script, add or modify the **Expanded Call Variables**.

---

## Manipulate Call Variables Layouts with a Workflow

You can manipulate the call variables layout that an agent sees when a call is answered by using a workflow. To do so, configure an HTTP Request workflow action and set the value of the ECC variable user. Layout to the name of the custom layout to display.

For information about how and when workflows are executed, see **Workflows and Workflow Actions**.

For more details, see the section, "Adding an HTTP Request Workflow Action" in the white paper *Cisco Finesse: How to Create a Screen-Pop Workflow*.

## Manage Desktop Layout

You can define the layout of the Finesse desktop on the Desktop Layout tab.



### Important

Requirements, such as processor speed and RAM, for clients that access the Finesse desktop can vary. Desktops that receive events for more than one agent (such as agent and supervisor desktops running Live Data reports that contain information about other agents and skill groups) require more processing power than desktops that receive events for a single agent.

Factors that determine how much power is required for the client include, but are not limited to, the following:

- Contact center traffic
- Additional integrated gadgets in the desktop (such as Live Data reports or third-party gadgets)
- Other applications that run on the client and share resources with the Finesse desktop

## Gadgets and Components

### Gadgets

Cisco Finesse is an OpenSocial gadget, which is an XML document that defines metadata for an OpenSocial Gadget container. The gadgets are applications that are placed within the Cisco Finesse desktop. This helps administrator to provide access to the contact center agents for all the applications that is required to service calls inside a single application.

Cisco Finesse comes with default gadgets such as, the team performance gadget, call control gadget, and call popover. JavaScript library is available for any customers with specific requirements that are not available out of the box.

Gadgets are listed in the desktop layout using the `<gadget>` tag.



### Note

Finesse Desktop is tested to perform well with an average of 20 gadgets per Desktop (across all tabs), over a sign in period of 8 minutes for 2000 users (agents and supervisors). When you increase the total number of gadgets that are configured on the Desktop, the CPU consumption marginally increases during users sign in. When all the configured gadgets are enabled for all the users, it impacts the Finesse server. Higher number of gadgets will also need more browser memory and network bandwidth.

If considerably larger number of gadgets are configured or if more users sign in (more than the tested number of users) in a short time frame, you must monitor the CPU consumption and network bandwidth during users sign in and ensure that the end-point devices have enough memory.

Failover uses optimization to sign in the users quickly and is not considered the same as a new browser sign in.

Third-party gadgets are hosted on the Cisco Finesse server using the `3rdpartygadget` web application or on an external web server. Gadgets can make REST requests to services hosted on external servers using the Cisco Finesse JavaScript Library API. To avoid browser cross-origin issues, REST requests are proxied

through the backend Shindig web application. Third-party gadgets must implement their own authentication mechanisms for third-party REST services.

For more information about gadgets, see <https://developer.cisco.com/docs/finesse/>.

### Components

Components are simple scripts that are loaded into the desktop directly at predefined positions as directed by the layout, without an enclosing frame and its document.

Components are introduced in the desktop to overcome a few rendering limitations and performance considerations inherent to gadgets.

The `<component>` tag lists the components in the desktop layout. Currently, the layout validations prevent creating custom components. Hence, default components are allowed in the desktop layouts. The default desktop functionalities are currently registered as components to provide flexibility and to reduce the load on the server.

## Finesse Desktop Layout XML

The Finesse Layout XML defines the layout of the Finesse desktop, and the gadgets and components displayed on the desktop.

Use the Manage Desktop Layout gadget to upload an XML layout file to define the layout of the Finesse desktop for agents and supervisors.

Actions on the **Manage Desktop Layout** gadget are as follows.

- Edit the code using any of the following editors:
  - **Text Editor**
  - **XML Editor**
- **View Default Layout** - Displays the Cisco Finesse default layout.
- **Restore Default Layout** - Restores the Cisco Finesse desktop to the default layout.
- **Save** - Saves your configuration changes.
- **Revert** - Retrieves and applies the most recently saved desktop layout.

## Default Layout XML

The Finesse default desktop layout XML for Unified CCX contains optional tabs and gadgets for Web Chat and Email, Advanced Supervisor Capabilities, and notes that describe how to modify the layout for your deployment type.

Remove the comments from the optional gadgets and tabs that you want to appear on the Finesse desktop.

Remove any gadgets or tabs that you do not want to use.

The **Manage Desktop Layout** supports the following types of editors:

- **Text Editor**—A plain text editor. It is the default editor. You can use the **Expand All** option to see all the code details and Search text box to refine your search results.
- **XML Editor**—An XML editor.





- 
- Note**
- You cannot add or edit comments (<!-- and -->) in the **XML Editor**.
  - In this document, all the examples that are related to desktop layout are applicable for text editor.
- 

Both the editors support the following features:

- Expand and collapse option
- Syntax highlights and color code for the visual indication
- Auto-complete suggestions and hints for valid elements in the tags

Following are the updates available in the default layout XML in Unified CCX 12.5(1) release:

- Sample configurations for customizing desktop properties are added to the default layout (**Desktop Layout**) and team-specific layout (**Team Resources > Desktop Layout**).  
For upgraded layouts, sample configurations for customizing desktop properties do not appear by default. The administrator must copy the XML from the **View Default Layout** and add to the respective custom layouts.
- Horizontal Header is available in the layout configuration and the Header can be customised.
- Title and Logo of Finesse desktop can be customised.
- Desktop Chat, TeamMessage, Dialer, Agent Identity, and Non-Voice State Control are added as part of the header component.
- Vertical tabs in Finesse desktop are moved to collapsable left navigation bar for which the icons can be customised.
- Support for inbuilt java script components has been added.
- The **ID** attribute (optional) is the ID of the HTML DOM element used to display the gadget or component. The ID should start with an alphabet and can contain alpha numeric characters along with hyphen(-) and underscore(\_).It can be set through the Finesse Administrative portal and has to be unique across components and gadgets.
- The **managedBy** attribute (optional) for Live Data gadgets defines the gadgets which manage these Live Data gadgets. The value of **managedBy** attribute for Live Data gadgets is **team-performance**. This means that the rendering of the gadget is managed by the Team Performance gadget. These gadgets are not rendered by default, but will be rendered when the options Show State History and Show Call History are selected in the Team Performance gadget.

For upgraded layouts, the **managedBy** attribute will be introduced, and will have the value of the **ID** of the Team Performance gadget in the same tab. If there are multiple instances of Team Performance gadgets and Live Data gadget pairs, they will be associated in that order. If the **ID** of the Team Performance gadget is changed, the value of the **managedBy** attribute should also be updated to reflect the same **ID** for the Live Data gadgets. Otherwise, the Team Performance gadget instance will not show its respective Live Data gadgets.

- The **Hidden** attribute (optional) is used to support headless gadgets. When an attribute is set to "hidden=true", then the gadget is loaded by the container, but will not be displayed. The default value set for the attribute is "false".
- The **maxRow** attribute (optional) is used to adjust the height of the Team Performance gadget. If there are multiple instances of the Team Performance gadget, each instance height can be set by using this attribute. By default the **maxRow** attribute value is set to 10 rows.
- Agents can view Recent Call History and Recent State History gadgets in the My History tab.
- Supervisors can view Recent Call History and Recent State History gadgets in the My History tab.

**Important**

After a system upgrade, the old desktop layout is retained. If you had a modified desktop layout before upgrade, perform the following steps to ensure you obtain the latest changes:

- Sign in to the Finesse administration console and click the **Desktop Layout** tab.
- Copy the desktop layout to a text file.
- On the Manage Desktop Layout gadget, click **Restore Default Layout**.
- Click **Save**.
- Using the text file of the desktop layout that you saved before the upgrade as a reference, modify the layout to include the changes that you made to the previous layout.
- Click **Save** to save your changes.

If any changes are made to the component IDs or URLs in the default XML layout, the following features may not work as expected.



**Note** The components can be rearranged in any order to show on the Finesse desktop.

Feature	Component ID	URL
Title and Logo	cd-logo	<url>/desktop/scripts/js/logo.js</url>
Voice State control	agent-voice-state	<url>/desktop/scripts/js/agentvoicestate.component.js</url>
Non-voice state control	nonvoice-state-menu	<url>/desktop/scripts/js/nonvoice-state-menu.component.js</url>
Team Message	broadcastmessagepopover	<url>/desktop/scripts/js/teammessage.component.js</url>
Desktop Chat	chat	<url>/desktop/scripts/js/chat.component.js</url>
Dialer	make-new-call-component	<url>/desktop/scripts/js/makenewcall.component.js</url>
Agent identity	identity-component	<url>/desktop/scripts/js/identity-component.js</url>

## Update Default Desktop Layout

When you modify the layout of the Finesse desktop, the changes you make take effect on the desktop after 3 seconds. However, agents who are signed in when the changes are made must sign out and sign in again to see those changes reflecting on the desktop.



**Note** The call control gadget is only supported at the page level. You must ensure that the call control gadget (`<gadget>/desktop/scripts/js/callcontrol.js</gadget>`) is placed within the `<page></page>` tag for it to work correctly. Do not place this gadget within a `<tab></tab>` tag.

The version tag of Desktop Layout XML cannot be edited.

For the changes to take effect, refresh the page, or sign out and sign in again into Cisco Finesse.

### Procedure

- Step 1** Click **Desktop Layout**.
- Step 2** Select from the following editors:
- **Text Editor**
  - **XML Editor**
- Step 3** Make changes to the XML as required.

#### Example:

If you want to add a new tab called Reports, add the following XML within the tabs tags under the `<role>Agent</role>` tag:

```
<tab>
  <id>reports</id>
  <icon>Reports</icon>
  <label>Reports</label>
</tab>
```

If you want to add this tab to the supervisor desktop, add the XML within the tabs tags under the `<role>Supervisor</role>` tag.

To add a gadget to a tab, add the XML for the gadget within the gadgets tag for that tab.

```
<gadgets>
<gadget>https://<ipAddress>/gadgets/<gadgetname>.xml</gadget>
</gadgets>
```

Replace `<ipAddress>` with the IP address of the server where the gadget resides.

If you want to add multiple columns to a tab on the Finesse desktop, add the gadgets for each column within the columns tags for that tab. You can have up to four columns on a tab.

```
<tabs>
  <tab>
    <id>home</id>
    <icon>home</icon>
    <label>finesse.container.tabs.agent.homeLabel</label>
    <columns>
```

```

        <column>
          <gadgets>
            <gadget>/desktop/scripts/js/queueStatistics.js</gadget>
          </gadgets>
        </column>
      </columns>
    </tab>
  <tab>
    <id>myHistory</id>
    <icon>history</icon>
    <label>finesse.container.tabs.agent.myHistoryLabel</label>
    <columns>
      <column>
        <!-- The following gadgets are used for viewing the call history
and state history of an agent. -->
      </column>
    </columns>
  </tab>

```

**Step 4** Click **Save**.

Finesse validates the XML file to ensure that it is valid XML syntax and conforms to the Finesse schema.

**Step 5** After you save your changes, if you want to revert to the last saved desktop layout, click **Revert**. If you want to revert to the default desktop layout, click **Restore Default Layout**.

**Note** During upgrade, any changes made to the Cisco Finesse Default Layout will be not be updated. You need to click on **Restore Default Layout** to get the latest changes.

---

The Finesse default XML layout is as follows:

```

<finesseLayout xmlns="http://www.cisco.com/vtg/finesse">
  <layout>
    <role>Agent</role>
    <page>
      <gadget>/desktop/scripts/js/callcontrol.js</gadget>
    </page>
    <tabs>
      <tab>
        <id>home</id>
        <label>finesse.container.tabs.agent.homeLabel</label>
        <gadgets>
          <gadget>/desktop/scripts/js/queueStatistics.js</gadget>
        </gadgets>
      </tab>
    </tabs>
  </layout>
<!--
  The following Gadgets are for LiveData. They are *ONLY* supported in a Packaged CCE
Deployment.
  If you are using Packaged CCE and wish to show LiveData Reports, then do the following:

  1) Uncomment out each Gadget you wish to show.
  2) Replace all instances of "my-cuic-server" with the Fully Qualified Domain Name
of your Intelligence Center Server.
  3) [OPTIONAL] Adjust the height of the gadget by changing the "gadgetHeight"
parameter.

  IMPORTANT NOTES:
  - In order for these Gadgets to work, you must have performed all documented
pre-requisite steps.
  - The use of HTTP/HTTPS *must* match what your Users use for the Finesse Desktop
(HTTP or HTTPS).
-->

```

- If you wish to use HTTP, then HTTP must be enabled on both Finesse and Intelligence Center.

- Do \*NOT\* change the viewId (unless you have built a custom report and know what you are doing).

- The "teamName" will be automatically replaced with the Team Name of the User logged into Finesse.

-->

```

<!-- HTTPS Version of LiveData Gadgets -->
  <!-- "Agent" Report -->
  <!-- <gadget>https://my-cuic-server:8444/cuicui/gadget/LiveData/
    LiveDataGadget.xml?gadgetHeight=310&viewId=
    99E6C8E210000141000000D80A0006C4&filterId=
    agent.id=CL%20teamName</gadget> -->
  <!-- "Agent Skill Group" Report -->
  <!-- <gadget>https://my-cuic-server:8444/cuicui/gadget/LiveData/
    LiveDataGadget.xml?gadgetHeight=310&viewId=
    9AB7848B10000141000001C50A0006C4&filterId=
    agent.id=CL%20teamName</gadget> -->
  <!-- "Agent All Fields" Report -->
  <!-- <gadget>https://my-cuic-server:8444/cuicui/gadget/LiveData/
    LiveDataGadget.xml?gadgetHeight=310&viewId=
    9A08E23510000141000001230A0006C4&filterId=
    agent.id=CL%20teamName</gadget> -->
  <!-- "Agent Skill Group All Fields" Report -->
  <!-- <gadget>https://my-cuic-server:8444/cuicui/gadget/LiveData/
    LiveDataGadget.xml?gadgetHeight=310&viewId=
    A30EC25810000141000003A60A0006C4&filterId=
    agent.id=CL%20teamName</gadget> -->
<!-- HTTP Version of LiveData Gadgets -->
  <!-- "Agent" Report -->
  <!-- <gadget>http://my-cuic-server:8081/cuicui/gadget/LiveData/
    LiveDataGadget.xml?gadgetHeight=310&viewId=
    99E6C8E210000141000000D80A0006C4&filterId=
    agent.id=CL%20teamName</gadget> -->
  <!-- "Agent Skill Group" Report -->
  <!-- <gadget>http://my-cuic-server:8081/cuicui/gadget/LiveData/
    LiveDataGadget.xml?gadgetHeight=310&viewId=
    9AB7848B10000141000001C50A0006C4&filterId=
    agent.id=CL%20teamName</gadget> -->
  <!-- "Agent All Fields" Report -->
  <!-- <gadget>http://my-cuic-server:8081/cuicui/gadget/LiveData/
    LiveDataGadget.xml?gadgetHeight=310&viewId=
    9A08E23510000141000001230A0006C4&filterId=
    agent.id=CL%20teamName</gadget> -->
  <!-- "Agent Skill Group All Fields" Report -->
  <!-- <gadget>http://my-cuic-server:8081/cuicui/gadget/LiveData/
    LiveDataGadget.xml?gadgetHeight=310&viewId=
    A30EC25810000141000003A60A0006C4&filterId=
    agent.id=CL%20teamName</gadget> -->

  </gadgets>
</tab>
<tab>
  <id>manageCall</id>
  <label>finesse.container.tabs.agent.manageCallLabel</label>
</tab>
</tabs>
</layout>
<layout>
  <role>Supervisor</role>
  <page>
    <gadget>/desktop/scripts/js/callcontrol.js</gadget>
  </page>
</tabs>
  <tab>

```

```

        <id>home</id>
        <label>finesse.container.tabs.supervisor.homeLabel</label>
        <gadgets>
            <gadget>/desktop/scripts/js/teamPerformance.js</gadget>
            <gadget>/desktop/scripts/js/queueStatistics.js</gadget>
        </gadgets>
    </tab>
    <tab>
        <id>manageCall</id>
        <label>finesse.container.tabs.supervisor.manageCallLabel</label>
    </tab>
</tabs>
</layout>
</finesseLayout>

```

## 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.
- When you resize the browser, based on the width of the browser, gadgets in the desktop layout are organized one below the other.




---

**Note** By default, the drag-and-drop and resize features are disabled. The administrator must set the `enableDragDropAndResizeGadget` desktop property value as `true` to enable these features.

---

The administrator can customize the desktop property value of these features through the desktop layout:

- **Default layout (Desktop Layout)**—In the **Text Editor**, remove the comment (`<!--and -->`) from the `enableDragDropAndResizeGadget` code snippet and enter the value as `true` to add these features to the desktop layout. For more information, see [Customize Desktop Properties, on page 27](#).

The following is the sample code snippet, as displayed in the default **Desktop Layout**.

```
<!-- <config key="enableDragDropAndResizeGadget" value="false"/> -->
```

- **Team-specific layouts (Manage Team Resources > Desktop Layout)**—Select a specific team and then in the **Text Editor**, remove the comment (`<!--and -->`) from the `enableDragDropAndResizeGadget` code snippet and enter the value as `true` to add these features to the team desktop layout. For more information, see [Customize Desktop Properties at Team Level, on page 85](#).

The following is the sample code snippet, as displayed in the team **Desktop Layout**.

```
<!-- <config key="enableDragDropAndResizeGadget" value="false"/> -->
```

**Note**

- For upgraded layouts, the sample configuration for customizing desktop property (`enableDragDropAndResizeGadget`) doesn't appear by default in the **Desktop Layout**. Administrators must copy the XML from the **View Default Layout** and add to the respective custom layouts.
- For new layouts, the sample configuration for customizing desktop property (`enableDragDropAndResizeGadget`) appears by default in the **Desktop Layout**.
- The administrator can also use the CLI and set the `utils finesse set_propertydesktop enableDragDropAndResizeGadget` to `true` to enable these features. For more information see *Desktop Properties*.
- 
- If the property value is defined in the team-specific desktop layout (**Manage Team Resources > Desktop Layout**), the team-specific desktop layout takes precedence over the property value defined in the **Desktop Layout** and CLI.
- These features aren't applicable for gadgets that don't have a defined title. For more information, see the *Gadget Limitations* section in the *Cisco Finesse Web Services Developer Guide* at <https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide>.

## Customize Desktop Properties

You can customize the Finesse desktop properties.

### Procedure

- Step 1** Click **Desktop Layout**.
- Step 2** Select from the following editors:
- **Text Editor**
  - **XML Editor**
- Step 3** Enter the desktop property name in the config key tag.
- Step 4** Enter the possible value of the desktop property in the value tag.

The following are the sample desktop property entries, as displayed in the default **Desktop Layout**. To change these desktop property entries in **Text Editor**, remove the comment (`<!--` and `-->`) and set appropriate values.

**Note** If the property value is defined in the **Desktop Layout**, then the **Desktop Layout** value takes precedence over the property value defined using the CLI. For more information on Finesse CLIs, see *Desktop Properties*.

The following table lists the supported desktop properties:

Config Key	Value	Default Value
<code>enableDragDropAndResizeGadget</code>	<code>true false</code>	<code>false</code>
<code>enableShortCutKeys</code>	<code>true false</code>	<code>true</code>

Config Key	Value	Default Value
forceWrapUp	true false	true
wrapUpCountDown	true false	true
showWrapUpTimer	true false	true
desktopChatAttachmentEnabled	true false	true
desktopChatMaxAttachmentSize	Range: 1—10 (MB)	5
desktopChatUnsupportedFileTypes	Unsupported file formats include comma-separated valid file extensions. For example: .exe, .sh	.exe, .msi, .sh, .bat
showAgentHistoryGadgets	true false	true
showActiveCallDetails (for Supervisor Only)	true false	true
pendingDTMFThresholdCount	Range: 1—20	20
dtmfRequestTimeoutInMs	Range: 1000—200000 (1 to 200 seconds)	5000 (5 seconds)
enableDropParticipantFor	supervisor_only conference_controller_ and_supervisor all	supervisor_only
dropParticipant	agents all	agents

- Note**
- To enable the following Finesse desktop properties in Cisco Finesse, install Cisco Finesse Release 12.5(1) ES1 COP or higher.
    - pendingDTMFThresholdCount
    - dtmfRequestTimeoutInMs
  - To enable the following Finesse desktop properties in Cisco Finesse, install Cisco Finesse Release 12.5(1) ES4 COP or higher.
    - enableDropParticipantFor
    - dropParticipant

For more information on Finesse desktop properties, see *Desktop Properties*.

**Step 5** Click **Save**.

The change takes effect when the agent or supervisor refreshes the Finesse desktop or sign out and sign in again.



**Note** If you clear the **Override System Default** check box and click **Save**. The changes are overwritten, and the editing pane reverts to the default desktop layout XML.

## Horizontal Header

The Horizontal Header on the Finesse desktop has the following components from left to right. All these components can be removed and replaced with custom gadgets as required.

- **Logo:** Default is Cisco logo. Can be customized.
- **Product Name:** Default is Cisco Finesse. Can be customized.
- **Agent State for Voice:** Displays agent state for voice call.
- **Agent State for Digital Channels:** Displays agent state for digital channels.
- **Dialer Component:** Agent can make a new call.
- **Identity Component:** Displays agent name and signout functionality with reason codes.



**Note** The sum of widths set for all gadgets and components in the header (inside right aligned columns and left aligned columns) should not exceed the total header width. If it exceeds the header width, some of the gadgets/components will not be visible.

## Customize Title and Logo in the Header

You can customize the title and logo displayed on the Finesse desktop:

### Procedure

- Step 1** Click **Desktop Layout**.
- Step 2** Select from the following editors:
- **Text Editor**
  - **XML Editor**
- Step 3** Enter the product name in the config value tag with title key.
- Step 4** Upload the logo file just like any third-party gadget.  
For more information, see section *Upload Third-Party Gadgets* in *Cisco Finesse Admin Guide*.
- Step 5** Enter the URL of the logo file in the config value tag with logo key.

### Example:

```
<configs>
  <!-- The Title for the application which can be customised.-->
  <config value="product.full-name" Key="title"/>
  <!-- The logo file for the application-->
```

```
<!--<config key="logo" value="/3rdpartygadgets/<some_sample_image>"-->
</configs>
```

The customized logo and product name is displayed on the Finesse desktop.



**Note** The file size that can be uploaded for the logo must be kept within 40 pixels. The file types supported are .svg, .png, .gif, and .jpeg/jpg.

## alternateHosts Configuration

The `<gadget>` element in the Finesse Layout XML provides an attribute to specify alternate hosts from which the gadget can be loaded. This allows the Cisco Finesse desktop to load the gadget using a different host if the primary server is unavailable.

The **alternateHosts** attribute contains a comma-separated list of FQDNs that will be used if the primary-host-FQDN is unavailable.

```
<gadget alternateHosts="host1,host2,host3,...">
  https://<primary-host-FQDN>/<gadget-URL>
</gadget>
```

The **alternateHosts** attribute is only applicable for gadgets with an absolute URL. That is URLs containing the FQDN of a host, an optional port, and the complete URL path to the gadget. For example: `<gadget alternateHosts="host1,host2">https://primary host/relative_path</gadget>`

If loading the gadget from the primary-host fails, the Cisco Finesse container attempts to load the gadget from the alternate hosts in the order specified in the **alternateHosts** attribute.

The Cisco Finesse desktop may fail to load the gadget even if some of the hosts are reachable. In such cases, refresh the Cisco Finesse desktop.

When the gadget is specified with a relative URL, for example: `<gadget >/3rdpartygadgets/relative_path</gadget>`, the **alternateHosts** attribute does not apply and is ignored by the Cisco Finesse desktop.



**Note** If the host serving the gadget fails after the Cisco Finesse desktop was successfully loaded, the desktop must be refreshed in order to load the gadget from an alternate host. The gadget does not implement its own failover mechanism.

## Headless Gadget Configuration

Headless gadgets are gadgets which do not need a display space, but can be loaded and run like a background task in the browser. The **Hidden** attribute (optional) is used to support headless gadgets in the layout XML. When an attribute is set to "hidden=true", then the gadget is loaded by the container, but will not be displayed. The default value set for the attribute is "false".

## Customize Icons in Left Navigation Bar

You can add icons (both custom and inbuilt) to the collapsible left navigation bar of the Finesse desktop:

## Procedure

---

- Step 1** Click **Desktop Layout**.
- Step 2** Select from the following editors:
- **Text Editor**
  - **XML Editor**
- Step 3** Enter name of the gadget or component in the id tag.
- Step 4** Enter the value of the icon in the icon tag.
- Step 5** Upload the icon file just like any third-party gadget.

For more information, see section *Upload Third-Party Gadgets* in *Cisco Finesse Admin Guide*.

**Note** When adding a custom icon, provide the path in the icon tag and if you are adding an inbuilt icon, provide the icon value in the icon tag

### Example:

**Note** The file size that can be uploaded in the left navigation bar as custom icons is 25 pixels by 25 pixels. The maximum width of the tab title in the left navigation bar must be 80 pixels or less. The file types supported are .svg, .png, .gif, and .jpeg/jpg.

---

## Customize Icons for Gadgets





















As part of the Cisco Finesse container, various standard icons are available. Use the following procedure to customize the icons for the gadgets hosted in Finesse desktop.

## Procedure

---

- Step 1** Click **Desktop Layout**.
- Step 2** Select from the following editors:
- **Text Editor**
  - **XML Editor**

**Step 3** Enter the value of the icon in the icon tag. Get the icon name from the [List of Icons, on page 33](#). The icon name is located on the right of the icon image. For example, search.

	search ← Icon Name		remove-contain
	dial		remove-outline
	keyboard		close
	close-keyboard		exit-contain
	delete		exit-outline
	trash		refresh
	add		more
	add-contain		sign-in
	add-outline		forced-sign-in
	Remove / Delete		sign-out

510878

**Note** Icon name is case sensitive. Enter the icon name exactly as displayed in the [List of Icons, on page 33](#).

### Example





















An example of the desktop layout using the *Search* and *Close-Keyboard* icons.

```
<tab>
  <id>home</id>
  <icon>search</icon>
  <label>finesse.container.tabs.agent.homeLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>/desktop/scripts/js/queueStatistics.js</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
<tab>
  <id>sample</id>
  <icon>close-keyboard</icon>
  <label>finesse.container.tabs.agent.homeLabel2</label>
  <columns>
    <column>
      <gadgets>
        <gadget>/desktop/scripts/js/samplequeue.js</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```





















```
</columns>
</tab>
```

### List of Icons













The following are the icons for Actions.

	search		remove-contain
	dial		remove-outline
	keyboard		close
	close-keyboard		exit-contain
	delete		exit-outline
	trash		refresh
	add		more
	add-contain		sign-in
	add-outline		forced-sign-in
	Remove / Delete		sign-out











The following are the icons for Audio.

	microphone		line-out-right
	mute		audio-settings
	mic-in		headset
	speaker		headset-cross
	speaker-cross		active-speaker
	volume-cross		locked-speaker
	audio-min		active-speaker-cross
	audio		bluetooth-contain-cross
	speaker-out-left		handset-cross
	line-out-left		headset-outline























The following are the icons for Camera.

	video		zoom-in
	video-cross		zoom-out
	aux-camera		
	self-view		
	self-view-crossed		
	self-view-alt		
	web-camera		
	camera		
	swap-camera		
	swap-video-camera		







The following are the icons for Chat.

	chat
	chats
	persistent-chat
	comment
	waiting-silence
	broadcast-message
	invite
	send
	emoticons
	bot-outline

















The following are the icons for Collaboration.

	schedule-add		leave-meeting		micro-blog
	day		community		timeline
	week		web-sharing		bookmark
	calendar-icon-date		mobile-presenter		chapters
	external-calendar		presentation		feedback
	instant-meeting		slides		like
	webex		point		
	meeting-room		extension-mobility		
	conference		participant-list		
	meet-me		browser		

The following are the icons for Contacts.


























	contact
	add-contact
	remove-contact
	directory
	contact-card
	star

The following are the icons for Content.

	attachment		watchlist
	link		playlist
	document		prevent-download
	create-page		prevent-download-container
	move-page		download
	notes		download-contain
	image		upload
	folder		upload-contain
	export		share
	import		share-contain

The following are the icons for Editor.

















	edit		screen-capture-square		view-feed-multi
	draw		popout		video-preview-telePresence
	transcript		filter		panel-slides-left
	annotation		picture-in-picture		panel-slides-right
	list-view		video-layout		print
	thumbnail-view		layout		
	text-format		view-side-by-side		
	text-color		view-stacked		
	text-size		view-feed-single		
	fullscreen		view-feed-dual		








The following are the icons for Email.

	email		send-email
	read-email		
	spam		
	inbox		
	outbox		
	sent		
	universal-inbox		
	arrow-right-tail		
	arrow-left-tail		
	reply-all		
















The following are the icons for Hardware.

	display		power
	multi-display		dc-power
	soft-phone		ac-power
	video-input		power-contain
	computer		charging
	notebook-in		battery
	devices		
	idefix		
	mobile-phone		
	tablet		















The following are the icons for Media.

	image
	sound
	music
	graph
	text
	tables
	zip

The following are the icons for Navigation.

	home		hamburger-menu
	android-home		way-nav
	right-arrow		right-arrow-contained
	right-arrow-contain		right-arrow-closed-contained
	right-arrow-outline		right-arrow-closed-outline
	touch		
	touch-point		
	touch-gesture		
	back		
	recent-apps		

The following are the icons for Network.

	wifi		signal-3
	proximity		signal-4
	proximity-not-connected		public-network
	bluetooth		private-network
	bluetooth-contained		
	bluetooth-outline		
	ethernet		
	no-signal		
	signal-1		
	signal-2		

The following are the icons for Notifications and Alerts.

	warning		quality		location
	alert-badge		broken-image		compass
	error		blocked		flagged
	info		check		keywords
	help		certified	DMS	dms
	lock		bell		popup-dialog
	unlock		bell-cross		applications
	private		alarm		application
	privacy		running-application		default-app
	report		pin		













510892

The following are the icons for Phone.






























	calls		incoming-call		call-forward-divert		key-expansion-module
	other-phone		outgoing-call		merge-call		desk-phone
	call-log		missed-call		group-call		
	work		rtprx		hunt-group		
	desk-phone		rtptx		edit-call		
	voicemail		rtprx-rtptx-duplex		intercom		
	callback		speed-dial		intercom-whisper		
	redial		off-hook		intercom-duplex-connected		
	DND		alerting		forward-to-mobility		
	swap-calls		parked		transfer-to-mobile		

510893






The following are the icons for Sources.

	pc		sd
	disc		custom-desktop
	document-camera		
	whiteboard		
	general-source		
	disc-not-connected		
	document-camera-cross		
	whiteboard-cross		
	general-source-cross		
	usb		































































The following are the icons for Settings.

	settings		animation		reset
	sliders		accessibility		backup-data
	user		setup-assistant		bug
	admin		tools		lock-contain
	activities		hue		ground
	profile-settings		brightness		storage
	ringer-settings		volume		data-usage
	language		call-rate		numbered-inputs
	wallpaper		vibrate		numbered-outputs
	manage-cables		time		

The following are the icons for Video Controls.

-  play
-  play-container
-  stop
-  pause
-  skip-fw
-  skip-bw
-  ffw
-  fbw
-  circle

































The following are the icons for Miscellaneous Icons.








































	circle-bar chart		circle-pie chart		line-chart		D
	circle-column chart		unknown-customer		inbound-call		R
	dashboard		circle-note		outbound-call		RD
	circle-gauge		circle-custom-widget		call-back		SC
	circle-line chart		grid		phone-outline		SE
	event		bar-chart		chat-outline		VL
	social		bars		circle-grid		organization-setup
	web		text-and-font		drag-row		campaign-outbound
	node		report-view		edit-properties		desktop-agent
	formula		resize		key		
	maximize		manage-team		thumbs-down-outline		
	save		manage-call		thumbs-up-filled		
	history		analysis		thumbs-down-filled		
	minimize		analysis-active				
	tabs		manage-chat				
	vd-silent-monitoring		manage-email				
	time-arrow		reports-more				
	device-outSync		fb-chat				
	team-data		fb-group-chat				
	phone-cross		thumbs-up-outline				

510898

510899

## List of Icons







































	applause		folder		recurring		webhook
	at		highlighter		rotate-object-ccw		paired-audio
	at-contain		highlighter-check		rotate-object-cw		
	bot-one		highlighter-line		Spark		
	bot-two		integration		team-collapsed-view		
	bot-three		media-viewer		team-expanded-view		
	bot-four		paired-call		too-fast		
	cisco-logo		pencil		too-slow		
	feedback-clear		Q and A		video-group		
	feedback-result		raise-hand		video-tips		

	arrow-back		asterisk		circle-analysis		content-share
	arrow-down		audio-broadcast		circle-care		data
	arrow-next		bottom		circle-location		device-inProgress
	arrow-up		chevron-down		circle-supervisor		device-inSync
	call-forwarding		chevron-left		circle-webex		diagnostics-active
	call-handling		chevron-right		clipboard		diagnostics
	care-filled		chevron-up		clock		edit-time
	chat-active		checkbox		cloud-active		end-call
	check-gear		circle-agent		cloud		endpoint-active
	check-refresh		eraser		company-active		

510900

510901



	Euro		info-outline		panel-close		screen-capture
	help-outline		laser-pointer		pass-mouse		settings-active
	filter		left-arrow		plan-review		sort
	glyphicon-calendar		lightbulb		people-active		tools-active
	glyphicon-time		location-active		plugin		top
	grid-large		manage-recordings-tab		poll		user-chat
	grid-list		manage-recordings		priority		video-settings
	home-active		minus		plus		yen
	image-contain		new-call		question-circle		
	eraser		paired-call-outline		report-definition		

510902

For more information on customizing the visual experience, see *Visual Design Kit* at <https://developer.cisco.com/docs/finesse/#!visual-design-guide>.

## XML Schema Definition

You must ensure that the XML uploaded conforms to the XML schema definition for Finesse. The XML schema definition for Finesse is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://www.cisco.com/vtg/finesse" targetNamespace="http://www.cisco.com/vtg/finesse"
elementFormDefault="qualified">
  <!-- definition of version element -->
  <xs:element name="version">
    <xs:simpleType>
      <xs:restriction base="xs:double">
        <xs:pattern value="[0-9\.]+" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <!-- The below elements are for common desktop header and configs -->
  <!-- Copied from:
https://github5.cisco.com/ccu-shared/common-desktop/blob/master/java/layout-manager/src/main/resources/layoutSchema.xsd
-->
  <!-- If the common-desktop XSD changes, this too needs to be updated -->
  <!-- Only difference is that, column has been renamed to headercolumn, since column is
already there in finesse desktop layout -->
  <xs:complexType name="configs">
    <xs:sequence>
      <xs:element name="config" type="config" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="config">
    <xs:attribute name="key">
```

```

        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[a-zA-Z]*" />
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="value" type="xs:string" />
</xs:complexType>
<xs:complexType name="header">
    <xs:choice>
        <xs:sequence>
            <xs:element name="leftAlignedColumns" type="listOfColumns" minOccurs="1"
maxOccurs="1" />
            <xs:element name="rightAlignedColumns" type="listOfColumns" minOccurs="0"
maxOccurs="1" />
        </xs:sequence>
        <xs:sequence>
            <xs:element name="rightAlignedColumns" type="listOfColumns" minOccurs="1"
maxOccurs="1" />
        </xs:sequence>
    </xs:choice>
</xs:complexType>
<xs:complexType name="component">
    <xs:sequence>
        <xs:element name="url" type="xs:string" minOccurs="1" maxOccurs="1" />
        <xs:element name="stylesheet" type="xs:string" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="id" use="required">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="."+ />
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="order">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[0-9]{0,10}" />
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
</xs:complexType>
<xs:complexType name="listOfColumns">
    <xs:sequence>
        <xs:element name="headercolumn" type="headercolumn" minOccurs="1"
maxOccurs="unbounded" />
    </xs:sequence>
</xs:complexType>
<xs:complexType name="headercolumn">
    <xs:choice minOccurs="0" maxOccurs="1">
        <xs:element ref="gadget" />
        <xs:element name="component" type="component" />
    </xs:choice>
    <xs:attribute name="width">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[0-9]+(px|%)" />
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
</xs:complexType>
<!-- The above elements are for common desktop header and configs -->
<!-- definition of role type -->
<xs:simpleType name="role">

```

```

        <xs:restriction base="xs:string">
            <xs:enumeration value="Agent" />
            <xs:enumeration value="Supervisor" />
            <xs:enumeration value="Admin" />
        </xs:restriction>
    </xs:simpleType>
    <!-- definition of simple elements -->
    <xs:element name="id">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:pattern value="[a-zA-Z]([-_:\.a-zA-Z0-9])*" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="label">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:minLength value="1" />
                <xs:pattern value="^[^\r\n]+" />
                <!-- This regex restricts the label string from carriage returns or newline
characters -->
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="icon" type="xs:anyURI" />
    <xs:element name="gadget">
        <xs:complexType>
            <xs:simpleContent>
                <xs:extension base="restrictWhiteSpaces">
                    <!-- <xs:attribute name="staticMessage" type="xs:string"/> -->
                    <xs:attribute name="id">
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:pattern value="[a-zA-Z]([-_a-zA-Z0-9])*" />
                            </xs:restriction>
                        </xs:simpleType>
                    </xs:attribute>
                    <xs:attribute name="alternateHosts" type="xs:string" />
                    <xs:attribute name="managedBy" type="xs:string" />
                    <xs:attribute name="hidden" type="xs:boolean" />
                </xs:extension>
            </xs:simpleContent>
        </xs:complexType>
    </xs:element>
    <xs:element name="role" type="role" />
    <xs:element name="gadgets">
        <!-- Grouping of a set of gadgets -->
        <xs:complexType>
            <xs:sequence minOccurs="0" maxOccurs="unbounded">
                <!-- No limit to number of gadget URIs for now -->
                <xs:element ref="gadget" />
                <!-- URI of the gadget xml -->
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:simpleType name="restrictWhiteSpaces">
        <xs:restriction base="xs:anyURI">
            <xs:minLength value="1" />
            <xs:pattern value="\S+" />
            <!-- This regex restricts anyURI from containing whitespace within -->
        </xs:restriction>
    </xs:simpleType>
    <xs:element name="column">
        <!-- Grouping of a set of gadgets within a column -->

```

```

<xs:complexType>
  <xs:sequence minOccurs="0" maxOccurs="unbounded">
    <!-- No limit to number of gadget URIs for now -->
    <xs:element ref="gadgets" />
    <!-- URI of the gadget xml -->
  </xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="columns">
  <!-- Grouping of a set of columns -->
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="column" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="page">
  <!-- Grouping of a set of persistent gadgets -->
  <xs:complexType>
    <xs:sequence minOccurs="0" maxOccurs="unbounded">
      <!-- No limit to number of gadget URIs for now -->
      <xs:element ref="gadget" />
      <!-- URI of the gadget xml -->
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="tab">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="id" />
      <!-- Id of the tab selector in the desktop -->
      <xs:element ref="icon" minOccurs="0" maxOccurs="1" />
      <xs:element ref="label" />
      <!-- Label of the tab selector -->
      <xs:choice>
        <xs:element ref="gadgets" minOccurs="0" maxOccurs="1" />
        <xs:element ref="columns" minOccurs="0" maxOccurs="1" />
      </xs:choice>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="tabs">
  <!-- Grouping of tabs -->
  <xs:complexType>
    <xs:sequence maxOccurs="unbounded">
      <!-- No limit to number of tabs for now -->
      <xs:element ref="tab" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="layout">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="role" />
      <!-- Type of the role -->
      <xs:element ref="page" />
      <!-- List of page gadgets -->
      <xs:element ref="tabs" />
      <!-- Grouping of tabs for this particular role -->
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="finesseLayout">
  <!-- Layout of the desktop -->

```

```

<xs:complexType>
  <xs:sequence>
    <xs:element ref="version" />
    <xs:element name="configs" type="configs" minOccurs="0" maxOccurs="1" />
    <xs:element name="header" type="header" minOccurs="1" maxOccurs="1" />
    <xs:sequence maxOccurs="3">
      <!-- only support 3 roles for now -->
      <xs:element ref="layout" />
    </xs:sequence>
  </xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>

```

## Add Webchat and Email to Finesse

The Cisco Finesse default layout XML contains commented XML code for Web Chat and Email gadgets available for the Finesse desktop. Each gadget or tab is surrounded by comment characters (<!-- and -->) and comments that describe what the tab or gadget is for and how to add it to the desktop.



**Note** The Chat and Email Control gadget is only supported at the page level. You must ensure that the Chat and Email Control gadget (<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>) is placed within the <page></page> tag. Placing this gadget within a <tab></tab> tag is not supported.

The procedure that you follow depends on your deployment. The following table describes when to use each procedure.

Procedure	When to use
Add Web Chat and Email to the default desktop layout.	Follow this procedure if you want to add Web Chat and Email to the Finesse desktop after a fresh installation or after an upgrade if you have not customized the default desktop layout.
Add Web Chat and Email to a custom desktop layout.	Follow this procedure if you want to add Web Chat and Email and have customized the desktop layout.
Add Web Chat and Email to a team layout.	Follow this procedure if you want to add Web Chat and Email to the desktop only for specific teams.



**Note** After you add the Web Chat and Email gadgets, sign in to the Finesse desktop and make sure they appear the way you want. Agents who are signed in to Finesse when you change the desktop layout must sign out and sign back in to see the change on their desktops.

## Add Web Chat and Email to the Default Desktop Layout



**Note** If you upgraded from a previous release but do not have a custom desktop layout, click **Restore Default Layout** on the Manage Desktop Layout gadget and then follow the steps in this procedure.

### Procedure

- Step 1** In the Finesse administration console, click the **Desktop Layout** tab.
- Step 2** Select from the following editors:
- **Text Editor**
  - **XML Editor**
- Step 3** To add the Chat and Email Control gadget to the agent desktop, look for the following under the `<role>Agent</role>` tag and within the `<page></page>` tag:
- ```
<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
```
- Step 4** Remove the comments and comment characters (`<!--` and `-->`) that surround the gadget, leaving only the gadget (`<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>`).
- Step 5** To add the Manage Chat and Email tab and gadget to the agent desktop, look for the following within the `<tabs></tabs>` tag:
- ```
<tab>
  <id>manageNonVoiceMedia</id>
  <label>finesse.container.tabs.agent.manageNonVoiceMediaLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://my-CCP-server/multisession/ui/gadgets/
          multisession-reply-gadget.xml?gadgetHeight=590</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```
- Step 6** Remove the comments and comment characters (`<!--` and `-->`) that surround the tab.
- Step 7** Replace `my-CCP-server` in the gadget URL with the fully-qualified domain name (FQDN) of your Customer Collaboration Platform server.
- Step 8** Optionally, change the height of the Manage Chat and Email gadget.

#### Example:

The height specified in the gadget URL is 590 pixels. If you want to change the height, change the `gadgetHeight` parameter in the URL to the desired value. For example if you want the gadget height to be 600 pixels, change the code as follows:

```
<gadget>https://my-CCP-server/multisession/ui/gadgets/
  multisession-reply-gadget.xml?gadgetHeight=600</gadget>
```

The default and minimum height of the Manage Chat and Email gadget is 590 pixels. If you do not specify a value for the `gadgetHeight` parameter or if you specify a value that is less than 590, the gadget defaults to 590 pixels.

**Note** An agent can be configured to handle up to five chat contacts and five email contacts at a time. If the agent has the maximum number of contacts on the desktop, not all contacts are visible. If your agents are configured to handle the maximum number of contacts, you must increase the height of this gadget to a minimum of 570 pixels to ensure there is enough space for all of the contacts to appear.

- Step 9** To add the Chat and Email Control gadget to the supervisor desktop, look for the following under the `<role>Supervisor</role>` tag and within the `<page></page>` tag:
- ```
<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
```
- Step 10** Remove the comments and comment characters (`<!--` and `-->`), leaving only the gadget (`<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>`).
- Step 11** To add the Live Data report for Agent Chat Statistics to the supervisor desktop, look for the following:
- ```
<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=F2F1FC17100001440000014E0A4E5D48&filterId=ChatAgentStats.agentId=CL</gadget>
```
- Step 12** Remove the comments and comment characters (`<!--` and `-->`), leaving only the gadget.
- Step 13** To add the Live Data report for Chat Queue Statistics to the supervisor desktop, look for the following:
- ```
<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=E42ED788100001440000007B0A4E5CA1&filterId=ChatQueueStatistics.queueName=CL</gadget>
```
- Step 14** Remove the comments and comment characters (`<!--` and `-->`), leaving only the gadget.
- Step 15** To add the Manage Chat and Email tab and gadget to the supervisor desktop, look for the following within the `<tabs></tabs>` tag:
- ```
<tab>
  <id>manageNonVoiceMedia</id>
  <label>finesse.container.tabs.supervisor.manageNonVoiceMediaLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://my-CCP-server/multisession/ui/gadgets/multisession-reply-gadget.xml?gadgetHeight=590</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```
- Step 16** Remove the comments and comment characters (`<!--` and `-->`) that surround the tab.
- Step 17** Replace `my-CCP-server` in the gadget URL with the fully-qualified domain name (FQDN) of your Customer Collaboration Platform server.
- Step 18** Optionally, change the height of the Manage Chat and Email gadget.
- Step 19** Click **Save**.

## Add Webchat and Email to a Custom Desktop Layout

### Procedure

**Step 1** In the Finesse administration console, click the **Desktop Layout** tab.

**Step 2** Select from the following editors:

- **Text Editor**
- **XML Editor**

**Step 3** Copy the XML code for the Chat and Email Control gadget for the agent desktop.

```
<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
```

**Step 4** To add the gadget to the agent desktop, paste the code within the `<page></page>` tags under the Call Control gadget as follows:

```
<role>Agent</role>
<page>
  <gadget>/desktop/gadgets/CallControl.xml</gadget>
  <gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
</page>
```

**Step 5** To add the gadget to the supervisor desktop, paste the code within the `<page></page>` tags under the Call Control gadget as follows:

```
<role>Supervisor</role>
<page>
  <gadget>/desktop/gadgets/CallControl.xml</gadget>
  <gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
</page>
```

**Step 6** Copy the code for the agent Manage Chat and Email tab and gadget from the default layout XML.

```
<tab>
  <id>manageNonVoiceMedia</id>
  <label>finesse.container.tabs.agent.manageNonVoiceMediaLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://my-CCP-server/multisession/ui/gadgets/
          multisession-reply-gadget.xml?gadgetHeight=430</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```

**Step 7** Paste the code within the `<tabs></tabs>` tag for the agent role after the Manage Call tab:

```
<tab>
  <id>manageCall</id>
  <label>finesse.container.tabs.agent.manageCallLabel</label>
</tab>
<tab>
  <id>manageNonVoiceMedia</id>
  <label>finesse.container.tabs.agent.manageNonVoiceMediaLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://my-CCP-server/multisession/ui/gadgets/
          multisession-reply-gadget.xml?gadgetHeight=430</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```



```

        </gadgets>
      </column>
    </columns>
  </tab>

```

**Step 8** Replace my-social-miner-server with the FQDN of your Customer Collaboration Platform server.

**Step 9** Optionally, change the height of the Manage Chat and Email gadget.

**Example:**

The height specified in the gadget URL is 430 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example if you want the gadget height to be 600 pixels, change the code as follows:

```

<gadget>https://my-CCP-server/multisession/ui/gadgets/
  multisession-reply-gadget.xml?gadgetHeight=600</gadget>

```

The default and minimum height of the Manage Chat and Email gadget is 430 pixels. If you do not specify a value for the gadgetHeight parameter or if you specify a value that is less than 430, the gadget defaults to 430 pixels.

**Note** An agent can be configured to handle up to five chat contacts and five email contacts at a time. If the agent has the maximum number of contacts on the desktop, not all contacts are visible. If your agents are configured to handle the maximum number of contacts, you must increase the height of this gadget to a minimum of 570 pixels to ensure there is enough space for all of the contacts to appear.

**Step 10** Copy the code for the Live Data gadgets for Agent Chat Statistics and Chat Queue Statistics from the default layout XML.

```

<gadget>https://localhost:8444/cuic/gadget/LiveData/
  LiveDataGadget.xml?gadgetHeight=310&
  viewId=F2F1FC17100001440000014E0A4E5D48&
  filterId=ChatAgentStats.agentId=CL</gadget>

<gadget>https://localhost:8444/cuic/gadget/LiveData/
  LiveDataGadget.xml?gadgetHeight=310&
  viewId=E42ED788100001440000007B0A4E5CA1&
  filterId=ChatQueueStatistics.queueName=CL</gadget>

```

**Step 11** Paste the code for these gadgets within the <gadgets></gadgets> tags for the tabs on which you want them to appear.

**Step 12** Copy the code for the supervisor Manage Chat and Email tab and gadget from the default layout XML.

```

<tab>
  <id>manageNonVoiceMedia</id>
  <label>finesse.container.tabs.supervisor.manageNonVoiceMediaLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://my-CCP-server/multisession/ui/gadgets/
          multisession-reply-gadget.xml?gadgetHeight=430</gadget>
      </gadgets>
    </column>
  </columns>
</tab>

```

**Step 13** Paste the code within the <tabs></tabs> tag for the supervisor role after the Manage Call tab:

```

<tab>
  <id>manageCall</id>
  <label>finesse.container.tabs.supervisor.manageCallLabel</label>

```

```

</tab>
<tab>
  <id>manageNonVoiceMedia</id>
  <label>finesse.container.tabs.supervisor.manageNonVoiceMediaLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://my-CCP-server/multisession/ui/gadgets/
          multisession-reply-gadget.xml?gadgetHeight=430</gadget>
      </gadgets>
    </column>
  </columns>
</tab>

```

**Step 14** Replace my-social-miner-server with the FQDN of your Customer Collaboration Platform server.

**Step 15** Optionally, change the height of the gadget.

**Step 16** Click **Save**.

## Add Web Chat and Email to a Team Layout

### Procedure

**Step 1** In the Finesse administration console, click the **Desktop Layout** tab.

**Step 2** Select from the following editors:

- **Text Editor**
- **XML Editor**

**Step 3** Copy the XML code for the Chat and Email Control gadget for the agent desktop and paste it into a text file.

```
<gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
```

**Step 4** Copy the code for the agent Manage Chat and Email tab and gadget and paste it into your text file.

```

<tab>
  <id>manageNonVoiceMedia</id>
  <label>finesse.container.tabs.agent.manageNonVoiceMediaLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://my-CCP-server/multisession/ui/gadgets/
          multisession-reply-gadget.xml?gadgetHeight=430</gadget>
      </gadgets>
    </column>
  </columns>
</tab>

```

**Step 5** Copy the code for the Live Data gadgets for Agent Chat Statistics and Chat Queue Statistics and paste it into your text file.

```

<gadget>https://localhost:8444/cuic/gadget/LiveData/
  LiveDataGadget.xml?gadgetHeight=310&
  viewId=F2F1FC17100001440000014E0A4E5D48&
  filterId=ChatAgentStats.agentId=CL</gadget>

<gadget>https://localhost:8444/cuic/gadget/LiveData/
  LiveDataGadget.xml?gadgetHeight=310&

```

```
viewId=E42ED788100001440000007B0A4E5CA1&
filterId=ChatQueueStatistics.queueName=CL</gadget>
```

**Step 6** Copy the code for the supervisor Manage Chat and Email tab and gadget and paste it into your text file.

```
<tab>
  <id>manageNonVoiceMedia</id>
  <label>finesse.container.tabs.supervisor.manageNonVoiceMediaLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://my-CCP-server/multisession/ui/gadgets/
          multisession-reply-gadget.xml?gadgetHeight=430</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```

**Step 7** Click the **Team Resources** tab.

**Step 8** Select the team from the list of teams for which you want to add Web Chat and Email.

**Step 9** Check the **Override System Default** check box.

**Step 10** In the Resources for <team name> area, click the **Desktop Layout** tab.

**Step 11** Select from the following editors:

- **Text Editor**
- **XML Editor**

**Step 12** To add the Chat and Email Control gadget to the agent desktop, copy the code for the gadget from your text file and paste it within the <page></page> tags under the Call Control gadget as follows:

```
<role>Agent</role>
<page>
  <gadget>/desktop/gadgets/CallControl.xml</gadget>
  <gadget>https://localhost/uccx-nvcontrol/gadgets/NonVoiceControl.xml</gadget>
</page>
```

**Step 13** To add the gadget to the supervisor desktop, paste the code within the <page></page> tags under the Call Control gadget as follows:

**Step 14** To add the Manage Chat and Email tab and gadget to the agent desktop, copy the code from your text file and paste it within the <tabs></tabs> tag for the agent role after the Manage Call tab:

```
<tab>
  <id>manageCall</id>
  <label>finesse.container.tabs.agent.manageCallLabel</label>
</tab>
<tab>
  <id>manageNonVoiceMedia</id>
  <label>finesse.container.tabs.agent.manageNonVoiceMediaLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://my-CCP-server/multisession/ui/gadgets/
          multisession-reply-gadget.xml?gadgetHeight=430</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```

**Step 15** Replace my-social-miner-server with the FQDN of your Customer Collaboration Platform server.

**Step 16** Optionally, change the height of the Manage Chat and Email gadget.

**Example:**

The height specified in the gadget URL is 430 pixels. If you want to change the height, change the `gadgetHeight` parameter in the URL to the desired value. For example if you want the gadget height to be 600 pixels, change the code as follows:

```
<gadget>https://my-CCP-server/multisession/ui/gadgets/
    multisession-reply-gadget.xml?gadgetHeight=600</gadget>
```

The default and minimum height of the Manage Chat and Email gadget is 430 pixels. If you do not specify a value for the `gadgetHeight` parameter or if you specify a value that is less than 430, the gadget defaults to 430 pixels.

**Note** An agent can be configured to handle up to five chat contacts and five email contacts at a time. If the agent has the maximum number of contacts on the desktop, not all contacts are visible. If your agents are configured to handle the maximum number of contacts, you must increase the height of this gadget to a minimum of 570 pixels to ensure there is enough space for all of the contacts to appear.

- Step 17** To add the Live Data gadgets for Web Chat and Email to the supervisor desktop:
- Copy the code for the Agent Chat Statistics Live Data gadget from your text file and paste it within the `<gadgets></gadgets>` tags for the tab on which you want it to appear.
  - Copy the code for the Chat Queue Statistics Live Data gadget from your text file and paste it within the `<gadgets></gadgets>` tags for the tab on which you want it to appear.

- Step 18** To add the Manage Chat and Email tab gadget to the supervisor desktop, copy the code from your text file and paste it within the `<tabs></tabs>` tag for the supervisor role after the Manage Call tab:

```
<tab>
  <id>manageCall</id>
  <label>finesse.container.tabs.supervisor.manageCallLabel</label>
</tab>
<tab>
  <id>manageNonVoiceMedia</id>
  <label>finesse.container.tabs.supervisor.manageNonVoiceMediaLabel</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://my-CCP-server/multisession/ui/gadgets/
          multisession-reply-gadget.xml?gadgetHeight=430</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```

- Step 19** Replace `my-social-miner-server` with the FQDN of your Customer Collaboration Platform server.

- Step 20** Optionally, change the height of the gadget.

- Step 21** Click **Save**.

---

## Enable Advanced Supervisor Capabilities in Finesse

The Cisco Finesse default layout XML contains commented XML code of Advanced Supervisor Capabilities gadget for the Finesse desktop. Each gadget or tab is surrounded by comment characters (`<!--` and `-->`) and comments that describe what the tab or gadget is for and how to add it to the desktop.



**Note** The Advanced Supervisor Capability is designed for only supervisors.

The procedure that you must follow to enable the gadget depends on your deployment. The following table describes when to use each procedure.

Procedure	When to use
Enable Advanced Supervisor Capabilities for Default Desktop Layout	Follow this procedure if you want to enable Advanced Supervisor Capabilities in the Finesse desktop after a fresh installation or after an upgrade if you have not customized the default desktop layout.
Add Advanced Supervisor Capabilities in Custom Desktop Layout	Follow this procedure if you want to add Advanced Supervisor Capabilities and have customized the desktop layout.
Add Advanced Supervisor Capabilities to a team layout.	Follow this procedure if you want to add Advanced Supervisor Capabilities to the desktop for specific teams.



**Note** After you enable the Advanced Supervisor Capabilities gadget, sign in to the Finesse desktop as a supervisor and ensure that they appear the way you want. When you change the desktop layout, supervisors who are signed in to Finesse must sign out and sign in again to see the change on their desktops.

### Enable Advanced Supervisor Capabilities in Default Desktop Layout

If you upgraded from a previous release but do not have a custom desktop layout, click **Restore Default Layout** on the **Manage Desktop Layout** gadget and then follow the steps in this procedure.



**Note** Perform this task only once at the beginning of Default Desktop Layout modification. If you do it later, the previous changes will be lost.

#### Procedure

- Step 1** In the Finesse administration console, click the **Desktop Layout** in the left pane. **Manage Desktop Layout** page is displayed with **Desktop Layout XML**.
- Step 2** Select from the following editors:
  - **Text Editor**
  - **XML Editor**
- Step 3** To enable Advanced Supervisor Capabilities gadget in the supervisor desktop, look for the following under the `<role>Supervisor</role>` tag:

```
<id>ASCGadget</id>
```

- Step 4** Remove the comments and comment characters (<!-- and -->) that surround the gadget, leaving only the gadget <gadget>https://localhost/ascgadget/gadgets/ascgadget.xml</gadget>.
- Step 5** Click **Save**.

## Add Advanced Supervisor Capabilities in Custom Desktop Layout

### Procedure

- Step 1** In the Finesse administration console, click the **Desktop Layout** in the left pane. **Manage Desktop Layout** page is displayed with **Desktop Layout XML**.
- Step 2** Select from the following editors:
- **Text Editor**
  - **XML Editor**
- Step 3** Copy the XML code of Advanced Supervisor Capabilities gadget.
- ```
<gadget>https://localhost/ascgadget/gadgets/ascgadget.xml</gadget>
```
- Step 4** In the **Desktop Layout XML**, look for the <role>Supervisor</role> tag.
- Step 5** Paste the copied code within the <tab> </tab> tags in the Desktop Layout XML, below the WebChat and Email gadget as follows:

```
<tab>
  <id>ASCGadget</id>
  <icon>admin</icon>
  <label>finesse.container.tabs.supervisor.advancedcapabilities</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://localhost/ascgadget/gadgets/ascgadget.xml</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```

**Note** Ensure that the gadget is available only for supervisors.

- Step 6** Click **Save**.

## Add Advanced Supervisor Capabilities in Team Layout

### Procedure

- Step 1** In the Finesse administration console, click the **Desktop Layout** in the left pane. **Manage Desktop Layout** page is displayed with **Desktop Layout XML**.
- Step 2** Select from the following editors:

- **Text Editor**
- **XML Editor**

**Step 3** Copy the XML code of Advanced Supervisor Capabilities gadget.

```
<gadget>https://localhost/ascgadget/gadgets/ascgadget.xml</gadget>
```

**Step 4** Click the **Team Resources** in the left pane.

**Step 5** Select the team from the list of teams for which you want to add Advanced Supervisor Capabilities.

**Step 6** Check the **Override System Default** check box.

**Step 7** In the Resources for <team name> area, click the **Desktop Layout** tab.

**Step 8** Select from the following editors:

- **Text Editor**
- **XML Editor**

**Step 9** In the XML, look for the <role>Supervisor</role> tag.

**Step 10** Paste the copied code within the <tab> </tab> tags in the XML, below the WeChat and Email gadget as follows:

```
<tab>
  <id>ASCGadget</id>
  <icon>admin</icon>
  <label>finesse.container.tabs.supervisor.advancedcapabilities</label>
  <columns>
    <column>
      <gadgets>
        <gadget>https://localhost/ascgadget/gadgets/ascgadget.xml</gadget>
      </gadgets>
    </column>
  </columns>
</tab>
```

**Note** Ensure that the gadget is available only for supervisors.

**Step 11** Click **Save**.

## Add Team Message in Custom Desktop Layout

### Procedure

**Step 1** In the Finesse administration console, click the **Desktop Layout** in the left pane. **Manage Desktop Layout** page is displayed with **Desktop Layout XML**.

**Step 2** Select from the following editors:

- **Text Editor**
- **XML Editor**

**Step 3** Copy the XML code where `component id="broadcastmessagepopover"`.

```
<component id="broadcastmessagepopover">
  <url>/desktop/scripts/js/teammessage.component.js</url>
</component>
```

- Step 4** Click the **Team Resources** in the left pane.
- Step 5** Check the **Override System Default** check box.
- Step 6** In the Resources for <team name> area, click the **Desktop Layout** tab.
- Step 7** Select from the following editors:

- **Text Editor**
- **XML Editor**

- Step 8** In the XML, look for the </headercolumn> tag in the XML.
- Step 9** Paste the copied code below the </headercolumn> tag as follows:

```
<headercolumn width="50px">
  <component id="broadcastmessagepopover">
    <url>/desktop/scripts/js/teammessage.component.js</url>
  </component>
</headercolumn>
```

- Step 10** Click **Save**.

## Add Desktop Chat in Custom Desktop Layout

### Procedure

- Step 1** In the Finesse administration console, click the **Desktop Layout** in the left pane. **Manage Desktop Layout** page is displayed with **Desktop Layout XML**.
- Step 2** Select from the following editors:
- **Text Editor**
  - **XML Editor**
- Step 3** Copy the XML code where `component id="chat"`.
- ```
<component id="chat">
  <url>/desktop/scripts/js/chat.component.js</url>
</component>
```
- Step 4** Click the **Team Resources** in the left pane.
- Step 5** Check the **Override System Default** check box.
- Step 6** In the Resources for <team name> area, click the **Desktop Layout** tab.
- Step 7** Select from the following editors:
- **Text Editor**
  - **XML Editor**
- Step 8** In the XML, look for the </headercolumn> tag in the XML.
- Step 9** Paste the copied code below the </headercolumn> tag as follows:



```
<headercolumn width="50px">
  <component id="chat">
    <url>/desktop/scripts/js/chat.component.js</url>
  </component>
</headercolumn>
```

**Step 10** Click **Save**.

## Live Data Gadgets

Cisco Finesse for Unified CCX supports Live Data gadgets. Live Data gadgets display information about the current state of the contact center. The gadgets receive data from the real-time data source at frequent intervals and display reports in grid format only.

Cisco Unified Intelligence Center provides Live Data real-time reports that you can add to the Cisco Finesse agent and supervisor desktop.

This feature provides the following access:

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

### Gadgets URLs for Reports

The following table displays gadgets URLs for reports.

Users	Reports	Report View	Is the Report Available in Default Layout ?	Tab	Gadget URLs
Agent	Agent CSQ Statistics Report	Agent CSQ Statistics Report	Yes	Home	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=76D964AD10000140000000830A4E5E6F&filterId=AgentCSQStats.csqName=CL&compositeFilterId=AgentCSQStats.AgentIds.agentId=loginId</gadget>
Agent	Agent State Log Report	Agent State Log Report	Yes	My Statistics	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=420&viewId=5D411E8A10000140000000230A4E5E6B&filterId=AgentStateDetailStats.agentID=loginId</gadget>
Agent	Agent Statistics Report	Agent Statistics Report	Yes	My Statistics	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=150&viewId=67D4371110000140000001080A4E5E6B&filterId=ResourceIAQStats.resourceId=loginId</gadget>

Users	Reports	Report View	Is the Report Available in Default Layout ?	Tab	Gadget URLs
Agent	Agent Team Summary Report	Agent Team Summary Report	Yes	Home	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=5C626F9C10000140000000600A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>
Supervisor	Agent Outbound Team Summary Report	Report since midnight	No	Team Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=FD919FB9100001440000005D0A4E5B29&filterId=ResourceIAQStats.resourceId=CL</gadget>
Supervisor	Agent Outbound Team Summary Report	Short and long term average	No	Team Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=FD919FB510000144000000470A4E5B29&filterId=ResourceIAQStats.resourceId=CL</gadget>
Supervisor	Chat Agent Statistics Report	Chat Agent Statistics Report	No	Team Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=120&viewId=F2F1FC17100001440000014E0A4E5D48&filterId=ChatAgentStats.agentId=CL</gadget>
Supervisor	Chat CSQ Summary Report	Chat CSQ Summary Report	No	Queue Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=120&viewId=E42ED788100001440000007B0A4E5CA1&filterId=ChatQueueStatistics.queueName=CL</gadget>
Supervisor	Email Agent Statistics Report	Email Agent Statistics Report	No	Team Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=BCC5767B1000014F0000000580A4D3FA7&filterId=EmailAgentStats.agentId=CL</gadget>
Supervisor	Email CSQ Summary Report	Email CSQ Summary Report	No	Queue Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=13970B4E100001500000021C0A4D3FA7&filterId=EmailQueueStatistics.queueName=CL</gadget>
Supervisor	Team State Report	Team State Report	No	—	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=5C90012F10000140000000830A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>

Users	Reports	Report View	Is the Report Available in Default Layout ?	Tab	Gadget URLs
Supervisor	Team Summary Report	Report since midnight	Yes	Team Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=728283C210000140000000530A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>
Supervisor	Team Summary Report	Short and long term average	Yes	Team Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=7291DCB410000140000000890A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>
Supervisor	Voice CSQ Agent Detail Report	Voice CSQ Agent Detail Report	Yes	Queue Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=9A7A14CE10000140000000ED0A4E5E6B&filterId=VoiceCSQDetailsStats.agentId=CL&compositeFilterId=VoiceCSQDetailsStats.AgentVoiceCSQNames.agentVoiceCSQName=CL</gadget>
Supervisor	Voice CSQ Summary	Snapshot	Yes	Queue Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=C8E2DB1610000140000000A60A4E5E6B&filterId=VoiceIAQStats.esdName=CL</gadget>
Supervisor	Voice CSQ Summary	Short and long term average	Yes	Queue Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=C8EE241910000140000000C30A4E5E6B&filterId=VoiceIAQStats.esdName=CL</gadget>
Supervisor	Voice CSQ Summary	Report since midnight	No	Queue Data	<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=C8EF510810000140000000EB0A4E5E6B&filterId=VoiceIAQStats.esdName=CL</gadget>

### Gadgets Customization

You can use optional query parameter to adjust height of the gadgets.

### Query Parameter

```
<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=200&viewId=5C626F9C10000140000000600A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>
```

## Add Live Data Gadgets to Desktop Layout

The Cisco Finesse default layout XML contains commented XML code for the Live Data gadgets available for Cisco Finesse desktop. Perform the following steps to add Live Data gadgets to desktop layout:

### Procedure

- 
- Step 1** Sign in to Cisco Finesse administration console.  
Cisco Finesse home page appears.
- Step 2** Click the **Desktop Layout** tab.
- Step 3** Select from the following editors:
- **Text Editor**
  - **XML Editor**
- Step 4** Copy the gadget URL for the report you want to add from **Live Data Gadgets**.

#### Example:

To add the Agent Report, copy the following:

```
<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=150&viewId=67D4371110000140000001080A4E5E6B&filterId=ResourceIAQStats.resourceId=loginId</gadget>
```

- Step 5** Paste the gadget URL within the tab tags where you want it to appear.

#### Example:

To add the report to the home tab of the agent desktop:

```
<finesseLayout xmlns="http://www.cisco.com/vtg/finesse">
  <layout>
    <role>Agent</role>
    <page>
      <gadget>/desktop/gadgets/CallControl.xml</gadget>
    </page>
    <tabs>
      <tab>
        <id>home</id>
        <label>finesse.container.tabs.agent.homeLabel</label>
        <gadgets>
          <gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=76D964AD10000140000000830A4E5E6F&filterId=AgentCSQStats.csqName=CL&compositeFilterId=AgentCSQStats.AgentIds.agentId=loginId</gadget>
          <gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId=5C626F9C10000140000000600A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>
        </gadgets>
        <gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=150&viewId=67D4371110000140000001080A4E5E6B&filterId=ResourceIAQStats.resourceId=loginId</gadget>
      </tab>
      <tab>
        <id>myStatistics</id>
        <label>finesse.container.tabs.agent.myStatisticsLabel</label>
        <gadgets>
          <gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=600&viewId=5D411E8A10000140000000230A4E5E6B&filterId=AgentStateDetailStats.agentID=loginId</gadget>
        </gadgets>
      </tab>
    </tabs>
  </layout>
</finesseLayout>
```

```

    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
  </tabs>
</layout>
<layout>
  <role>Supervisor</role>
<page>
  <gadget>/desktop/gadgets/CallControl.xml</gadget>
</page>

```

- Step 6** Click **Save**. Cisco Finesse validates the XML file to ensure that it is valid XML syntax and conforms to the Cisco Finesse schema.
- Step 7** To verify, log in to Cisco Finesse agent desktop as agent/Cisco Finesse supervisor desktop as supervisor and check the reports.

---

### Related Topics

[Live Data Gadgets](#), on page 61

## Add Customized Live Data Gadgets to Desktop Layout

This procedure explains how to create gadget URLs for customized Live Data reports, which are copied from stock reports, and add them to desktop layout.




---

**Note** The new gadget renders the report only when the appropriate permission on that report is given in Cisco Unified Intelligence Center.

---

### Procedure

---

- Step 1** Copy the gadget URL of the stock report that you want to customize from **Live Data Gadgets** and paste it in a text editor.

**Example:**

Consider the URL shown here as the gadget URL. Copy and paste it in a text editor. The underlined ID is the value of viewID.

```

<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310
&viewId=5C626F9C10000140000000600A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>

```

- Step 2** In Cisco Unified Intelligence Center, in the Edit view of the customized report, select the view for which you want to create the gadget URL and then click **Links**.

The HTML Link field displays the permalink of the customized report.

- Step 3** Copy the permalink of the customized report from the **HTML Link** field and paste it in a text editor, then copy the viewID value from this link.

**Example:**

Copy the underlined viewID value from the permalink of the customized report.

```

https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid

```

**Step 4** Replace the viewID value in the gadget URL with the viewID value from the permalink of the customized report.

**Example:**

The customized gadget URL appears as shown here after replacing the viewID value with the viewID value of the customized report.

```
<gadget>https://localhost:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310
&viewId=5C90012F10000140000000830A4E5B33&filterId=ResourceIAQStats.resourceId=CL</gadget>
```

**Step 5** Add the customized gadget URL to Desktop Layout in the Finesse administration console and save.

**Step 6** Log in to Finesse desktop and check the report.

---

**Related Topics**

[Live Data Gadgets](#), on page 61

## Configure Live Data Reports with Multiple Views

Cisco Finesse allows you to display multiple Live Data reports or views on a single gadget. Supervisors 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.

This procedure describes how to add multiple Live Data views to the Finesse desktop layout using the viewId\_n and filterId\_n keys. You can specify up to five report views to appear in your gadget. The first view among the five is the default view. There is no defined order for how the remaining views are displayed.

Finesse still supports the display of a single gadget using a single viewId. However, if you specify the single viewId along with multiple viewId\_n keys, the multiple views are used and the single viewId is ignored.




---

**Note** To make sure the modified gadget renders in the Finesse desktop, you must give the appropriate permission for that report in Unified Intelligence Center.

---

**Procedure**

---

**Step 1** For each report or view that you want to include in the gadget, obtain the associated viewId from the permalink for the view:

- a) In Unified Intelligence Center, in Edit view of the report, select the desired view then click **Links**.

The HTML Link field displays the permalink of the customized report.

- b) Copy the permalink of the customized report from the **HTML Link** field, and paste it in a text editor, and then copy the viewID value from the permalink and save it.

**Example:**

Copy the viewId, which is underlined in this example, from the permalink for the report.

```
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid
```

- Step 2** From the Finesse default layout XML, copy the gadget URL for one of the Live Data reports and paste it into a text editor.

**Example:**

Copy the URL for the Agent Skill Group for HTTPS from the default layout XML and paste it into a text editor:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId_1=9AB7848B10000141000001C50A0006C4&filterId_1=agent.id=CL%20teamName</gadget>
```

- Step 3** To update the URL to refer to a different report view, populate the viewId\_1 value (after the equal sign) with the desired viewId obtained in step 1.

**Example:**

The following shows the URL updated with the example viewId copied from step 1.

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName</gadget>
```

- Step 4** For each additional view you want to include:

- a) At the end of the URL, copy and paste the viewId\_1 and agentId\_1 strings with a leading ampersand.

**Example:**

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName</gadget>
```

- b) Update the copied viewId\_1 and filterId\_1 in the URL to the next available integer (in this example, viewId\_2 and filterId\_2).

**Example:**

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&viewId_2=5C90012F10000140000000830A4E5B33&filterId_2=agent.id=CL%20teamName</gadget>
```

- c) Populate the copied viewId value (after the equal sign) with the value defined in the permalink for the desired report (in this example, 99E6C8E210000141000000D80A0006C4).

**Example:**

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.xml?gadgetHeight=310&viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&viewId_2=99E6C8E210000141000000D80A0006C4&filterId_2=agent.id=CL%20teamName</gadget>
```

- d) Make sure that the filterId value matches the type required by the report type, as follows:

- Agent Reports: filterId\_N=agent.id=CL%20teamName
- Agent Skill Group Reports: filterId\_N=agent.id=CL%20teamName
- Skill Group Reports: filterId\_N=skillGroup.id=CL%20teamName
- Precision Queue Reports: filterId\_N=precisionQueue.id=CL%20teamName

- Step 5** Replace my-cuic-server with the FQDN of your Cisco Unified Intelligence Center Server.
- Step 6** Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click **Save**.

## Manage Phone Books

On the Phone Books tab of the Cisco Finesse administration console, you can create and manage global and team phone books and phone book contacts. Global phone books are available to all agents; team phone books are available to agents in that specific team.

### Phone Books and Contacts

Finesse supports the following number of phone books:

- 10 global phone books
- 300 team phone books

The system supports a total of 50,000 contacts. The total number of contacts per agent across all phone books is limited to 6000.

Use the Manage Phone Books gadget to view, add, edit, or delete phone books and phone book contacts. Click the Name or Assign To headers to sort the phone books in ascending or descending order. Click the last Name, First Name, Number, or Note headers to sort the contacts in ascending or descending order.

The following table describes the fields on the Manage Phone Books gadget:

Field	Explanation
Name	The name of the phone book. It must be unique, and can be a maximum of 64 alphanumeric characters.
Assign To	Indicates if the phone book is global (All Users) or team (Teams).
Last Name	The last name of a contact. The last name can be a maximum of 128 characters. This field is optional.
First Name	The first name of a contact. The first name can be a maximum of 128 characters. This field is optional.
Number	The phone number for the contact. The phone number can be 1-32 characters long and cannot be blank.
Note	Optional text that describes the contact. The note can be a maximum of 128 characters.

#### Actions on the Manage Phone Books gadget:

- **New:** Add a new phone book or contact
- **Edit:** Edit an existing phone book or contact
- **Delete:** Delete a phone book or contact



- **Refresh:** Reload the list of phone books or contacts from the server
- **Import:** Import a list of contacts to the phone book
- **Export:** Export a list of contacts from the phone book

## Add Phone Book

### Procedure

---

- Step 1** In the Manage Phone Books gadget, click **New**.
- Step 2** In the **Name** field, enter a name for the phone book.
- Note** Phone book names can be a maximum of 64 characters.
- Step 3** From the **Assign To** drop-down, select **All Users** if the phone book is global or **Teams** if the phone book is available to specified teams.
- Step 4** Click **Save**.
- 

## Edit Phone Book

### Procedure

---

- Step 1** In the Manage Phone Books gadget, select the phone book you want to edit.
- Step 2** Click **Edit**.
- Step 3** In the **Name** field, enter the new name for the phone book. If you want to change who can access the phone book, in the **Assign To** drop-down, choose **All Users** or **Teams**.
- Step 4** Click **Save**.
- If you change the Assign To field from Teams to All Users, click **Yes** to confirm the change.
- 

## Delete Phone Book

### Procedure

---

- Step 1** In the Manage Phone Books gadget, select the phone book that you want to delete.
- Step 2** Click **Delete**.
- Step 3** Click **Yes** to confirm the deletion of the selected phone book.
-

## Import Contacts

The Import function allows you to replace all the contacts in a phone book with a new list of contacts, or to populate a new phone book with contacts.

The import list must be in the specified comma separated values (CSV) format, and can contain a maximum of 6000 contacts. Import lists that contain more than 6000 contacts are rejected with an error message.

The CSV file contains the fields described in the following table:

Field	Max Length	Can Be Blank?	Permitted Characters
First Name	128	Yes	<b>Note</b> The CSV file that contains the contacts to import must use Latin encoding.
Last Name	128	Yes	
Phone Number	32	No	
Notes	128	Yes	

The following is an example of a phone book CSV file:

```
"First Name","Last Name","Phone Number","Notes"
"Amanda","Cohen","6511234",""
"Nicholas","Knight","612-555-1228","Sales"
"Natalie","Lambert","952-555-9876","Benefits"
"Joseph","Stonetree","651-555-7612","Manager"
```

A phone book CSV file must conform to this format and include the headers in the first line. During import, the file is scanned for illegal characters. If any are found, they are replaced with question marks.



**Note** Exported CSV files always show each field enclosed in double quotes to ensure that any commas or double quotes that are part of the actual filed data are not mistaken for field delimiters. If your data does not include these characters, you can omit the double quotes in files you prepare for importing.

### Procedure

- 
- Step 1** In the Manage Phone Books gadget, select the phone book into which you want to import a list of contacts.
  - Step 2** Click **Import**.
  - Step 3** Click **Browse** and navigate to the location of the CSV file containing the contacts you want to import.
    - Note** The CSV file must use Latin encoding.
  - Step 4** Click **OK**.
- 

## Export Contacts

The Export function allows you to extract a list of contacts from an existing phone book. The exported list is saved in CSV format.

### Procedure

---

- Step 1** In the Manage Phone Books gadget, select the phone book that contains the contacts you want to export.
- Step 2** Click **Export**.
- Step 3** Click **Open** to open the CSV file in Excel, or click the **Save** drop-down list and choose **Save**, **Save as**, or **Save and open**.
- Step 4** A message appears that gives you the option to view the downloaded file, open the folder into which the download was saved, view the Internet Explorer View Downloads window, or dismiss the message without viewing the file.
- Step 5** A message appears that gives you the option to view the downloaded file, open the folder into which the download was saved, view the Internet Explorer View Downloads window, or dismiss the message without viewing the file.
- 

## Add Contact

### Procedure

---

- Step 1** In the Manage Phone Books gadget, select the phone book to which you want to add a contact.  
The List of Contacts for <phone book name> area appears.
- Step 2** Click **New**.
- Step 3** Complete the fields. The First Name, Last Name, and Note fields are optional and have a maximum length of 128 characters. The Number field is required and has a maximum length of 32 characters.
- Step 4** Click **Save**.
- 

## Edit Contact

### Procedure

---

- Step 1** In the Manage Phone Books gadget, select the phone book that contains the contact you want to edit.  
The List of Contacts for <phone book name> area appears.
- Step 2** Select the contact you want to edit.
- Step 3** Click **Edit**.
- Step 4** Edit the fields that you want to change. The First Name, Last Name, and Note fields are optional and have a maximum of 128 characters. The Number field is required and has a maximum of 32 characters.
- Step 5** Click **Save**.
-

## Delete Contact

### Procedure

- 
- Step 1** In the Manage Phone Books gadget, select the phone book that contains the contact you want to delete. The List of Contacts for <phone book name> area appears.
- Step 2** Select the contact that you want to delete.
- Step 3** Click **Delete**.
- Step 4** Click **Yes** to confirm the deletion of the selected contact.
- 

## Manage Reasons

The Reasons tab on the Cisco Finesse administration console allows you to view, add, edit, and delete Not Ready reason codes, Sign Out reason codes, and Wrap-Up reasons.



- 
- Note** Certain reason codes are reserved and cannot be used. For Unified CCX systems, these reserved reason codes are as follows: 0, 22, and 33.
- 

## Not Ready Reason Codes

Not Ready reason codes represent reasons that agents can select when they change their state to Not Ready. Use the Manage Reason Codes (Not Ready) gadget to view, add, edit, or delete Not Ready reason codes.

1. Click the Reason Label or Reason Code headers to sort the Not Ready reason codes by label or reason code in ascending or descending order.
2. Click the Type header to sort and display system or custom reason codes.
3. Click the Global header to sort reason codes by whether they are global (Yes) or not (No).

Not Ready reason codes can be global (visible to all agents) or team (visible only to agents on specified teams).



- 
- Note** Finesse supports a total of 200 Not Ready reason codes. This includes a maximum of 100 global Not Ready reason codes, and 100 team Not Ready reason codes. The team reason codes can be mapped to any team, and the same reason code can be mapped to multiple teams.
- 

The following table describes the fields on the Manage Reason Codes (Not Ready) gadget:

Field	Explanation
Reason Label	The label for the Not Ready reason code.

	The label has a maximum length of 40 characters and should be unique for each Not Ready reason code. Alphanumeric and special characters are supported.
Type	The type of reason code (System or Custom). The column is default and can be sorted to display both System reason codes and Custom reason codes.
Reason Code	A code for the Not Ready reason. The value of the code must be between 1 and 999 and must be unique.
Global?	Yes/No. Indicates if the reason code is available globally to all agents (Yes) or to specific teams of agents (No).

#### Actions on the Manage Reason Codes (Not Ready) gadget:

- **New:** Add a new Not Ready reason code
- **Edit:** Edit an existing Not Ready reason code
- **Delete:** Delete a Not Ready reason code
- **Refresh:** Reload the list of Not Ready reason codes from the server



**Note** When you add, edit, or delete a Not Ready reason code, the changes you make take effect on the Finesse desktop after three seconds. However, agents who are signed in when the changes are made must sign out and sign back in to see those changes reflected on their desktops.

When an agent signs in to the Finesse desktop, the agent state is set to Not Ready. The agent can then choose to go to Ready status or choose from one of the configured Not Ready reason codes from the agent state drop-down list.

If an agent wants to change from Ready to Not Ready status, that agent can choose the appropriate Not Ready reason code from the list of configured codes.

An agent who is on a call can select a state to be applied when the call is complete. For example, if an agent wants to be in Not Ready state when the call ends, that agent can choose Not Ready from the drop-down list while still on the call. The Finesse desktop shows the agent in Talking state and a pending state of Not Ready.

Pending state changes appear on the desktop while the agent's state is Talking (for example, on hold, in a consult call, conference, or silent monitor call).



**Note** During a PG or CTI server failover, the pending state of an agent is not retained.

## Add Not Ready Reason Code

### Procedure

- Step 1** In the Manage Reason Codes (Not Ready) gadget, click **New**.

- Step 2** In the Reason Label box, enter a label for the reason code.
- Note** Not Ready reason code labels are limited to 40 characters.
- Step 3** In the Reason Code box, an auto populated reason code is displayed. If you choose not to save the prepopulated reason code, you can enter your own reason code.
- Note** The code must be between 1 and 999 and must be unique.  
Ensure there are no leading or trailing spaces.
- Step 4** If the reason code is global, select the Global? check box. If the reason code is specific to a team, clear the Global? check box.
- Note** By default, the Global? check box is selected.
- Step 5** Click **Save**.
- Note** The Finesse server removes leading or trailing spaces before saving the Reason Label in the database.
- 

## Edit Not Ready Reason Code

### Procedure

---

- Step 1** In the Manage Reason Codes (Not Ready) gadget, select the reason code that you want to edit.
- Step 2** Click **Edit**.
- Step 3** If you want to change the label for the Not Ready reason code, in the Reason Label field, enter a new label for the reason code. If you want to change the code, in the Reason Code field, enter the new code. If you want to change who has access to the code, select or clear the Global? check box.
- Step 4** Click **Save**.
- 

## Delete Not Ready Reason Code



- Note** An error may occur if an agent selects a Not Ready reason code after it has been deleted. Agents who are signed in when you make changes to Not Ready reason codes must sign out and sign back in to see those changes reflected on their desktops.
- 

### Procedure

---

- Step 1** In the Manage Reason Codes (Not Ready) gadget, select the Not Ready reason code that you want to delete.
- Step 2** Click **Delete**.

**Step 3** Click **Yes** to confirm the deletion of the selected reason code.

## Sign Out Reason Codes

Sign Out reason codes represent reasons that agents can select when they sign out of the Finesse desktop.

Use the Manage Reason Codes (Sign Out) gadget to view, add, edit, or delete Sign Out reason codes. Click the Reason Label or Reason Code headers to sort the Sign Out reason codes by label or by reason code, in ascending or descending order. Click the Type header to sort and display system or custom reason codes. Click the Global header to sort the reason codes by whether they are global (Yes) or not (No).

Sign Out reason codes can be global (visible to all agents) or team (visible only to agents on specified teams).



**Note** Finesse supports 200 Sign Out reason codes. These include 100 global Sign Out reason codes, and 100 Sign Out team reason codes. The team reason codes can be mapped to any team, and the same reason code can be mapped to multiple teams.

The following table describes the fields on the Manage Reason Codes (Sign Out) gadget:

Field	Explanation
Reason Label	The label for the Sign Out reason code. The label has a maximum length of 40 characters and should be unique for each Sign Out reason code. Alphanumeric and special characters are supported.
Type	The type of reason code (System or Custom). The column is default and can be sorted to display both System reason codes and Custom reason codes.
Reason Code	A code for the Sign Out reason. The code must be between 1 and 999 and must be unique.
Global?	Yes/No. Indicates if the reason code is available globally to all agents (Yes) or to specific teams of agents (No).

### Actions on the Manage Reason Codes (Sign Out) gadget:

- **New:** Add a new Sign Out reason code
- **Edit:** Edit an existing Sign Out reason code
- **Delete:** Delete a Sign Out reason code
- **Refresh:** Reload the list of Sign Out reason codes from the server



---

**Note** When you add, edit, or delete a Sign Out reason code, the changes you make take effect on the Finesse desktop after three seconds. However, agents who are signed in when the changes are made must sign out and sign in again to see those changes reflected on their desktops.

---

When an agent clicks Sign Out on the desktop, any configured Sign Out codes appear in a drop-down list. The agent can select the code that represents why that agent is signing out.

## Add Sign Out Reason Code

### Procedure

---

- Step 1** In the Manage Reason Codes (Sign Out) gadget, click **New**.
- Step 2** In the Reason Label box, enter a label for the reason code.
- Note** Sign Out reason code labels are limited to 40 characters.
- Step 3** In the Reason Code box, an auto populated reason code is displayed. If you choose not to save the prepopulated reason, you can enter your own reason code.
- Note** The code must be between 1 and 999 and must be unique.  
Ensure there are no leading or trailing spaces.
- Step 4** If the reason code is global, select the Global? check box. If the reason code is specific to a team, clear the Global? check box.
- Note** By default, the Global? check box is selected.
- Step 5** Click **Save**.
- 

## Edit Sign Out Reason Code

### Procedure

---

- Step 1** In the Manage Reason Codes (Sign Out) gadget, select the reason code that you want to edit.
- Step 2** Click **Edit**.
- Step 3** If you want to change the label of the Sign Out reason code, in the Reason Label field, enter a new label for the reason code. If you want to change the code, in the Reason Code field, enter the new code. If you want to change who has access to the code, select or clear the Global? check box.
- Step 4** Click **Save**.
-



## Delete Sign Out Reason Code



**Note** An error may occur if an agent selects a Sign Out reason code after it has been deleted. Agents who are signed in when you make changes to Sign Out reason codes must sign out and sign back in to see those changes reflected on their desktops.

### Procedure

- Step 1** In the Manage Reason Codes (Sign Out) gadget, select the Sign Out reason code that you want to delete.
- Step 2** Click **Delete**.
- Step 3** Click **Yes** to confirm the deletion of the selected Sign Out reason code.

## Predefined System Reason Codes

For Not Ready system reason codes and Sign Out system reason codes, only the reason code label can be edited and saved. The Global attribute and system code cannot be modified. In case the system reason code label is modified and you wish to revert to the default label, refer to the following list of predefined system reason codes:

System Reason Code	Reason Label	Reason Label Description
32767	Logged Out - Device Conflict	The system issues this reason code when an agent is already logged in to one device (computer or phone) and then tries to re-login to a second device.
32765	Logged Out - System Disconnect	The system issues this reason code when a Cisco Finesse IP Phone Agent or Cisco Finesse desktop crashes due to any reason or if the connection is disrupted.
32764	Logged Out - System Standby	The system issues this reason code when the active server becomes the standby server and the agent loses connection to the Unified CCX Platform.
32763	Not Ready - Call Not Answered	The system issues this reason code when the agent fails to answer a Unified CCX call within the specified timeout period.
32762	Not Ready - Offhook	The system issues this reason code when the agent goes off the hook to place a call. If the agent remembers to do this task the corresponding agent-triggered reason code is displayed. If the agent does not remember to do this task, the system issues this reason code.
32761	Not Ready - Non ACD Busy	The system issues this reason code when the agent is logged on to the Cisco Finesse desktop or Cisco Finesse IP phone and then receives a call that is not queued on the Unified CCX Platform.

32760	Not Ready - Log On	The system issues this reason code when an agent logs in and is automatically placed in the Not Ready state.
32759	Not Ready - Phone Failure	The system issues this reason code if the agent's phone crashes and that agent is placed in the unavailable state.
32758	Not Ready - Wrap Up Timer Expiry	The system issues this reason code when an agent's state is changed from WORK to Not Ready. This change occurs if the WORK state for that agent's CSQ is associated with an expired wrap-up timer.
32757	Not Ready - CUCM Failover	The system issues this reason code when the Unified CM fails over and the agent is moved to the Not Ready state.
32756	Not Ready - Phone Working	The system issues this reason code when the agent's phone comes up after it has been through a Phone Down state.
32755	Not Ready - Call Ended	<p>The system issues this reason code when an agent is moved to the Not Ready state after handling a Unified CCX call. This situation occurs in one of two cases:</p> <ol style="list-style-type: none"> <li>1. If an agent (Agent 1) is in the Not Ready state and gets a consult Unified CCX call from another agent (Agent 2). In this case, after handling the call, Agent 1 moves back to the Not Ready state.</li> <li>2. If an agent's Automatic Available option is disabled and this agent gets a Unified CCX call, then this agent goes to the Not Ready state after handling the call.</li> </ol>
32749	Not Ready - Call Cancel	The system issues this reason code when an agent's state is changed from TALKING to Not Ready because of the Cancel feature. The feature is triggered during an ICD consult call between two agents. When the consulting agent presses the Cancel softkey on the phone, the consulted agent is no longer associated with an ICD call and their state changes to Not Ready. This feature is only available on some newer phone models.
32754	Not Ready - Restricted Device	The system issues this reason code if the agent device is flagged as a restricted device by the Unified CM Administrator.
32753	Not Ready - Restricted Line	The system issues this reason code if the agent's phone line is flagged as a restricted device by the Unified CM Administrator.
32752	Not Ready - Cancel Reservation Preview Call	The system issues this reason code when an agent receives a preview outbound call and decides to cancel the reservation by pressing "Decline" button on Cisco Finesse desktop.
32751	Not Ready - Skip Preview Call	The system issues this reason code when an agent receives a preview outbound call and skips the call.
32748	Log Out - Agent Deleted	Agent is logged out from Unified CCX as the agent is deleted from Unified Communications Manager. This event is triggered

		when Unified CCX synchronizes the agent information with Unified Communications Manager.
32750	Not Ready - Extension Modified	The system issues this reason code when an agent is logged out from CCX because the agent's IPCC extension was changed in Unified Communications Manager.
32742	Not Ready - Non ACD Offhook	Agent's state is changed from Ready state to Not Ready state when the monitored Non ICD lines are used for Incoming or Outgoing calls.
32741	Logged Out - Extension Conflict	The system issues this reason code when an agent logs in to Cisco Finesse using an extension number that has already been used by another agent to log in, the first agent is logged out forcibly with this reason code.
32740	Logout - System Initiated Relogin	The system logs out the agent from one session when the agent tries to log in with the same credentials in another session.
33	Not Ready - Supervisor Initiated	The system issues this reason code when the Supervisor changes an agent's state to Not Ready state.
22	Logged Out - Supervisor Initiated	The system issues this reason code when the Supervisor changes an agent's state to log out.
255	Logged Out - Connection Failure	The system issues this reason code when the agent is forcibly logged out when there is a connection failure between the Cisco Finesse Desktop and the Cisco Finesse Server.

## Manage Reason Code Conflicts During Upgrade

System Reason Codes are auto-generated reason codes that may conflict with custom reason codes when upgrading from an older version to Cisco Finesse 11.6(1). If there is a reason code conflict then the following message appears when you sign in to the administration console:

**Custom reason codes conflict with system reason codes. Resolve to avoid reporting inconsistency.**



**Note** Clear your browser cache to ensure that you are allowed to view and resolve system reason code conflicts.

All conflicting reason codes are highlighted. To edit, select each conflicting reason code and click **Edit**. The **Edit Reason Code** area appears. Select the reason code from the available options listed or enter any other code you wish. The code must be unique to the particular category (Not Ready or Sign Out).

Once resolved, the reason code gets sorted based on the reason code number and placed in the table accordingly.

## Wrap-Up Reasons

Wrap-Up reasons represent the reasons that agents can apply to calls. A Wrap-Up reason indicates why a customer called the contact center. For example, you may have one Wrap-Up reason for sales calls and another for support calls.

You can configure Wrap-Up reasons to be available globally to all agents or only to specific teams.

Use the Manage Wrap-Up Reasons gadget to view, add, edit, or delete Wrap-Up reasons. Click the Reason Label header to sort the Wrap-Up reasons in ascending or descending order.



**Note** Cisco Finesse supports a maximum of 100 global and 1500 team Wrap-Up reasons. No more than 100 Wrap-Up reasons can be assigned to any one team.

Cisco Finesse supports the wrap-up functionality for all types of inbound and outbound calls.

- Set the Work mode on incoming attribute to either *Optional* or *Required*.
- Set the Work mode on outgoing attribute to either *Optional* or *Not Allowed*.

If the Work mode on incoming attribute is set to Required, agents automatically transition to wrap-up state after an incoming or Outbound Option call ends. If the Work mode on incoming attribute is set to Optional, agents must select Wrap-Up from the agent state drop-down list while on a call to transition to wrap-up state when the call ends. If the agent does not select Wrap-Up during the call, the agent does not transition to wrap-up state when the call ends.



**Note** The showWrapUpTimer property can be used to show or hide timer in wrap-up state.

If showWrapUpTimer is set to true then timer is displayed.

If showWrapUpTimer is set to false then timer is hidden.



**Note** Wrap-Up timer is configurable. By default wrapUpCountDown property is set to true. The timer counts down by default when the agent is in wrap-up state. For more information, see *Desktop Properties*.

For Example, if you set the timer to 30 seconds, by default the timer starts from 30 and ends at zero.

The default behavior can be changed by setting the wrapUpCountDown property to false.

If an agent is configured for wrap-up and selects a pending state during a call, when the call finishes that agent goes into the pending state selected during the call.

The following table describes the fields on the Manage Wrap-Up Reasons gadget:

Field	Explanation
Reason Label	The label for the Wrap-Up reason.  This label must be unique for each Wrap-Up reason and has a maximum length of 39 bytes (which equals 39 US English characters). Both alphanumeric and special characters are supported.
Global?	Yes/No. Indicates if the Wrap-Up reason is available globally to all agents (Yes) or to specific teams of agents (No).

**Actions on the Manage Wrap-Up Reasons gadget:**

- **New:** Add a new Wrap-Up reason

- **Edit:** Edit an existing Wrap-Up reason
- **Delete:** Delete a Wrap-Up reason
- **Refresh:** Reload the list of Wrap-Up reasons from the server



---

**Note** When you add, edit, or delete a Wrap-Up reason, the changes you make take effect on the agent or supervisor desktop after three seconds. However, agents who are signed in when the changes are made must sign out and sign in again to see those changes reflected on their desktops.

---

#### Related Topics

[Contact Service Queue Configuration Web Page](#)

### Add Wrap-Up Reason

#### Procedure

---

- Step 1** In the Manage Wrap-Up Reasons gadget, click **New**.
- Step 2** In the Reason Label field, add a label for the Wrap-Up reason.
- Note** Wrap-Up reason labels are limited to 39 bytes.
- Step 3** If the Wrap-Up reason is global, select the Global? check box. If the Wrap-Up reason is specific to a team, clear the Global? check box.
- Note** By default, the Global? check box is selected.
- Step 4** Click **Save**.
- 

### Edit Wrap-Up Reason

#### Procedure

---

- Step 1** In the Manage Wrap-Up Reasons gadget, select the Wrap-Up reason that you want to edit.
- Step 2** Click **Edit**.
- The Edit Wrap-Up Reason area appears.
- Step 3** In the Wrap-Up Reason Label field, enter the new label for the Wrap-Up reason. If you want to change who has access to the Wrap-Up reason, select or clear the Global? check box.
- Step 4** Click **Save**.
-

## Delete Wrap-Up Reason

### Procedure

- 
- Step 1** In the Manage Wrap-Up Reasons gadget, select the Wrap-Up reason that you want to delete.
- Step 2** Click **Delete**.
- A question appears asking you to confirm that you want to delete the selected Wrap-Up reason.
- Step 3** Click **Yes** to confirm the deletion of the selected Wrap-Up reason.
- 

## Force Wrap-Up Reason

**For voice channel-**If the Force Wrap-Up reason is configured, agents must select a Wrap-Up reason before changing the state after the call ends. The agent cannot change the state until the Wrap-up reason is applied. The Wrap-Up reason can be selected during the call or after the call ends.

**For digital channels-**If the Force Wrap-Up reason is configured, agents must select a Wrap-Up reason before transferring or ending an interaction.




---

**Note** The Force Wrap-Up reason is disabled by default. Use the CLI commands to enable and disable this feature. For more information, see *Desktop Properties* in [Cisco Finesse Administration Guide](#).

---

## Manage Team Resources

You can assign phone books, reason codes, wrap-up reasons, custom desktop layouts, and workflows to teams on the Team Resources tab of the administration console.

### Team Resources

Use the Manage Team Resources gadget on the Team Resources tab to assign and unassign phone books, reasons, custom desktop layouts, and workflows to teams. Click the Name or ID header to sort the teams in ascending or descending order.

The Manage Team Resources gadget contains six tabs, each enabling you to assign or unassign resources to a team. The tabs are defined in the following table:

Tab Name	Description
Desktop Layout	Use this tab to customize the desktop layout for the team. The default layout is defined in the Manage Desktop Layout gadget. You can define one custom layout for the team.
Phone Books	Use this tab to assign and unassign phone books to the team. Only phone books that are defined in the Manage Phone Books gadget as available to teams are available for assignment.

Tab Name	Description
Reason Codes (Not Ready)	Use this tab to assign and unassign Not Ready reason codes to the team. Only Not Ready reason codes that are defined in the Manage Reason Codes (Not Ready) gadget as available to teams (not global) are available for assignment.
Reason Codes (Sign Out)	Use this tab to assign and unassign Sign Out reason codes to the team. Only Sign Out reason codes that are defined in the Manage Reason Codes (Sign Out) gadget as available to teams (not global) are available for assignment.
Wrap-Up Reasons	Use this tab to assign and unassign Wrap-Up reasons to the team. Only Wrap-Up reasons that are defined in the Manage Wrap-Up Reasons gadget as available to teams (not global) are available for assignment.
Workflows	Use this tab to assign and unassign workflows to the team. Only workflows that are defined in the Manage Workflows gadget are available for assignment.

### Actions on the Manage Team Resources Gadget

- **Add:** Assign a phone book, reason, or workflow to the team
- **Save:** Save the phone book, reason, desktop layout assignment, or workflow to the team
- **Revert:** Cancel any changes made before they are saved
- **Refresh:** Refresh the list of teams




---

**Note** If you select a team and then click Refresh, the team is deselected and the Resources area for that team disappears. The list of teams is refreshed and you must select a team again.

---

### Add or Delete a Team When Database is Not Accessible

If you add or delete a team when Finesse cannot access the Finesse database, those changes do not appear in the Finesse administration console unless you restart Cisco Finesse Tomcat or the Cisco Unified CCX Engine.

## Assign Phone Books and Reasons to Team

### Procedure

---

- Step 1** In the Manage Team Resources gadget, select a team.
- Step 2** Click the tab for the resource you want to assign for the selected team.
- Step 3** Click **Add**.
- Step 4** Select one or more resources from the list to assign them to the team.

Resources you assign are highlighted in blue in the Add <resources> popup and added to the List of <resources> area.

**Step 5** When you finish assigning resources, click **Save**.

**Note** You can make changes on all resource tabs and then save them at the same time. If there is an error on one resource tab but not others, the changes on the tabs with no errors are saved while the changes on the tab with errors are not saved.

---

## Unassign Phone Books and Reasons from Team

### Procedure

---

**Step 1** In the Manage Team Resources gadget, select a team.

**Step 2** Click the tab for the resource you want to unassign from the selected team.

**Step 3** Click the red X next to the resource you want to unassign.

**Step 4** Click **Save**.

---

## Assign Custom Desktop Layout to Team

### Procedure

---

**Step 1** In the **Manage Team Resources** gadget, select a team.

**Step 2** Click **Desktop Layout**.

The Desktop Layout XML area appears. The area contains the default desktop layout XML.

**Step 3** Select the **Override System Default** check box.

The XML becomes editable.

**Step 4** Select from the following editors:

- **Text Editor**
- **XML Editor**

For more information, see *Default Layout XML*.

**Step 5** Edit the XML.

**Step 6** Click **Save**.

The custom desktop layout replaces the default desktop layout for the team after 10 seconds. If a supervisor or agent is signed in when the change is saved, the change does not take effect on their desktop until the supervisor or agent signs out and signs in again.

**Note** If you clear the Override System Default check box, any changes you made to the XML are lost and the XML in the editing pane reverts to the default desktop layout XML.

---





**Note** If the Supervisor is managing single / multiple teams, the custom layout of the team for which the supervisor is a resource/agent is displayed. However, if the supervisor is not the resource/agent of a team, the layout of the default team is displayed.

## Customize Desktop Properties at Team Level

You can customize the Finesse desktop properties for a specific team.

### Procedure

- Step 1** In the **Manage Team Resources** gadget, select a team.
- Step 2** Click **Desktop Layout**.
- Step 3** Select the **Override System Default** check box.
- Step 4** Select from the following editors:
  - **Text Editor**
  - **XML Editor**
- Step 5** Enter the desktop property name in the config key tag.
- Step 6** Enter the possible value of the desktop property in the value tag.

The following are the sample desktop property entries, as displayed in the default **Desktop Layout**. To change these desktop property entries in **Text Editor**, remove the comment (`<!--` and `-->`) and set appropriate values.

**Note** If the property value is defined in the team-specific desktop layout (**Manage Team Resources > Desktop Layout**), then the team-specific desktop layout takes precedence over the property value defined in the **Desktop Layout** and CLI.

For more information on customizing desktop properties at **Desktop Layout**, see *Customize Desktop Properties*.

For more information on Finesse CLIs, see *Desktop Properties*.

The following table lists the desktop properties that support team-level updates:

Config Key	Value	Default Value
enableDragDropAndResizeGadget	true false	false
enableShortCutKeys	true false	true
forceWrapUp	true false	true
wrapUpCountDown	true false	true
showWrapUpTimer	true false	true
desktopChatAttachmentEnabled	true false	true
desktopChatMaxAttachmentSize	Range: 1—10 (MB)	5

Config Key	Value	Default Value
desktopChatUnsupportedFileTypes	Unsupported file formats include comma-separated valid file extensions. For example: .exe, .sh	.exe, .msi, .sh, .bat
showAgentHistoryGadgets	true false	true
showActiveCallDetails (for Supervisor Only)	true false	true
pendingDTMFThresholdCount	Range: 1—20	20
dtmfRequestTimeoutInMs	Range: 1000—200000 (1 to 200 seconds)	5000 (5 seconds)
enableDropParticipantFor	supervisor_only conference_controller_ and_supervisor all	supervisor_only
dropParticipant	agents all	agents

- Note**
- To enable the following Finesse desktop properties in Cisco Finesse, install Cisco Finesse Release 12.5(1) ES1 COP or higher.
    - pendingDTMFThresholdCount
    - dtmfRequestTimeoutInMs
  - To enable the following Finesse desktop properties in Cisco Finesse, install Cisco Finesse Release 12.5(1) ES4 COP or higher.
    - enableDropParticipantFor
    - dropParticipant

For more information on Finesse desktop properties, see *Desktop Properties*.

#### Step 7

Click **Save**.

The change takes effect when the agent or supervisor refreshes the Finesse desktop or sign out and sign in again.

- Note** If you clear the **Override System Default** check box and click **Save**. The changes are overwritten, and the editing pane reverts to the default desktop layout XML.

## Assign Workflows to Team

### Procedure

- Step 1** In the Manage Team Resources gadget, select a team.

- Step 2** Click the Workflows tab.
- Step 3** Click **Add**.
- Step 4** Select one or more workflows from the list to assign them to the team.
- Workflows you assign are highlighted in blue in the Add Workflows popup and added to the List of Workflows area.
- Step 5** Workflows are executed in the order they are listed. Use the up and down arrows to move a selected workflow to the desired position in the list.
- Step 6** When you have finished assigning workflows, click **Save**.
- Note** You can make changes on all resource tabs and then save them at the same time. If there is an error on one resource tab but not on others, the changes on the tabs with no errors are saved while the changes on the tab with errors are not saved.
- 

## Unassign Workflows from Team

### Procedure

---

- Step 1** In the Manage Team Resources gadget, select a team.
- Step 2** Click the Workflows tab.
- Step 3** Click the red X next to the workflow to unassign.
- Step 4** Click **Save**.
- 

## Manage Workflows

On the Workflows tab of the Cisco Finesse administration console, you can create and manage workflows and workflow actions.

## Workflows and Workflow Actions

You can use workflows to automate common repetitive agent tasks. A workflow has a unique name and a helpful description. Use the Manage Workflows and Manage Workflow Actions gadgets to view, add, edit, or delete workflows and workflow actions.

All workflows are team-level workflows. You cannot create a global workflow. If you need a global workflow, create a team workflow and assign it to all teams.

Cisco Finesse supports the following number of workflows and workflow actions:

- 100 workflows per Cisco Finesse system
- 100 actions per Cisco Finesse system
- 20 workflows per team
- Five conditions per workflow

- Five actions per workflow
- Five variables per action
- For Voice - Call variables, Outbound Option variables, queue details, wrap-up reasons, agent details, or team details.
- For Email - Queue name and email attributes like From, To, Cc, Bcc, or Subject.
- For Chat - Queue name, chat type, or system defined customer details as available from the web chat form.

Click the column headers to sort workflows and workflow actions in ascending or descending order.

The following table describes the fields on the Manage Workflows gadget:

The following table describes the fields on the Manage Workflow Actions gadget:

Field	Explanation
Name	The name of the workflow action must be unique and can have a maximum length of 64 characters.
Type	The type of workflow. Possible values are Browser Pop and HTTP Request.

#### Actions on the Manage Workflows and Manage Workflow Actions gadgets:

- **New:** Add a new workflow or workflow action
- **Edit:** Edit a workflow or workflow action
- **Delete:** Delete a workflow or workflow action
- **Refresh:** Reload the list of workflows or workflow actions from the server.

You can configure workflow actions to be handled by the Cisco Finesse desktop or in a third-party gadget. A third-party gadget can be designed to handle the action differently than Cisco Finesse does.

Each workflow must contain only one trigger. Triggers are based on Cisco Finesse dialog events.




---

**Note** You can configure the trigger only after you select the media.

---

- Voice dialog events include the following:
  - When a Call arrives
  - When a Call is answered
  - When a Call ends
  - When making a Call




---

**Note** The call variable workflow responds as expected only when you add both the conditions **Is not equal** and **Is not empty**.

---

- While previewing an Outbound Option call.

The workflow engine uses the following simple logic to determine whether to execute a workflow:




---

**Note** The workflow logic and examples are similar for all media.

---

- Its trigger set and conditions are evaluated against each dialog event received.
- The workflow engine processes workflow events for the first call that matches any configured workflow's trigger set and conditions. No other workflows run until this call has ended. If the agent accepts a second call while still on the first call, workflows do not run on the second call even after the first call has ended.
- After a workflow for a particular trigger type (for example, Call Arrives) executes, it never triggers again for the same dialog ID.

The workflow engine caches workflows for an agent when the agent signs in. Workflows do not change for the agent until the agent signs out and signs in again or refreshes the browser.




---

**Note** Whenever the browser is refreshed, the workflows that trigger the following events run:

- when a call arrives
- when a call is answered
- when making a call

When an agent refreshes the browser, the workflow engine considers the call as newly arrived or newly made. If an HTTP request action is part of the workflow, the HTTP request is sent when the agent refreshes the browser. Applications that receive the HTTP requests must account for this scenario.

---

An example of a workflow is a Call Arrival event that triggers an action that collects information from the dialog event (for example, the ANI or customer information) and displays a web page containing customer information.

You can filter trigger events by the value of the data that comes in the event. You can configure a workflow to execute if any of the conditions are met or if all the conditions are met.

Individual conditions comprise of the following:

- A piece of event data to be examined. For example, **DNIS** or call variables.
- A comparison between the event data and the values entered (for example **contains**, **is equal to**, **is not equal to**, **begins with**, **ends with**, **is empty**, **is not empty**, and **is in list**).

When the trigger and its conditions are satisfied, a list of actions assigned to the workflow are executed. The actions are executed in the listed order.

Workflows run only for agents and supervisors who are Cisco Finesse users. The Workflow Engine is a JavaScript library that runs client-side on a per-user basis within the Cisco Finesse desktop application. The desktop retrieves the workflows that are to be executed for a user from the server when the user signs in or when the browser is refreshed.




---

**Note** Changes made to a workflow or its actions while a user is signed in are not automatically pushed to that user.

---

It is possible to set workflows, conditions, and actions that are contradictory so that a workflow or action cannot function. Workflows are not validated.

If multiple workflows are configured for a team, the Workflow Engine evaluates them in the configured order. The Workflow Engine ignores workflows with no actions. When the Workflow Engine finds a workflow with a matching trigger for an event and the workflow conditions evaluate to true, that workflow is used, and the subsequent workflows in the list are not evaluated. Workflows with no conditions evaluate to true if the event matches the workflow trigger. All workflows are enabled by default. Only one workflow for a specific user can run at a time.

The Workflow Engine retrieves dialog-based variables that are used in workflow conditions from the dialog that triggered the workflow. If a variable is not found in the dialog, its value is considered to be empty.

The Workflow Engine executes the actions that are associated with the matched workflow in the order in which they are listed. The Workflow Engine executes actions in a workflow even if the previously executed action fails. Failed actions are logged.

The Cisco Finesse server controls the calls that are displayed to the Cisco Finesse user. If the user has multiple calls, the workflow applies only to the first call that matches a trigger. If the first call displayed does not match any triggers but the second call does match a trigger, the Workflow Engine evaluates and processes the triggers for the second call.

A call is considered to be the first displayed call if it is the only call on the Cisco Finesse desktop when it appears. If two calls on a phone are merged (as they are in a conference call), then the first displayed call flag value of the surviving call is used.

If a user has a call and the user refreshes the browser, the Workflow Engine evaluates the call as it is. If the dialog data (call variable values) change, the data may not match the trigger and conditions of the original workflow. The data may match a different workflow or no workflows at all.

If a user has multiple calls and the user refreshes the browser, the Workflow Engine treats the first dialog received from the Cisco Finesse server as the first displayed call. This call may not be the same call that was first displayed before the refreshing the browser. Dialogs received for any other call are ignored because they are not considered as first displayed calls. After refreshing the browser, if dialogs for more than one call are received before the Workflow Engine is loaded, none of the dialogs are evaluated because they are not considered as first displayed calls.

Workflows that are run for both Cisco Finesse agents and supervisors. The team to which the supervisor belongs (as distinguished from the team that the supervisor manages) determines which workflows run for the supervisor. Put the supervisors in their own team to keep agent workflows from being run for them.

## Workflow Triggers and Outbound Calls




---

**Note** When you create a workflow specifically for Outbound Option calls, add a condition of BAStatus is not empty (except for the Workflow Trigger 'When a call arrives' as BAStatus will be empty at that point of time). This condition ensures that the workflow can distinguish Outbound Option calls from agent-initiated outbound calls.

---

The following table illustrates when workflows trigger in outbound call scenarios:

Workflow Trigger	Direct Preview Outbound Call	Preview Outbound Call	Progressive/Predictive Outbound Call
While previewing a call	When the agent previews the call (before accepting or rejecting it)	When the agent previews the call (before accepting or rejecting it)	Does not trigger
When a call arrives	Does not trigger	When the agent accepts the call	When the call arrives on the agent desktop
When a call is answered	When the customer answers the call and during failover	When the customer answers the call and during failover	When the customer answers the call
When a call is made	When the customer call is initiated	When the customer call is initiated	When the customer call is initiated, and during failover
When a call ends	When the customer call ends	When the customer call ends	When the customer call ends

## Add Browser Pop Workflow Action

The Browser Pop workflow action opens a browser window or tab on the user's desktop when workflow conditions are met.



**Note** Whether the action opens a new window or tab on the desktop depends on the target user's browser settings.

### Procedure

**Step 1** In the Manage Workflow Actions gadget, click **New**.

**Step 2** In the Name box, enter a name for the action.

**Note** Workflow action names are limited to 64 characters.

**Step 3** From the Type drop-down list, choose **Browser Pop**.

**Step 4** From the Handled By drop-down list, choose what will execute the action, either the Finesse Desktop or Other (a third-party gadget).

**Step 5** In the Window Name box, enter the ID name of the window that is opened. Any action that uses this window name reuses that specific window.

**Note** Window names are limited to 40 characters, and can be blank. If you leave the window name blank, a new window opens every time the action runs.

- Step 6** Enter the URL of the browser window and click the tag icon at the right of the box and select one or more variables from the drop-down list to add tags.

**Example:**

`http://www.google.com/search?q=`

For every variable you select, you can enter test data in the Sample Data box. A sample URL is automatically built in the Browser URL box below the Sample Data area. To test the URL, click Open to open the URL in your browser.

**Note** Finesse does not validate the URL you enter.

- Step 7** Click **Save**.

## Add HTTP Request Workflow Action

The HTTP Request workflow action makes an HTTP request to an API on behalf of the desktop user.

### Procedure

- Step 1** In the Manage Workflow Actions area, click **New**.
- Step 2** In the Name box, enter a name for the action.  
A workflow action name can contain a maximum of 64 characters.
- Step 3** From the Type drop-down list, select **HTTP Request**.
- Step 4** From the Handled By drop-down list, select what will execute the action, the Finesse desktop or Other (a third-party gadget).
- Step 5** From the Method drop-down list, select the method to use.  
You can select either PUT or POST.
- Step 6** From the Location drop-down list, select the location.  
If you are making the HTTP request to a Finesse API, select **Finesse**. If you are making a request to any other API, select **Other**.
- Step 7** In the Content Type box, enter the content type.  
The default content type is application/xml, which is the content type for Finesse APIs. If you are using a different API, enter the content types for that API (for example, application/JSON).
- Step 8** In the URL box, enter the URL to which to make the request. To add variables to the URL, click the tag icon at the right of the box and select one or more variables from the drop-down list.

**Example:**

The following is the URL example for a Finesse API:

`/finesse/api/Dialog/`



**Note** When the location is FINESSE, do not specify the protocol, host, and port information. Finesse automatically fetches these details when the REST request is executed.

If you want to make a request to another API, you must enter the entire URL (for example, <http://googleapis.com>).

You can click the tag icon at the right of the box and select one or more variables from the drop-down list to add tags to the URL. In the preceding example, to add the dialogId, click the tag icon and select dialogId from the list.

**Step 9** In the Body box, enter the text for the request. The body must match the content type (for example, if the content type is application/xml, the body must contain XML). To add variables to the body, click the tag icon at the right of the box and select one or more variables from the drop-down list.

**Example:**

To make an HTTP request to the Dialog - Start a recording API, enter the following into the Body box:

```
<Dialog>
<targetMediaAddress> extension ✖ </targetMediaAddress>
<requestedAction>SEND_DTMF</requestedAction>
<actionParams><ActionParam><name>dtmfString</name><value>8</value></ActionParam></actionParam
</Dialog>
```

To add the extension, click the tag icon and select extension.

For every variable you add, you can enter test data in the Sample Data box.

**Step 10** Click **Save**.

## Edit Workflow Action

### Procedure

- Step 1** In the Manage Workflow Actions gadget, select the action that you want to edit.
- Step 2** Click **Edit**.
- Step 3** Edit the fields that you want to change.
- Step 4** Click **Save**.

## Delete Workflow Action

### Procedure

- Step 1** In the Workflow Actions gadget, select the action that you want to delete.
- Step 2** Click **Delete**.

**Step 3** Click **Yes** to confirm the deletion of the selected action.

---

## Add Workflow

### Procedure

---

**Step 1** In the Manage Workflows gadget, click **New**.

**Step 2** From the **Choose Media** drop-down, select the media.

**Note** In case of a voice only configuration, the **Choose Media** drop-down will display only Voice.

**Step 3** In the **Name** box, enter the name of the workflow.

**Note** The name is limited to 40 characters.

**Step 4** In the **Description** box, enter a description of the workflow.

**Note** The description is limited to 128 characters.

**Step 5** In the **When to perform Actions** drop-down list, select the event that triggers the workflow.

**Note** The drop-down actions change depending on the selected media.

**Step 6** In the **How to apply Conditions** box, select if all conditions are met, or if any conditions are met, and then click **Add Condition** to add up to five conditions.

**Note** Variables in the drop-down for conditions are grouped depending on the selected media.

The fields **To**, **Cc**, and **Bcc** support comma separated values, so that, agents can enter multiple email IDs.

### Example:

For example, you can specify that the action is taken when CallVariable 1 equals 123 and CallVariable 2 begins with 2.

**Step 7** In the Ordered List of Actions area, click **Add** to open the Add Actions area. Click an action in this area to add it to the Ordered List of Actions.

**Step 8** Use the up and down arrows next to the Ordered List of Actions to move actions into the performance order.

**Step 9** Click **Save**.

**Step 10** Assign the workflow to one or more teams.

**Note** A workflow does not run until it is assigned to a team.

---

## Edit Workflow

### Procedure

- 
- Step 1** In the Manage Workflows gadget, select the workflow you want to edit.  
**Step 2** Click **Edit**.

**Note** The media for an existing workflow can be changed by editing the workflow.

- Step 3** Edit the fields that you want to change.  
**Step 4** Click **Save**.
- 

## Delete Workflow

### Procedure

- 
- Step 1** In the Manage Workflows gadget, select the workflow that you want to delete.  
**Step 2** Click **Delete**.  
**Step 3** Click **Yes** to confirm the deletion of the selected workflow.
- 

## Manage Connected Agents

### Connected Agents

Use the Connected Agents gadget on the Connected Agents tab to view the list of agents currently signed in to Cisco Finesse

You can use this gadget to determine which agents are signed in to the Publisher Side or the Subscriber Side. You can use this gadget also to filter the client types and identify the client type through which an agent has logged in. The client types can be Finesse Desktop, Finesse IP Phone, and Custom Desktop.

The list of signed-in agents is displayed in the form of a table, the Connected Agents table.

You can search the Connected Agents table for certain entries, sort the table, or refresh the table to view the latest data. The number of agents signed in to the Publisher Side and the Subscriber Side are displayed in the gadget (above the table).

The columns of the Connected Agents table are displayed below:

Column	Explanation
Agent Name	The first and last name of an agent.
Username	The Agent ID or username required to sign in to Cisco Finesse.
Extension	The extension number of the agent.

Column	Explanation
Team	The team the agent belongs to.
Connected Time	The total duration (in hh:mm:ss) for which the agent has been logged in.
Connected Side	Publisher/Subscriber/Both Sides.
Finesse Host	The Finesse host through which the agent is connected.

### Actions on the Connected Agents Gadget

- **Search:** Searches for the entered text across all columns of the Connected Agents table.
- **Sort:** Sorts the column values of the Connected Agents table in ascending or descending order.
- **Filter:** Filters agents connected to Both Sides, the Publisher side, or the Subscriber side.  
The default selection for this drop-down box is Both Sides.
- **Refresh:** Refreshes the Connected Agents table. When the Refresh button is clicked, a new REST API call is made to both the publisher and subscriber servers to get the latest information about the signed-in agents.  
The time at which the agent information was last fetched from the server is displayed beside the Refresh button (For example, Updated 45 minutes ago).

## Manage Security

The Cisco Finesse administration console and agent desktop support secure HTTP (HTTPS). To access the administration console, enter the following URL in your browser (where *FQDN* is the fully qualified domain name of your primary server):

`https://FQDN:8445/cfadmin`

Similarly, agents and supervisors can access their desktops as follows:

`https://FQDN:8445/`

For HTTPS access, you can eliminate browser security warnings by choosing to trust the self-signed certificate provided with Finesse or uploading a CA certificate.

If you add custom gadgets that perform HTTPS requests to Finesse, you must add a certificate to the Finesse server for that gadget.




---

**Note** Wildcard Certificates are not supported in Unified CCX.

---

## HTTPS Support

The Cisco Finesse administration console and agent desktop supports only HTTPS. To access the administration console using HTTPS, enter the following URL in your browser:

`https://FQDN: 8445/cfadmin`

Where *FQDN* is the name of your primary Finesse server and 8445 is the port number.

Similarly, agents and supervisors can access their desktops using HTTPS as follows:

- `https://FQDN:8445/desktop`

For HTTPS access, you can eliminate browser security warnings by choosing to trust the self-signed certificate provided with Finesse or uploading a CA certificate.

If you add custom gadgets that perform HTTPS requests to Finesse, you must add a certificate to the Finesse server for that gadget.

## HSTS

Finesse supports HTTP Strict Transport Security (HSTS) for increased security. HSTS is automatically enabled, in which case the Finesse server sends HTTPS responses indicating to browsers that Finesse can only be accessed using HTTPS. If users then try to access Finesse using HTTP instead of HTTPS, the browser changes the connection to HTTPS before generating any network traffic. This functionality prevents browsers from sending requests to Finesse using unencrypted HTTP before the server can redirect them.

## Cross-Origin Resource Sharing (CORS)

Finesse supports CORS requests and allows the customization of the domains which are allowed to make CORS requests to the Finesse desktop. Once CORS is enabled via the CLI **utils finesse cors enable**, the CORS origin request from external domains is blocked by the browser. To enable specific domains to access Finesse desktop via CORS, the domains need to be added to the CORS origin allowed list using the CLI **utils finesse cors allowed\_origin add**. For more information on the CORS CLIs, see *Cisco Finesse CLI*.

## Gadget Source Allowed List

Shindig proxies requests from the Finesse desktop to external servers and this introduces the possibility of server side request forgery (SSRF). To prevent SSRF, you can choose to restrict outgoing connections requested by the gadgets to specific URIs by enabling Shindig allowed listing CLIs and adding the required URIs to the allowed list. For more information on Gadget Source Allowed List CLIs, see *Cisco Finesse CLI*.

## Security Enhancements

The security enhancements in Cisco Finesse are as follows:

- By default, Cisco Finesse Notification Service unsecure XMPP port 5222 and BOSH/WebSocket (HTTP) port 7071 are disabled.

Use the CLI command **utils finesse set\_property webservices enableInsecureOpenfirePort true** to enable these ports.

For more information on CLI commands, see *Service Properties*.

# Manage Finesse IP Phone Agent

## Finesse IP Phone Agent

With Finesse IP Phone Agent (IPPA), agents and supervisors can access Finesse features on their Cisco IP Phones as an alternative to accessing Finesse through the browser. Finesse IPPA supports fewer features than the Finesse desktop in the browser, but it does allow agents and supervisors to receive and manage Finesse calls if they lose or do not have access to a computer.

### Supervisor Tasks

Finesse IPPA does not support supervisor tasks such as monitor, barge, and intercept, but supervisors can sign in and perform all agent tasks on their IP Phones.

### Administration Tasks

After you configure Finesse IPPA, the administration tasks that you perform for the Finesse desktop also apply for the supported Finesse IPPA features. For example, the Call Variables Layouts that you configure for the desktop also apply for Finesse IPPA, although the column layout is modified to fit the IP Phone screen.

### Reason Code Limitations

- On the IP Phone, Finesse can display a maximum of 100 Not Ready, Wrap Up, or Sign Out reason codes. If more than 100 codes are configured, the phone lists the first 100 applicable codes (global or applicable team codes).
- When Finesse IPPA displays reason codes, some IP Phone models truncate the codes due to character length limitations on the phone. To ensure they meet your requirements, verify the display of the reason codes on all phone models in your environment.

### Finesse IP Phone Agent Service Access Protocol

Finesse IPPA phone clients communicate with the Finesse server using Secure HTTP (HTTPS) protocol.

### Failure Behavior

Unlike the Finesse desktop, the Finesse IP Phone Agent does not automatically failover to the alternate Finesse server. To resume normal operations in a failure scenario, the Finesse IPPA agents must exit from the current Finesse IP Phone service and manually sign in to another configured Finesse service that connects to an alternate Finesse server.

To ensure continued operations in a failure situation, you must configure at least two Finesse IP Phone services in Unified CM, each pointing to different Finesse servers.

## One Button Sign In

With One Button Sign In, you can set up the Finesse IPPA phones with prepopulated agent ID, extension, and password. In this case, agents can sign in to Finesse on the IP Phone without credentials just by selecting Cisco Finesse from the Services menu.

Alternatively, you can set up One Button Sign In and prepopulate only a subset of agent credentials. For example:

- You can prepopulate only the agent ID and extension, forcing the agents to manually enter their password at sign-in for increased security.
- You can prepopulate only the extension, forcing agents to manually enter their ID and password at sign-in (useful for agents who share the same phone).

You can use Unified CM Administration to prepopulate the agent credentials, or you can set up the agents with access to the Unified CM Self Care Portal to prepopulate their own credentials.

The following table shows examples of how you can assign the responsibility of defining agent credentials to the administrator or the agent, or share that responsibility between them:

<b>Example Set Up</b>	<b>Prepopulated in Unified CM Administration (by Administrator)</b>	<b>Prepopulated in Self Care Portal (by Agent)</b>	<b>Entered at Sign-In (by Agent)</b>
<b>Administrator populates the extension only</b>	extension	-	id password
<b>Administrator populates the ID and extension</b>	id extension	-	password
<b>Agents enter password only using Self Care Portal</b>	id extension	password	-
<b>Agents enter all credentials using Self Care Portal</b>	-	id extension password	-
<b>Agents enter ID and extension only using Self Care Portal</b>	-	id extension	password

## Finesse IP Phone Service Subscription Options

To set up access to Finesse on agent IP phones in Cisco Unified Communications Manager, you must create the Finesse IP Phone service to which the phones can subscribe. To set up the Finesse service, you can choose one of the following options:

- Set up an enterprise subscription to automatically subscribe all IP phones in the cluster to the Finesse service. (Not supported with One Button Sign In.)
- Set up a manual subscription, and manually subscribe each IP phone to the Finesse service.
- Set up a manual subscription, and set up the agents with access to the Unified CM Self Care Portal to subscribe to the Finesse service.

The following table lists the Finesse IPPA configuration procedures and indicates which procedures are required depending on the subscription option you choose:

Finesse IPPA Configuration Procedures	Enterprise Subscription	Manual Subscription	
		Administrator Manually Subscribes the Phones	Agents Manually Subscribe Their Phones Using the Self Care Portal
<i>Set Up Application User, Web Access, and HTTPS Server Parameters</i>	Required	Required	Required
<i>Configure Finesse IP Phone Service in Unified CM</i>	Required	Required	Required
<i>Add Service Parameters for One Button Sign In</i>	Not applicable	Required only with One Button Sign In	Required only with One Button Sign In
<i>Subscribe Agent Phones to Manual Subscription Service</i>	Not applicable	Required	Optional. Allows the administrator to enter agent credentials for One Button Sign In.
<i>Set Up Agent Access to the Self Care Portal</i>	Not applicable	Optional. Allows agents to enter their own credentials for One Button Sign In.	Required

## Set Up Application User, Web Access, and HTTPS Server Parameters

To support Finesse IPPA functionality, you must configure an application user in Unified Communications Manager that is associated with all Finesse IPPA phones. For proper Finesse IPPA operation, you must also set the Web Access and HTTPS Server parameters in Unified CM.

The following steps are required for both manual and enterprise subscriptions:

### Before you begin

Set up call capabilities for the agent phones in Cisco Unified Communications Manager.

### Procedure

**Step 1** Set the following parameters in Unified CM:

- Set the **Web Access** parameter to **Enabled**.
- Set the **HTTPS Server** parameter to **HTTPS Only**.

To set these parameters in Cisco Unified CM Administration, use either of the following pages:

- Phone Configuration page (Product Specific Configuration portion of page): choose **Device > Phone**.
- Enterprise Phone Configuration page: choose **System > Enterprise Phone Configuration**.

**Step 2** Configure an application user in Unified Communications Manager.



- a) In Cisco Unified Communications Manager Administration, select **User Management > Application User**.
- b) Click **Add New**.
- c) Under User Information, enter a user ID and password for the new user.  
The password must be 95 characters or less and must contain ASCII characters only.
- d) Under Device Information, in the Available Devices pane, select all phones that Finesse IP Phone Agents will use and move them to the Controlled Devices pane using the arrows.
- e) Under Permissions Information, click **Add to Access Control Group**.
- f) From the list of search results, select **Standard CTI Enabled** and **Standard CTI Allow Control Of All Devices** and then click **Add Selected**.  
The application user is added to the Standard CTI Enabled and Standard CTI Allow Control Of All Devices groups.
- g) Click **Save** at the bottom of the page.

**Note** In UCCX deployments, usage of an existing RMCM User for Finesse IPPA is known to cause problems in functionality, however, the physical phones must be associated with the RMCM User.

**Step 3** Enter the application user's credentials in the Finesse IP Phone Agent Settings gadget.

- a) Sign in to the Cisco Finesse Administration Console.
- b) Choose **Settings > IP Phone Agent Settings**.
- c) Under Phone URL Authentication Settings, enter the same username and password that you entered in Unified CM for the application user.  
The password must be 95 characters or less and must contain ASCII characters only.
- d) Click **Save**.
- e) Restart Cisco Finesse Tomcat on the primary Unified CCX node.
- f) After replication is complete, restart Cisco Finesse Tomcat on the secondary Unified CCX node.

For information to check the replication status, see Step 3 of **Prepare System for IP Address/hostname Change**.

**Note** For Finesse IP Phone Agent (IPPA) from 11.0 (1) onwards, the User Device Profile (UDP) must be associated with the Finesse IP Phone Agent Application User along with the physical phones for agents using Extension Mobility. The Finesse Service URL must use the complete FQDN of the Unified CCX server.

---

## Configure Finesse IP Phone Service in Unified CM

The following procedure describes the steps required for manual and enterprise subscription.

### Procedure

---

- Step 1** Log in to the Unified CM Administration using administrator credentials.
- Step 2** Select **Device > Device Settings > Phone Services**.
- Step 3** Click **Add New** to create a new IP phone service.

- Step 4** In the **Service Name** field, enter **Cisco Finesse** (or another service name that is appropriate for your environment).
- Step 5** In the **Service URL** field, enter: `http://Finesse FQDN:8082/fippa/#DEVICENAME#`
- Note** The **Service URL** entry is mandatory for Unified CM.
- Step 6** In the **Secure-Service URL** field, enter: `https://Finesse FQDN:8445/fippa/#DEVICENAME#` to configure Finesse IP Phone Agent.
- Note**
- Support to HTTP is disabled from Cisco Finesse, Release 12.5(1) onwards. Step 5 and Step 6 are mandatory to save the Finesse IP Phone Agent settings.
  - Import certificates for Finesse IP Phone Agent to communicate with the Finesse server using Secure HTTP (HTTPS) mode. For more information, see *Finesse IP Phone Agent Certificate Management*.
- Step 7** Ensure that the **Service Category** is set to **XML Service**, and the **Service Type** is set to **Standard IP Phone Service**.
- Step 8** Check the **Enable** check box.
- Step 9** Perform one of the following:
- To automatically subscribe all phones in the cluster to the Finesse service, check the **Enterprise Subscription** check box, and click **Save**. Agents and supervisors can now access Cisco Finesse by selecting it from the **Services** menu on subscribed IP phones.
- Note** One Button Sign In is not supported with enterprise subscriptions.
- To subscribe only the desired phones to the Finesse service manually, leave the **Enterprise Subscription** check box unchecked and click **Save**.
- Step 10** With a two-node Finesse setup (primary and secondary Finesse servers), perform the preceding steps again to create a secondary Finesse service that points to the secondary Finesse server. When you create the secondary service, note the following procedural differences:
- At Step 4, in the **Service Name** field, enter a name that distinguishes the secondary service from the primary service, such as **Cisco Finesse Secondary**.
  - At Step 5 and Step 6, replace *Finesse FQDN* with the FQDN of the secondary server.
- Note** The language used in Finesse IPPA is selected based on the User Locale field in Unified CM. The language selected based on the User Locale must be available in the Unified CCX language pack for Unified CCX deployments. Unified CCX language pack for Unified CCX deployments and Unified CCE pack for Unified CCE deployments.
- If the language selected based on the User Locale in Unified CM is not available in the respective deployments Unified CCX deployment, Finesse IPPA displays all content in the default language (U.S. English).
-

## Finesse IP Phone Agent Certificate Management

The administrator must perform the following operations to enable Finesse IP phones to communicate with the Finesse server using HTTPS.

- For a CA-signed certificate, see [CA-Signed Certificate, on page 103](#).
- For a self-signed certificate, see [Self-Signed Certificate, on page 103](#).

### CA-Signed Certificate

#### Procedure

---

- Step 1** Obtain the CA-signed certificate from the signed authority for both Cisco Unified CCX and CUCM server.
- Step 2** Import the CA-signed certificate of CUCM to the Cisco Unified CCX server trust store as **tomcat-trust**. For more information, see [Import CUCM Certificate, on page 104](#).
- Step 3** Import the CA-signed certificate of Cisco Unified CCX certificate to the CUCM trust store as **Phone-trust**. For more information, see [Import Certificate into CUCM Trust Store, on page 105](#).
- 

### Self-Signed Certificate

#### Procedure

---

- Step 1** Export the self-signed CUCM certificate from the Cisco Unified Operating System Administration. For more information, see [Export CUCM Certificate, on page 103](#).
- Step 2** Import the downloaded self-signed CUCM certificate to the Cisco Unified CCX trust store as **tomcat-trust**. For more information, see [Import CUCM Certificate, on page 104](#).
- Step 3** Export the self-signed Cisco Unified CCX certificate from the Cisco Unified Operating System Administration. For more information, see [Export Cisco Unified CCX Certificate, on page 104](#).
- Step 4** Import the downloaded self-signed Cisco Unified CCX certificate to the CUCM trust store as **Phone-trust**. For more information, see [Import Certificate into CUCM Trust Store, on page 105](#).
- 

### Export CUCM Certificate

#### Procedure

---

- Step 1** Sign in to Cisco Unified OS Administration on the CUCM server using the following URL: `https://FQDN of CUCM server:8443/cmplatform`.
- Step 2** Select **Security > Certificate Management**.
- Step 3** Enter the search criteria as **tomcat** and then click **Find** to filter the certificate.

The tomcat certificates list is displayed. If you do not find the tomcat certificate for your server in the **Certificate List**, then click **Generate Self-signed**. When the certificate generation is complete, reboot your server. Then

restart this procedure. For more information on generating the self-signed certificate, see *Cisco Unified Operating System Administration Online Help*.

- Step 4** Click the tomcat certificate hyperlink in the **Common Name** column. The tomcat **Certificate Details** dialog box is displayed.
- Step 5** Click **Download .PEM File**.
- Step 6** Save the .PEM file in your local machine.

---

### What to do next

Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

### Import CUCM Certificate

#### Procedure

---

- Step 1** Sign in to Cisco Unified OS Administration on the Cisco Unified CCX server using the following URL: `https://FQDN of Unified CCX server:8443/cmplatform`.
- Step 2** Select **Security > Certificate Management > Upload Certificate/Certificate chain**.
- Step 3** From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
- Step 4** In the **Upload File** field, click **Choose File** and browse to the tomcat.pem or CA-signed certificate file that you saved on your system.
- Step 5** Click **Upload**.
- Step 6** Restart Cisco Finesse tomcat and Cisco Unified CCX Notification Service.

**Note** Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

---

### Export Cisco Unified CCX Certificate

#### Procedure

---

- Step 1** Sign in to Cisco Unified OS Administration on the Cisco Unified CCX server using the following URL: `https://FQDN of Unified CCX server:8443/cmplatform`.
- Step 2** Select **Security > Certificate Management**.
- Step 3** Enter the search criteria as **tomcat-trust** and then click **Find** to filter the certificate.  
  
The tomcat-trust certificates list is displayed. If you do not find the tomcat certificate for your server in the **Certificate List**, then click **Generate Self-signed**. When the certificate generation is complete, reboot your server. Then restart this procedure. For more information on generating the self-signed certificate, see *Cisco Unified Operating System Administration Online Help*.
- Step 4** Click the tomcat-trust certificate hyperlink in the **Common Name** column.

- The tomcat **Certificate Details** dialog box is displayed.
- Step 5** Click **Download .PEM File**.
- Step 6** Save the .PEM file in your local machine.
- 

### What to do next

Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

## Import Certificate into CUCM Trust Store

### Procedure

---

- Step 1** Sign in to Cisco Unified OS Administration on the CUCM server using the following URL: `https://FQDN of CUCM server:8443/cmplatform`.
- Step 2** Select **Security > Certificate Management > Upload Certificate/Certificate chain**.
- Step 3** From the **Certificate Purpose** drop-down list, select **Phone-trust**.
- Step 4** In the **Upload File** field, click **Browse** and browse to the tomcat.pem or CA-signed certificate file that you saved on your system.
- Step 5** Click **Upload**.
- Step 6** Reboot the Cisco Unified Communications Manager (CUCM) server.

**Note** Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

---

## Add Service Parameters for One Button Sign In

With One Button Sign In, for any agent credentials that you want prepopulated, you must set up corresponding service parameters in Unified CM.

Only perform this procedure if you are setting up One Button Sign In. Otherwise, skip this.

### Procedure

---

- Step 1** From Cisco Unified Communications Manager Administration, select the Finesse phone service (under **Device > Device Settings > Phone Services**).
- Step 2** Click **New** to the right of the Parameters box.
- Step 3** Set up service parameters for the agent id, extension, and password credentials as per the following table. Enter only the parameters that you want prepopulated for the agents. For each parameter, enter the required field values and click **Save**. To add parameters, click **Add New** and enter the required values.

Field	Description
<b>Parameter Name</b>	<p>Enter one of the following parameter names as follows:</p> <ul style="list-style-type: none"> <li>• Id</li> <li>• Extension</li> <li>• Password</li> </ul> <p>The values entered are the exact query string parameters used for the subscription URL.</p>
<b>Parameter Display Name</b>	Enter a descriptive parameter name; for example, id, extension, and password.
<b>Default Value</b>	Leave the default value blank for all parameters.
<b>Parameter Description</b>	Enter a description of the parameter. The user can access this text when they subscribe to the service.
<b>Parameter is Required</b>	<p>If the administrator prepopulates the parameter in Unified CM Administration, check the <b>Parameter is Required</b> box.</p> <p>However, if the agent prepopulates the parameter in the Self Care Portal, two options are available:</p> <ul style="list-style-type: none"> <li>• If the agents prepopulates all defined parameters, check the <b>Parameter is Required</b> box for each parameter.</li> <li>• If the agent and administrator share the responsibility of prepopulating the parameters, set only the administrator-defined parameters as required. This configuration ensures that the administrator can save the subscription without prepopulating all parameters. In this case, the administrator first prepopulates the required parameters, and then the agents prepopulate the nonrequired parameters.</li> </ul>
<b>Parameter is a Password (mask contents)</b>	<p>Check this box for the password only.</p> <p>This check box masks the password entries in the Self Care Portal, to display asterisks rather than the user entry.</p>

When you save the last parameter, click **Save and Close**.

### What to do next

You can prepopulate the agent credentials when you subscribe the agent phones, or the agents can prepopulate their own credentials using the Unified CM Self Care Portal.

## Subscribe Agent Phones to Manual Subscription Service

If you set up the Finesse service as a manual subscription, you can subscribe the agent phones to the Finesse service in Unified CM and optionally define agent credentials for One Button Sign In.

If you prefer to allow the agents to subscribe to the Finesse service using the Self Care Portal and prefer not to specify One Button Sign In credentials for the agents, you can skip this procedure.

### Procedure

---

- Step 1** From the menu bar, select **Device > Phone**.
- Step 2** Select the phone that you want to subscribe to the Finesse service.
- Step 3** From the **Related Links** drop-down list on the upper right side of the window, select **Subscribe/Unsubscribe Services** and click **Go**.
- The **Subscribed IP phone services** window displays for this phone.
- Step 4** From the **Select a Service** drop-down list, select **Cisco Finesse**.
- Step 5** Click **Next**.
- Step 6** (*Applicable for One Button Sign In only*) Enter values for any of the defined service parameters (id, password, and extension) that you do not want the agents to enter using the Self Service Portal or at sign-in.
- Step 7** Click the **Subscribe** button to subscribe this phone to the Cisco Finesse service.
- The Cisco Finesse service displays in the **Subscribed Services** list.
- Step 8** Click **Save**.
- The subscribed agents or supervisors can now access Cisco Finesse by selecting it from the **Services** menu on their IP phones.
- Step 9** With a two-node Finesse setup (primary and secondary Finesse servers), perform this procedure again to also subscribe the phones to the secondary Finesse service that points to the secondary Finesse server.
- 

## Set Up Agent Access to the Self Care Portal

You can optionally set up the agents with access to the Unified CM Self Care Portal to prepopulate their own credentials and to subscribe to the Finesse service.

If you are not setting up One Button Sign In, or not enabling the agents with access to the Self Care Portal, skip this procedure.

### Procedure

---

- Step 1** From the Unified CM Administration page, select **System > Enterprise Parameters**.
- Step 2** Under the Self Care Portal Parameters, in the **Self Care Portal Default Server** field, select the IP address of the Unified CM Publisher server from the drop-down list and click **Save**.
- Step 3** Select **User Management > End User**.
- Step 4** Select the user that you want to set up with access to the User Care Portal.
- Step 5** Under Permissions Information, click **Add to Access Control Group**.
- Step 6** From the list of Access Control groups displayed, check **Standard CCM End Users** and click **Add Selected**.
- Step 7** Click **Save**.
-

With access enabled to the Self Care Portal, agents can sign in to the portal at `http://<UCM address>/ucmuser` to subscribe to the Finesse service and enter their own credentials under **Phones > Phone Settings > Services**.




---

**Note** In a two-node Finesse setup with two services configured, the agents must enter their credentials on the primary and secondary Finesse services.

---

## Cisco Finesse Failover Mechanisms

### CTI Failover

CTI failover is when the Finesse service disconnects from one CTI server and reconnects to the same or another CTI server.

The prerequisites for successful CTI failover are as follows:

- Unified Contact Center Express (Unified CCX) must be configured in High Availability (two-node, publisher and subscriber) setup.
- Unified CCX REST service on the local CCX node must be up and running.

In the two-node setup, if Finesse loses connection to the Unified CCX server, it attempts to connect to the server which is running. Finesse alternates between the configured servers until it makes a successful connection.

While failover is in progress, Finesse transitions to `OUT_OF_SERVICE` state. During this period, Finesse does not entertain client requests or send out events. Any request made during this time receives a 503 Service Unavailable error message.

After reconnecting to a Unified CCX server and transitioning to `IN_SERVICE` state, Finesse responds to client requests and publishes events.




---

**Note** For Finesse transition to `IN_SERVICE`,

- Unified CCX REST services on the publisher must be `IN_SERVICE`.
- Unified CCX server CTI connectivity to the publisher or the subscriber must be successful.

---

Connection to the Unified CCX server can be lost due to the following reasons:

- Finesse misses three consecutive heartbeats from the connected Unified CCX server (heartbeat interval is five seconds).
- Finesse socket that is opened to the Unified CCX server.
- Unified CCX REST services on the publisher transitions to `OUT_OF_SERVICE`.

After the failover is complete, the last state of call control, call data, or agent state are published as events to all clients. This allows Finesse clients to reflect an accurate view of the call control, call data, and agent state.

If an agent either makes or answers a call, and then ends that call during failover (that is, the entire call takes place during failover), the corresponding events are not published.





---

**Note** An agent or supervisor might experience certain limitations, related to preservation of their states over failover. Examples include, but are not limited to, the following:

- The Finesse desktop does not show the agent state as it was before the failover, instead shows NOT READY state.
- The Finesse desktop does not show the pending state that the agent had set before the failover.
- The Finesse desktop shows NOT READY state even when there is an active call.

Despite these limitations, the agent and supervisor can continue to perform normal operations on the phone.

---

## Finesse Desktop Failover

Desktop failover can occur for the following reasons:

- When the Finesse desktop loses network connectivity to the Unified CCX Notification Service.
- When the Finesse Tomcat Service becomes *Unavailable*
- When the Finesse REST API Service becomes *Unavailable*
- When the Unified CCX Notification Service becomes *Unavailable*
- When the Finesse loses connection to the publisher



- 
- Note**
- After the failover, the pending state of an agent will not be displayed once the agent fails over to the subscriber. The pending state change is lost during the failover, as the agent will be logged out, and logged in again.
  - Finesse is IN\_SERVICE, coordinates the distribution of desktop reloads, such that failover and consequent desktop reloads are evenly distributed to prevent overwhelming of the Finesse service. Configuration data such as reason codes, workflows and so on are not reloaded during failover to improve the performance.
- 

If the server that an agent is connected transitions to OUT\_OF\_SERVICE, the agent receives a notification that the connection with the server is lost. The Finesse desktop:

- Checks whether the subscriber is available and IN\_SERVICE.
- Continues to check whether the publisher recovers its state.

If the subscriber is available, then the desktop automatically signs the agent into the subscriber. If the publisher recovers its state, the desktop notifies the agent that it has reconnected.

The failover logic has three triggers to detect desktop failure:

- The Finesse desktop receives a SystemInfo event that the publisher is OUT\_OF\_SERVICE.

- The Unified CCX Notification Service is disconnected.
- The XMPP presence of “Finesse” user changes to *Unavailable*.

No matter which trigger is detected, the desktop reconnection logic is as follows:

1. Poll SystemInfo for publisher every 20 seconds.
2. If SystemInfo API reports Finesse is IN\_SERVICE, check the Unified CCX Notification Service.
3. If SystemInfo is IN\_SERVICE, check whether the last CTI heartbeat status of the side being connected is a success.




---

**Note** The last CTI heartbeat status is checked to ensure that the subscriber is healthy before failover, and thus does not immediately transition to OUT\_OF\_SERVICE after the client has failed over. Removal of the publisher from the network can cause the Finesse service to disconnect and connect to its local Unified CCX server. Depending on the network topology the subscriber might be slower to sense a network disconnect.

---

4. If XMPP is disconnected, make the Unified CCX Notification Service request.
5. If the Unified CCX Notification Service is successful and Finesse service is IN\_SERVICE, refresh the data.

The failover logic prefers to stay with the publisher. If the failover logic detects that the subscriber is available, it checks the publisher one more time. If the publisher has recovered, the desktop reconnects to the publisher. If the publisher is still down, the desktop connects the agent to the subscriber. In this case, the agent does not automatically reconnect to the failed server after it recovers, but instead remains connected to the subscriber.

If the Unified CCX Notification Service is the source of failure, the desktop makes three attempts to reconnect before changing the state of the desktop to disconnected. These attempts occur before the failover logic begins.

## Desktop Behavior

When the agent is forcibly logged out due to the connection failure between the Finesse desktop and the Finesse service, then Finesse sends a reason code 255 to the Unified CCX server. The Unified CCX server places the agent in Logout state.




---

**Note** Finesse takes up to 120 seconds to detect when an agent closes the browser. If the browser crashes, Finesse waits 60 seconds before sending a forced logout request to the Unified CCX server. Under these conditions, Finesse can take up to 180 seconds to sign out the agent.

---

The following table lists the conditions under which Finesse sends this code to the Unified CCX server.

Scenario	Desktop Behavior	Server Action	Results
The agent closes the browser, the browser crashes, or the agent clicks the Back button on the browser.	Finesse desktop makes a best-effort attempt to notify the server.	Finesse receives a presence notification of <i>Unavailable</i> from the client. Finesse	<b>Race Conditions</b> <ol style="list-style-type: none"> <li>1. The agent closes the browser window. Finesse</li> </ol>

		<p>waits 60 seconds, and then sends a forced logout request to the Unified CCX server.</p>	<p>receives a presence notification of <i>Unavailable</i> for the user. Finesse tries to sign the agent out; however, that agent is already signed out.</p> <ol style="list-style-type: none"><li data-bbox="1271 533 1529 1289">2. If the browser crashes, it can take the Finesse service up to 120 seconds to detect that the client is gone and send a presence notification to Finesse. A situation can occur where the client signs into the subscriber before the publisher receives the presence notification caused by the browser crash. In this case, the agent may be signed out or put into Not Ready state on the subscriber.</li><li data-bbox="1271 1314 1529 1852">3. If the Finesse desktop is running over a slower network connection, Finesse may not always receive an <i>Unavailable</i> presence notification from the client browser. In this situation, the behavior mimics a browser crash, as described in the preceding condition.</li></ol>
--	--	--	---

			4. The agent is logged out, with reason code Connection Failure, which can be seen in the reports.
The client refreshes the browser	—	Finesse receives a presence notification of <i>Unavailable</i> from the client. Finesse waits 60 seconds before sending a forced logout request to the Unified CCX server to allow the browser to reconnect after the refresh.	—
The Refresh Token has expired. For more information on tokens, see <a href="https://developer.cisco.com/docs/finesse/#single-sign-on-apis">https://developer.cisco.com/docs/finesse/#single-sign-on-apis</a> .	Finesse desktop sends a forced logout request to the Unified CCX server.	The Finesse service forwards the forced logout request to the Unified CCX server.	The session expiry warning appears 10 minutes and 5 minutes before the Refresh Token expires. In the last minute, a countdown timer appears till the Refresh Token expires. The agent is forcefully logged out when the timer reaches zero and must log in again.

### Desktop Chat Failover

The following table lists the desktop chat failover scenarios:

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

## Finesse IP Phone Agent Failover

Finesse IPPA failover can occur for the following reasons:

- The Finesse REST API Service transitions to OUT\_OF\_SERVICE.
- The Unified CCX Notification Service transitions to OUT\_OF\_SERVICE.
- The Finesse connection to the Unified CCX server transitions to OUT\_OF\_SERVICE.
- If Finesse IPPA detects a server failure before Finesse fails over to the subscriber, then Finesse IPPA declares the Finesse service OUT\_OF\_SERVICE.

The server that an agent is connected transitions to OUT\_OF\_SERVICE, the Finesse IP Phone Agent (IPPA) displays a notification that the server is unavailable. Finesse IPPA continues to check whether the current Finesse service recovers its state and notifies the agent if it reconnects.

Finesse IPPA attempts to reconnect to the server every 5 seconds and declares it OUT\_OF\_SERVICE after three failed attempts. The total time required for the transition to OUT\_OF\_SERVICE is approximately 15 seconds.

Unlike the Finesse desktop, Finesse IPPA does not check whether the subscriber is available. To connect to subscriber, the agent must exit the publisher, and manually sign into the subscriber.

Finesse IPPA failover logic has the following two triggers to detect failure:

- Finesse IPPA receives a SystemInfo event that the publisher is OUT\_OF\_SERVICE.  
Finesse IPPA polls SystemInfo every 5 seconds to check whether the Finesse service is IN\_SERVICE. After three attempts, if the Finesse service is not IN\_SERVICE, Finesse IPPA displays a server unavailable message to the agent.
- Finesse IPPA receives notification that the Unified CCX Notification Service is disconnected.  
Finesse IPPA tries every 5 seconds to reconnect with the XMPP server. After three attempts, if the Unified CCX Notification Service cannot be reestablished, Finesse IPPA displays a server unavailable message to the agent.

While the agent is still signed into the current service, Finesse IPPA continues attempting to reestablish the connections with the Finesse and XMPP servers. If they both resume service, Finesse IPPA displays the **Sign In** screen and the agent can sign in again and continue as normal.

Alternately, the agent must exit the current Finesse service and try to connect using an alternate Finesse service.

## Guidelines for Optimal Desktop Failover

The following are the guidelines to optimize failover scenarios, to avoid server overload and unnecessary delays.

- [Browser Configuration, on page 114](#)
- [Agent Configuration, on page 115](#)
- [Finesse Configuration, on page 115](#)
- [Common Configuration Safeguards, on page 115](#)




---

**Note** The guidelines for optimal failover ensure that desktop initialization time and general system performance is optimized.

---

### Browser Configuration

Finesse browser failover performance depends on the number of requests made to the Finesse service. Fewer the requests, lesser the system load on the Finesse service. The following browser-specific configurations ensure that the browser does not fetch static resources unnecessarily from the server, and it is a key requirement for faster failover.




---

**Note** Clear the browser cookies before logging in to the Finesse desktop. This avoids unexpected expiry of the Refresh Token in the Single Sign-On mode for Unified CCX.

---

- Avoid loading the Finesse desktop with **bypassServerCache=true&nocache** as a query parameter in the desktop URL. The **bypassServerCache** is to bypass Webproxy cache, and **nocache** is to bypass Shindig cache.
- Host systems must have at least 200 MB of free disk space more than the free space required by the operating system (OS).
- Adequate network bandwidth must be available between the Finesse desktop and the Finesse service. Lower latency results in faster failover.

For more information on bandwidth measurements, see *Cisco Unified Contact Center Express Bandwidth Calculator* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-technical-reference-list.html>.

- Host systems must have adequate memory and CPU without being overloaded at any point in time. A slow host slows the browser enough to cause it to fail and reload resources randomly during failover.
- External gadget hosting servers must prefer CA-signed certificates for easy integration with the browser. If they are self-signed, then import those certificates into the agent browser.

For more information, see *Accept Security Certificates* section in *Cisco Finesse Agent and Supervisor Desktop User Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html>.

### Firefox Configurations

Disable the Race Cache With Network (RCWN) in all the agent desktops to avoid any unwanted requests to the Finesse service. If RCWN is enabled, the Firefox browser by-passes the cached data and fetches the static requests again from the server. Set the **network.http.rcwn.enabled** configuration as **false**.

For more information, see <https://support.mozilla.org/en-US/questions/1267945>.

### Google Chrome, Internet Explorer, and Edge Chromium (Microsoft Edge) Configurations

Import the Finesse self-signed certificates on Google Chrome, Internet Explorer, and Microsoft Edge browsers trust store.

For more information, see the *Accept Security Certificates* section in *Cisco Finesse Agent and Supervisor Desktop User Guide for Cisco Unified Contact Center Express* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html>.

### Agent Configuration

Agents configured must be evenly distributed between the publisher and subscriber. This prevents all agents from failing over when there is an outage that affects only one of the deployed Finesse service.

The number of agents failing over impacts system load and has a linear relationship with the maximum time taken for the operation to complete.

### Finesse Configuration

The number of signed-in users, the gadget types, and the average number of gadgets configured per user, significantly impacts failover load.

The following are the best practices for ensuring a trouble-free failover.

- **Number of Gadgets per Agent**—Gadget-initiated requests constitute the bulk of the requests made during Finesse desktop failover or startup. Configuring fewer gadgets in the desktop layout results in faster desktop failover and startup. The administrator must configure the team or desktop layouts such that only the required gadgets for each team are available in the desktop layout.
- **Type of Gadget**—XML-based gadgets load much faster. The gadget content is also cached at the WebProxy Service, which allows the Finesse service to scale further.
- **Gadget Configuration**—Gadgets developers must follow certain best practices to ensure that gadgets load faster.

For more information, see *Best Practices for Gadget Development* section of *Cisco Finesse Web Services Developer Guide* at <https://developer.cisco.com/docs/finesse/#best-practices-for-gadget-development>.

- **Secondary Resources**—The preloading of server resources reduces latency and improves performance during desktop failover. By default, the **preLoadSecondaryResources** property is enabled. Disabling this property impacts failover time. For more information, see *Desktop Properties*.

### Common Configuration Safeguards

- Import the self-signed certificates into the browser.
- Do not disable browser caching for Finesse desktop.
- Do not clear the cache every time the browser is launched.
- Distribute the agents between the publisher and subscriber.

## Failover Planning

### CTI Failover

CTI failover happens when Finesse service disconnects from the Unified CCX server due to network failure or server error. If the desktop is connected, it displays that the server is unavailable, and tries to reconnect to the available Unified CCX server.

The duration required for Finesse CTI failover depends on the following factors.

- Available bandwidth from the remote Unified CCX to the Finesse service.
- Round Trip Time (RTT) between the Unified CCX server and the Finesse service in case of WAN deployments.
- The number of signed-in users.
- The number of gadgets configured.




---

**Note** The time indicated does not include the Unified CCX server recovering from the failure it encountered. It indicates only the time taken for Finesse to reconnect and be IN\_SERVICE.

---

### Desktop Failover

The Finesse desktop failover happens in all failure scenarios. The Finesse desktop tries to find an active server and fails over to it, once it has located a reachable server which is IN\_SERVICE.

The duration required for Finesse desktop failover depends on the following factors.

- Bandwidth available to the client to reach the Finesse service.
- Time taken for Unified CCX server to become IN-SERVICE.
- RTT between the client and the network gateway.
- The number of signed-in users.
- The number of gadgets configured in the desktop per user.
- Type of gadgets (XML) and the resources it loads. For more information on Finesse gadgets, see <https://developer.cisco.com/docs/finesse/#finesse-gadgets>.

The average time taken for desktop failover, with 400 logged in users, and system defined gadgets per agent, is 35-75 seconds, after an IN-SERVICE Finesse service is identified. If Unified CCX server failover is involved, then the time taken is longer as it includes the time taken for Finesse service failover.

The numbers indicated varies depending on the customer configuration and the above-stated factors. It must be used as a guideline to determine the approximate range for failover time.




---

**Note** • The time indicated does not include the Unified CCX server recovering from the failure it encountered. It only indicates the time taken for Finesse to reconnect and be IN\_SERVICE. Unified CCX server sometimes takes up to 2 minutes to acquire mastership, and become IN\_SERVICE, consequently. This causes delay in Finesse service becoming IN-SERVICE.

For more information on mastership, see <https://www.cisco.com/c/en/us/support/docs/contact-center/unified-contact-center-express/214639-understand-the-algorithm-to-determine-ma.html>.

- During failover, agents are redirected to the subscriber and are signed in automatically, and desktop is reloaded.
-



## Backup and Restore

The Unified CCX backup and restore component also backs up and restores Finesse configurations and data.

For more information about backup and restore, see at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html>

## Additional Language Support

For the list of languages that are supported by Finesse, see the Unified CCX Compatibility related information, located at:

<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html>.

If you want to use the Finesse desktop interface in a language other than English, download and install the language COP file. For more information, see the “COP File” section of the *Cisco Unified Contact Center Express Install and Upgrade Guide*, located at:

<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-installation-guides-list.html>.

## Cisco Finesse Agent and Supervisor Desktop

Cisco Finesse Desktop provides easy access to the applications and information sources from a single customizable cockpit. Providing this unique access to information helps the agents deliver fast and accurate service.

For more information about Cisco Finesse Agent and Supervisor Desktop , see *Cisco Finesse Agent and Supervisor Desktop User Guide for Cisco Unified Contact Center Express* at [https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products\\_user\\_guide\\_list.html](https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_user_guide_list.html).

