



Getting Started

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

- [User Accounts](#) , on page 1
- [Administration Tools](#), on page 1
- [Certificate Management](#), on page 5
- [QoS Settings](#), on page 14
- [Localization](#), on page 14

User Accounts

Credentials for the following user accounts are defined during Cisco Finesse installation:

- **Administrator User account:** Use this account to access the CLI and Cisco Unified Communications Operating System Administration.
- **Application User account:** Use this account to access the Cisco Finesse administration console.

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 that you click to access the various administration features. The tab names and the tasks that you can perform on each tab are as follows:

- **Settings:** Configure CTI server, Administration & Data server, Cluster Settings, , Context Service Management and IP Phone Agent Settings.
- **Call Variables Layout:** Manage the call variables and ECC variables that appear on the agent desktop call control gadget.
- **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.
- **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.



Note Finesse administration tasks can be performed only on the primary Finesse server.

Sign In to Cisco Finesse Administration Console

The Cisco Finesse administration console supports both HTTP and secure HTTP (HTTPS). Whether the administration console uses HTTP or HTTPS depends on whether HTTPS Redirect is enabled (by default, HTTPS Redirect is enabled). The URLs in this procedure use HTTP.

When you sign in to Finesse, always use the fully qualified domain name (FQDN) of the Finesse server in the URL, not the server IP address or hostname.

Procedure

Step 1 Direct your browser to `http://FQDN/cfadmin`, where *FQDN* is the fully qualified domain name of your primary Finesse server.

Note Ensure that the self-signed certificate provided with Finesse uses the hostname of the server as the Common Name for the certificate by default. The hostname in the URL must match the Common Name on the certificate to avoid an address mismatch error.

Step 2 The first time 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 HTTP to access the administration console, this step is not required.

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 the *Cisco Finesse Installation and Upgrade Guide*.

Option	Description
If you use Internet Explorer:	<ol style="list-style-type: none"> A page appears that states this site is untrusted. Click More information > Go on to the webpage.
If you use Edge	<ol style="list-style-type: none"> A page appears that states this site is untrusted. Click Details and click Go on to the webpage.
If you use Firefox:	<ol style="list-style-type: none"> A page appears that states this connection is untrusted. Click I Understand the Risks, and then click Add Exception.

Option	Description
	<p>c. In the Add Security Exception dialog box, ensure the Permanently store this exception check box is checked.</p> <p>d. Click Confirm Security Exception.</p>
If you use Chrome:	<p>a. A page appears that states this connection is not private.</p> <p>b. Click Advanced.</p> <p>c. Click the <code>http://FQDN of Finesse Server/</code> link.</p> <p>d. Enter your agent ID or username, password, and extension, and then click Sign In.</p> <p>The following message appears: Establishing encrypted connection...</p> <p>A dialog box appears that lists the certificates to accept.</p> <p>e. Click OK.</p>

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

Step 4 In the Password field, enter the Application User password that was established 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, Finesse automatically signs you out of the administration console and you must sign in again.

Sign In Using IPv6

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

- For HTTPS access, enter:
`https://<FQDN>:8445/cfadmin`
- For HTTP access, enter:
`http://<FQDN>:8082/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 in a row, Finesse blocks access to that user account for a period up to 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 in a row with the wrong password, Finesse blocks access to that user account. However, in this case, the lockout period is only 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 whether a user account is locked, enter the following CLI command:

```
file get activelog desktop recurs compress
```

Then 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>"
```

CLI

The CLI provides a set of commands applicable to the operating system and to Cisco Finesse. These commands allow basic maintenance and failure recovery, and enable some system administration.

You can access the CLI on the primary Finesse server with a monitor and keyboard at the server console or by Secure Shell (SSH). Use the credentials for the Administrator User account to access the CLI.

Related Topics

[User Accounts](#) , on page 1

Cisco Unified Communications Operating System Administration

Cisco Unified Communications Operating System Administration is a web-based interface used to perform many common system administration functions. The Cisco Unified Communications Operating System Administration menus are as follows:

- **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.



Important You cannot change the IP address of a Finesse server after it is installed.

- **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 Communications Operating System Administration

Procedure

- Step 1** Direct your browser to `https://FQDN:8443/cmplatform`, where *FQDN* is the fully-qualified domain name 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.

Related Topics

[User Accounts](#) , on page 1

Certificate Management

Finesse provides a self-signed certificate that you can use or you can 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, 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 hostname in the certificate, a warning message is displayed in the IE browser about certificate address mismatch. The certificate must be re-generated so that the hostname in the certificate matches the server hostname before importing to Finesse. If there is a valid reason for the mismatch, you can uncheck the **Warn about certificate address mismatch** checkbox from **Tools > Internet Options > Advanced > Security** to allow the certificate to be accepted.
-

Server-Side Certificate Management

By default, Finesse comes with self-signed certificates. If you use these certificates, agents must complete a procedure to accept the certificates the first time they sign in. To simplify the agent experience, you can obtain and upload a CA certificate or produce your own certificate internally.

Obtain and Upload CA Certificate



Note This procedure only applies if you are using HTTPS.

This procedure is optional. If you are using HTTPS, you can choose to obtain and upload a CA certificate or you can choose to 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 Certificate Authority (CA). Use the Certificate Management utility from Cisco Unified Communications Operating System Administration.

To open Cisco Unified Communications Operating System Administration, enter the following URL in your browser:

`https://FQDN of primary Finesse server:8443/cmplatform`

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



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

Procedure

Step 1

Generate a CSR.

- a) Select **Security > Certificate Management > Generate CSR**.
- b) From the **Certificate Name** drop-down list, select **tomcat**.
- c) Click **Generate CSR**.

Note For information on updating Subject Alternate Names (SANs), refer to *Configuration Examples and TechNotes > Unified CCE Solution: Procedure to Obtain and Upload Third-Party CA certificates*.

Note To avoid certificate exception warnings, you must access the servers using the Fully Qualified Domain Name (FQDN).

Do not select "Multi-server (SAN)" as multi-server certificates is not supported with Cisco Finesse.

Step 2

Download the CSR.

- a) Select **Security > Certificate Management > Download CSR**.
- b) From the **Certificate Name** drop-down list, select **tomcat**.
- c) Click **Download CSR**.

Step 3

Generate and download a CSR for the secondary Finesse server.

To open Cisco Unified Operating System Administration for the secondary server, enter the following URL in the address bar of your browser:

<https://FQDN of secondary Finesse server:8443/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 correctly, you must upload the certificates in the order described in the following steps.
- Step 5** When you receive the certificates, select **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, select **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, select **tomcat**.
 - In the **Upload File** field, click **Browse** and browse to the application certificate file.
 - Click **Upload File**.
- Step 9** After the upload is complete, sign out from the Platform Admin page of Finesse.
- Step 10** Access the CLI on the primary Finesse server.
- Step 11** Enter the command **utils service restart Cisco Finesse Notification Service** to restart the Cisco Finesse Notification service.
- Step 12** Enter the command **utils service restart Cisco Finesse Tomcat** to restart the Cisco Finesse Tomcat service.
- Step 13** Upload the application certificate to the secondary Finesse server.
- You do not need to upload the root and intermediate certificates to the secondary Finesse server. After you upload these certificates to the primary server, they are replicated to the secondary server.
- Step 14** Access the CLI on the secondary Finesse server and restart the Cisco Finesse Notification Service and the Cisco Finesse Tomcat Service.
-

Produce Certificate Internally

Set up Microsoft Certificate Server for Windows 2008 R2

This procedure assumes that your deployment includes a Windows Server 2008 R2 (Standard) Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows 2008 R2 (Standard) domain controller.

Procedure

- Step 1** Click **Start**, right-click **Computer**, and select **Manage**.

- Step 2** In the left pane, click **Roles**.
 - Step 3** In the right pane, click **Add Roles**.
The Add Roles Wizard opens.
 - Step 4** On the Select Server Roles screen, check the **Active Directory Certificate Services** check box, and then click **Next**.
 - Step 5** On the Introduction to Active Directory Certificate Services screen, click **Next**.
 - Step 6** On the Select Role Services screen, check the **Certification Authority** check box, and then click **Next**.
 - Step 7** On the Specify Setup Type screen, select **Enterprise**, and then click **Next**.
 - Step 8** On the Specify CA Type screen, select **Root CA**, and then click **Next**.
 - Step 9** Click **Next** on the Set Up Private Key, Configure Cryptography for CA, Configure CA Name, Set Validity Period, and Configure Certificate Database screens to accept the default values.
 - Step 10** On the Confirm Installations Selections screen, verify the information, and then click **Install**.
-

Set up Microsoft Certificate Server for Windows Server

This procedure assumes that your deployment includes a Windows Server Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows Server domain controller.

Before you begin

Before you begin, Microsoft .Net Framework must be installed. See Windows Server documentation for instructions.

Procedure

- Step 1** In Windows, open the **Server Manager**.
- Step 2** In the **Quick Start** window, click **Add Roles and Features**.
- Step 3** In the **Set Installation Type** tab, select **Role-based or feature-based installation**, and then click **Next**.
- Step 4** In the **Server Selection** tab, select the destination server then click **Next**.
- Step 5** In the **Server Roles** tab, check the **Active Directory Certificate Services** box, and then click the **Add Features** button in the pop-up window.
- Step 6** In the **Features** and **AD CS** tabs, click **Next** to accept default values.
- Step 7** In the **Role Services** tab, verify that **Certification Authority** box is checked, and then click **Next**.
- Step 8** In the **Confirmation** tab, click **Install**.
- Step 9** After the installation is complete, click the **Configure Active Directory Certificate Service on the destination server** link.
- Step 10** Verify that the credentials are correct (for the domain Administrator user), and then click **Next**.
- Step 11** In the **Role Services** tab, check the **Certification Authority** box, and then click **Next**.
- Step 12** In the **Setup Type** tab, select **Enterprise CA**, and then click **Next**.
- Step 13** In the **CA Type** tab, select **Root CA**, and then click **Next**.
- Step 14** In the **Private Key**, **Cryptography**, **CA Name**, **Validity Period**, and **Certificate Database** tabs, click **Next** to accept default values.

- Step 15** Review the information in the **Confirmation** tab, and then click **Configure**.
-

Download CA certificate

This procedure assumes that you are using the Windows Certificate Services. Perform the following steps to retrieve the root CA certificate from the certificate authority. After you retrieve the root certificate, each user must install it in the browser used to access Finesse.

Procedure

- Step 1** On the Windows domain controller, run the CLI command `certutil -ca.cert ca_name.cer`, in which `ca_name` is the name of your certificate.
- Step 2** Save the file. Note where you saved the file so you can retrieve it later.
-

Client-Side Certificate Acceptance

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

Client Requirements

For more information on client requirements, see *Compatibility Information* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html>.



- Note** Finesse Desktop client machines should be time synchronized with a reliable NTP server for the correct updates to the Duration fields within Live data reports.
-

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 requirements for configuration.



- Note** To avoid certificate warnings, each user must use the fully-qualified domain name (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 are required 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, go to **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 Browser

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

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

Procedure

- Step 1** In Windows Explorer, double-click the *ca_name.cer* file (in which *ca_name* is the name of your certificate) and then click **Open**.
 - Step 2** Click **Install Certificate > Next > Place all certificates in the following store**.
 - Step 3** Click **Browse** and select **Trusted Root Certification Authorities**.
 - Step 4** Click **OK**.
 - Step 5** Click **Next**.
 - Step 6** Click **Finish**.
- A message appears that states you are about to install a certificate from a certification authority (CA).
- Step 7** Click **Yes**.
- A message appears that states the import was successful.
- Step 8** To verify the certificate was installed, open Internet Explorer. From the browser menu, select **Tools > Internet Options**.
 - Step 9** Click the **Content** tab.
 - Step 10** Click **Certificates**.
 - Step 11** Click the **Trusted Root Certification Authorities** tab.
 - Step 12** Ensure that the new certificate appears in the list.

Step 13 Restart the browser for certificate installation to take effect.

Note If using Internet Explorer 11, you may receive a prompt to accept the certificate even if signed by 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 fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

Procedure

- Step 1** From the Firefox browser menu, select **Options**.
- Step 2** Click **Advanced**.
- Step 3** Click the **Certificates** tab.
- Step 4** Click **View Certificates**.
- Step 5** Click **Authorities**.
- Step 6** Click **Import** and browse to the *ca_name.cer* file (in which *ca_name* is the name of your certificate).
- Step 7** Check the **Validate Identical Certificates** check box.
- Step 8** Restart the browser for certificate installation to take effect.

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 uploaded a CA certificate, you can skip this procedure.

Procedure

- Step 1** In your browser, enter the URL for the administration console (<https://FQDN of the primary Finesse server/cfadmin>) or the agent desktop (<https://FQDN of the primary Finesse server/desktop>).
- Step 2** Perform the steps in the following table for the browser you are using.

Option	Description
If you use Internet Explorer:	<ul style="list-style-type: none"> a. A page appears that states there is a problem with the website's security certificate. Click Continue to this website (not recommended). This action opens the sign in page for the administration console (or agent desktop). A certificate error appears in the address bar of your browser.

Option	Description
	<p>b. Click Certificate Error, and then click View Certificates to open the Certificate dialog box.</p> <p>c. In the Certificate dialog box, click Install Certificate. This action opens the Certificate Import Wizard.</p> <p>Note If you use Internet Explorer 11, you must add Finesse to your trusted sites before the Install Certificate option appears (Internet Options > Security > Trusted Sites > Sites).</p> <p>After you click Install Certificate, under Store Location, select Current User to install the certificate for the current user only, or select Local Machine to install the certificate for all Windows users who use this computer.</p> <p>d. Click Next.</p> <p>e. Select Place all certificates in the following store, and then click Browse.</p> <p>f. Select Trusted Root Certification Authorities, and then click OK.</p> <p>g. Click Next.</p> <p>h. Click Finish.</p> <p>i. If a Security Warning dialog box appears that asks if you want to install the certificate, click Yes.</p> <p>A Certificate Import dialog box that states the import was successful appears.</p> <p>j. Click OK.</p> <p>k. Enter your credentials, and then click Sign In.</p>
If you use Firefox:	<p>a. A page appears that states this connection is untrusted.</p> <p>b. Click I Understand the Risks, and then click Add Exception.</p> <p>c. In the Add Security Exception dialog box, ensure the Permanently store this exception check box is checked.</p> <p>d. Click Confirm Security Exception.</p> <p>The page that states this connection is untrusted automatically closes and the administration console (or agent desktop) loads.</p> <p>e. Enter your credentials, and then click Sign In.</p> <p>f. 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 OK.</p>

Add Certificate for HTTPS Gadget

Add a certificate for a secure HTTP (HTTPS) gadget to allow the gadget to load into 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 that 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 fully qualified domain name) 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 that was entered during installation. To verify that Finesse can resolve the name, run the CLI command “utils network ping <hostname>”.

Procedure

-
- Step 1** Download the tomcat.pem certificate from the third-party gadget host.
- Sign in to Cisco Unified Operating System Administration on the third-party gadget host (<https://FQDN:8443/cmplatform>, where *FQDN* is the fully qualified domain name of the third-party gadget host).
 - Click **Security > Certificate Management**.
 - Click **Find**.
 - Click **tomcat.pem**.
 - Click **Download** and save the file on your desktop.
- Step 2** Upload the certificate to the primary Finesse server.
- Sign in to Cisco Unified Operating System Administration on the primary Finesse server (<http://FQDN:8443/cmplatform>, where *FQDN* is the fully qualified domain name of the Finesse server).
 - Click **Security > Certificate Management**.
 - Click **Upload Certificate**.
 - From the Certificate Name drop-down list, select **tomcat-trust**.
 - Click **Browse** and navigate to the tomcat.pem file that you downloaded in the previous step.
 - Click **Upload File**.
- Step 3** Restart Cisco Finesse Tomcat on the primary Finesse server.
- Step 4** After synchronization is complete, restart Cisco Finesse Tomcat on the secondary Finesse server.
-

QoS Settings

The Cisco Finesse application currently does not support configuration of QoS settings in network traffic. The QoS classification and marking of traffic should be done at the Switch or Router level for signaling traffic to be prioritized, especially if agents are across WAN.

Localization

Cisco Finesse supports localization for the Finesse agent desktop when Finesse is deployed with Unified Contact Center Enterprise (Unified CCE). Use the Cisco Option Package (COP) file installation to install the languages you require for your agents and supervisors.

Finesse is installed with US English. If you do not require other languages for your agents and supervisors, you do not need to install the COP files.



Note You cannot uninstall a language pack after it is installed.

Table 1: Supported Languages for Desktop User Interface

Language	Locale File
Bulgarian	Bg_BG
Catalan	Ca_ES
Czech	Cs_CZ
Croatian	Hr_HR
Danish	da_DK
Dutch	nl_NL
English	en_US
Finnish	fi_FI
French	fr_FR
German	de_DE
Hungarian	Hu_HU
Italian	it_IT
Norwegian	nb_NO
Portuguese	pt_BR
Romanian	Ro_RO

Language	Locale File
Spanish	es_ES
Swedish	sv_SE
Slovak	Sk_SK
Slovenian	Sl_SI
Serbian	Sr_RS
Japanese	ja_JP
Chinese (simplified)	zh_CN
Chinese (traditional)	zh_TW
Korean	ko_KR
Polish	pl_PL
Russian	ru_RU
Turkish	tr_TR

After you install the COP files, agents and supervisors can set the language on their desktops in the following ways:

- Choose a language from the language selector drop-down list on the sign-in page.
- Change their browser preferred language.
- Pass the locale as part of the agent desktop URL (for example, an agent who wants to use French can enter the following URL: http://FQDN/desktop?locale=fr_FR)

The following items are localized on the desktop:

- labels for field names, buttons, and drop-down lists
- prompts
- messages
- tool tips
- page titles
- gadget tab names (Finesse gadgets only)

Configuration data defined using the Finesse administration console (such as Not Ready and Sign Out reason code labels, Wrap-Up reason labels, and phonebook entries) do not depend on the locale chosen for the desktop. For example, if you defined a Not Ready reason code with a Chinese label, the label appears on the desktop in Chinese, regardless of the language the agent chooses when signing in.



Note If you do not install the language COP files (you use English only for the desktop), you can still use Unicode characters for Finesse data such as reason codes, wrap-up reasons, and phonebook entries. For example, if you define a reason code using Chinese characters, it appears in Chinese on an English-only desktop.

Call Context data (WrapUp Reasons, call variables, and ECC variables) is Unicode enabled and independent of the desktop locale.

The following restrictions apply to Call Context data with localized characters.

Variable	Limit
Wrap-Up Reasons	Limited to 40 bytes of UTF-8 data.
Call Variables 1-10	Limited to 40 bytes of UTF-8 data. Note If Finesse sends a set call data request that exceeds 40 bytes of data, the request fails.
ECC Variables	UTF-8 data is limited to the maximum size in bytes for ECC variables specified in Unified CCE.

If any of the limits in this table are exceeded, the variable data is truncated. This is more likely with localized characters that occupy more than one byte in size (for example, characters with an accent require two bytes to store one character and Asian characters require three or four bytes).

Agent first and last names appear on the desktop as they are defined in the Unified CCE database. If the names contain Japanese, Chinese, or Korean characters, they appear correctly on the desktop. However, the maximum supported size for the agent first and last names in these languages is 10 bytes. If the names exceed 10 bytes, they are truncated.

See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* for details about how to set the correct Windows locale and SQL collation settings for Unified CCE.

Finesse does not support the following for localization:

- Finesse administration console
- Tab labels for third-party gadgets deployed in the Finesse gadget container



Note You can define the tab labels for third-party gadgets in the Finesse layout XML file. These labels are hard-coded and are independent of the locale chosen on the desktop. You can only define one label for a tab. You cannot define multiple labels for a tab using different languages.

- Agent usernames and team names that consist of characters other than Latin-1



Note Locale-based searching and sorting may not work as expected.