Getting Started

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

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 to click and access the various administration features. The tab names and the associated tasks are:

- **Settings:** Administration & Data server, Configure CTI server, Cluster Settings, Context Service Management, IP Phone Agent Settings, and Desktop Chat server.
- **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.

Note Finesse administration tasks are 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.

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
Internet Explorer:	**a.** A page appears that states this site is untrusted. **b.** Click **More information** > **Go on to the webpage**.
Firefox:	**a.** A page appears that states this connection is untrusted. **b.** Click **I Understand the Risks**, and then click **Add Exception**.

Option	Description
	c. In the Add Security Exception dialog box, ensure the **Permanently store this exception** check box is checked. **d.** Click **Confirm Security Exception**.
Chrome and Edge Chromium (Microsoft Edge):	**a.** A page appears that states this connection is not private. **b.** In Chrome, click **Advanced** > **Proceed to<Hostname>(unsafe)** **c.** In Microsoft Edge, click **Advanced** > **Continue to<Hostname>(unsafe)**

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, 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, include 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.

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>"
```

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 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.

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.

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 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.

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.

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, obtain and upload a CA certificate or produce your certificate internally.

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://*FQDN of primary Finesse server*:8443/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*.

Note Updating Cisco Finesse tomcat-trust certificate causes a temporary outage due to the impact on Cisco Notification Service. It is recommended to plan the certificate update during a maintenance window.

Procedure

Step 1 Generate a CSR.

a) Click **Security** > **Certificate Management** > **Generate CSR**.

b) From the Certificate Name drop-down list, choose **tomcat** and click **Generate CSR**.

Note To avoid certificate exception warnings, you must access the servers using the FQDN name. Do not select "Multi-server (SAN)" as Multi-Server Subject Alternate Name (SAN) Certificates are not supported with Cisco Finesse.

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.*

Step 2 Download the CSR.

a) Select **Security** > **Certificate Management** > **Download CSR**.

b) 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://*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, 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.

a) From the **Certificate Purpose** drop-down list, select **tomcat-trust**.

b) In the **Upload File** field, click **Browse** and browse to the root certificate file.

c) Click **Upload File**.

Step 7 Upload the intermediate certificate.
a) From the **Certificate Purpose** drop-down list, choose **tomcat-trust**.
b) In the **Upload File** field, click **Browse** and browse to the intermediate certificate file.
c) Click **Upload File**.

Step 8 Upload the application certificate.
a) From the **Certificate Purpose** drop-down list, choose **tomcat**.
b) In the **Upload File** field, click **Browse** and browse to the application certificate file.
c) 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.

The root and the intermediate certificates uploaded to the primary server 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 Server 2012 R2

A prerequisite of this procedure is that your deployment includes a Windows Server 2012 R2 (Standard) Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows Server 2012 R2 (Standard) domain controller.

Before you begin

Microsoft .Net Framework 3.5 Service Pack 1 must be installed. See the Windows Server 2012 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, choose **Role-based or feature-based installation** and click **Next**.

Step 4 In the **Server Selection** tab, choose the destination server and click **Next**.

Step 5 In the **Server Roles** tab, check the **Active Directory Certificate Services** box and click **Add Features** 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 the **Certification Authority** box is checked and 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 the credentials (for the domain Administrator user) and click **Next**.

Step 11 In the **Role Services** tab, check the **Certification Authority** box and click **Next**.

Step 12 In the **Setup Type** tab, choose **Enterprise CA** and click **Next**.

Step 13 In the **CA Type** tab, choose **Root CA** and 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 click **Configure**.

Download CA certificate

A prerequisite of this procedure is 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

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.

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 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

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 and Edge Chromium (Microsoft Edge) Browsers

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 In the Microsoft Edge browser, select **Privacy, search, and services**. Under **Security**, click **Manage Certificates**.

Step 4 Click **Trusted Root Certification Authorities** tab.

Step 5 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 6 Restart the browser for the certificate to install.

Manage Expired CA Certificates

If you receive a certificate expiry alert, it means that the validity of your CA certificate is about to expire. You can delete the certificate after expiry. If you use any CA to sign your certificates, you must upload the new certificates to ensure your system remains operational. Some CA certificates that are shipped with the platform do not require to be uploaded and can be deleted after expiry. For the complete list of CAs that can be safely deleted after expiry, refer to the *Manage Expired CA Certificates* section in the Cisco Unified Contact Center Express Administration and Operations Guide.

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 the primary Finesse server*/cfadmin) or the agent desktop (https://*FQDN of the primary Finesse server*/desktop).

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 an FQDN) as the name with which the certificate is signed. If the certificate name and the name in the gadget URL don't match, the connection isn't trusted, and the gadget doesn't 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 **utils network ping <hostname>** command.

Procedure

Step 1 Download the certificate from the third-party host running a Cisco-provided solution.

a) 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).
b) Click **Security** > **Certificate Management**.
The **Certificate List** page appears.
c) In the **Find Certificate List where** drop-down list, select **Common Name/Common Name SerialNumber** and in the next drop-down list, select **contains**.
d) In the **Select item or enter search text** field, enter hostname or the domain of the host and click **Find**.
All the certificates that have the hostname or the domain of the host that was entered as part of the **Common Name/Common Name SerialNumber** are listed in a tabular format.

Note You can also click **Find** without any search criteria to list all the available certificates. From the list of certificates, identify the required certificates based on the following:

- The **Certificate** column indicates the certificate purpose. The certificates listed as the **tomcat-trust** are used for establishing the webserver(tomcat) identity.
- The **Key Type** column indicates the algorithm used to generate the digital signature that is included in the certificate. For example **RSA**, **EC** (represents ECDSA).
- The **Usage** column indicates the certificate type and if the certificate is used to establish trust or is the host certificate. The term **Identity** indicates that the certificate is used for establishing the webserver(tomcat) identity.

e) Click the hyperlinked **Common Name/Common Name SerialNumber** that you want to download.
The **Certificate Details** pop-up window appears.
f) Click **Download .PEM File** or **Download .DER File** and save the file in the required location.

Step 2 Upload the certificate to the primary Finesse server.
a) 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).
b) Click **Security** > **Certificate Management**.
c) Click **Upload Certificate**.
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 Finesse Tomcat on the primary Finesse server.

Step 4 After synchronization is complete, restart the 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 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 An appropriate language needs to be selected before login on the desktop. If not, English will be the default language. You cannot uninstall a language pack after it is installed.

Table 1: Supported Languages for Desktop User Interface

Language	Locale File	Language	Locale File
Bulgarian	Bg_BG	Portuguese	pt_BR
Catalan	Ca_ES	Romanian	Ro_RO
Czech	Cs_CZ	Spanish	es_ES
Croatian	Hr_HR	Swedish	sv_SE
Danish	da_DK	Slovak	Sk_SK
Dutch	nl_NL	Slovenian	Sl_SI
English	en_US	Serbian	Sr_RS
Finnish	fi_FI	Japanese	ja_JP
French	fr_FR	Chinese (simplified)	zh_CN
German	de_DE	Chinese (traditional)	zh_TW
Hungarian	Hu_HU	Korean	ko_KR
Italian	it_IT	Polish	pl_PL
Norwegian	nb_NO	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 have 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 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.

For details on setting the correct Windows locale and SQL collation settings for Unified CCE, See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.

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.