The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided "as is" with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2010-2015 Cisco Systems, Inc. All rights reserved.
Preface

This document explains the two interfaces that you use to configure and maintain Cisco Finesse. These interfaces are as follows:

- The Administration Console: (URL: http://hostname or IP address/cfadmin) A web-based interface that you use to configure system and team settings for Cisco Finesse
- The Serviceability Console: (CLI) Used to manage the Cisco Finesse services

Access to the Administration Console is limited to system administrators who use the credentials of the Application User account created during the installation.

The Administrator User credentials can be used to access the CLI.

This guide is prepared for system administrators who configure, administer, and monitor Cisco Finesse.

This guide is organized as follows:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Administration Console</td>
<td>Explains the Administration Console, including:</td>
</tr>
<tr>
<td></td>
<td>• Sign In to Cisco Finesse Administration Console</td>
</tr>
<tr>
<td></td>
<td>• Configuring Contact Center Enterprise CTI Server Settings (adding and changing CTI Server settings)</td>
</tr>
<tr>
<td></td>
<td>• Configuring Cluster Settings (adding a secondary Finesse server)</td>
</tr>
<tr>
<td></td>
<td>• Configuring Contact Center Enterprise Administration &amp; Data Server Settings</td>
</tr>
<tr>
<td></td>
<td>• Configuring Not Ready Reason Codes, Sign Out Reason Codes, and Wrap-Up Reasons</td>
</tr>
<tr>
<td></td>
<td>• Defining the Call Variable Layout</td>
</tr>
<tr>
<td></td>
<td>• Managing Phone Books</td>
</tr>
<tr>
<td></td>
<td>• Managing Team Resources</td>
</tr>
<tr>
<td></td>
<td>• Updating the Finesse Layout XML</td>
</tr>
</tbody>
</table>
Cisco Finesse documentation includes user guides and a knowledge base of troubleshooting tips that have been entered by engineers and users.


- **Cisco Finesse Troubleshooting tips** are available at this location: http://docwiki.cisco.com/wiki/Troubleshooting_Cisco_Finesse

- Conventions, page viii
- Documentation and Service Requests, page ix
- Documentation Feedback, page ix

### Conventions

This manual uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **boldface** font | Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example:  
  - Choose **Edit > Find**.  
  - Click **Finish**. |
Convention | Description
---|---
italic font | Italic font is used to indicate the following:
| • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills.
| • For emphasis. Example: *Do not* use the numerical naming convention.
| • A syntax value that the user must replace. Example: IF (*condition*, *true-value*, *false-value*)
| • A book title. Example: See the *Cisco CRS Installation Guide*.

window font | Window font, such as Courier, is used for the following:
| • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems, Inc.</title></html>`

< > | Angle brackets are used to indicate the following:
| • For arguments where the context does not allow italic, such as ASCII output.
| • A character string that the user enters but that does not appear on the window such as a password.

---

**Documentation and Service Requests**

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

**Documentation Feedback**

You can provide comments about this document by sending email to the following address:

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.
The Administration Console

The Administration Console is the interface used to configure system settings in Cisco Finesse. An administrator must sign in to this tool and configure these settings after installing Cisco Finesse. Agents cannot sign in to the Finesse Agent Desktop until this configuration is complete.

After system configurations are defined and the Cisco Finesse services are restarted, the Cisco Finesse Agent Desktop is enabled. Agents who have a password configured in Cisco Unified Contact Center Enterprise (Unified CCE) and a phone device defined in Cisco Unified Communications Manager (Unified CM) can sign in.

Password is an optional field when you create an agent in Unified CCE Configuration Manager, but it is mandatory for Cisco Finesse. Agents who do not have passwords cannot sign in to Cisco Finesse.

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

- HTTPS Support, page 2
- Sign In to Cisco Finesse Administration Console, page 2
- Contact Center Enterprise CTI Server Settings, page 4
- Contact Center Enterprise Administration & Data Server Settings, page 5
- Cluster Settings, page 7
- Not Ready Reason Codes, page 7
- Sign Out Reason Codes, page 12
- Wrap-Up Reasons, page 16
- Call Variable Layout, page 20
- Phone Books, page 22
- Team Resources, page 30
- Finesse Layout XML, page 34
HTTPS Support

Cisco Finesse supports both HTTP and secure HTTP (HTTPS). Administrators can access the Administration Console using HTTP or HTTPS.

To access the Administration Console using HTTP, enter the following URL in the address bar of your browser (where hostname is the hostname of your primary Finesse server):

http://hostname/cfadmin

To access the Administration Console using HTTPS, enter the following URL in the address bar of your browser (where hostname is the hostname of your primary Finesse server):

https://hostname/cfadmin

Administrators can run the Cisco Finesse HTTPS Redirect CLI command to enforce HTTPS access for both the Administration Console and the Cisco Finesse Agent Desktop. For more information, see Cisco Finesse HTTPS Redirect, on page 39.

Note

This guide uses HTTP for all example URLs.

Sign In to Cisco Finesse Administration Console

Note

The Cisco Finesse administration console supports both Internet Explorer and Firefox.

The 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 uses HTTP.

Procedure

Step 1

Direct your browser to http://FQDN, hostname, or IP address of Finesse server//cfadmin, where FQDN, hostname, or IP address of Finesse server/ is the fully-qualified domain name (FQDN), hostname, or IP address 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 Installation and Getting Started Guide for Cisco Finesse.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| If you use Internet Explorer:      | 1 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. A certificate error appears in the address bar of your browser.  

2 Click **Certificate Error**, and then click **View Certificates** to open the Certificate dialog box.  

3 On the Certificate dialog box, click **Install Certificate**. This action opens the Certificate Import Wizard.  

4 Click **Next**.  

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

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

7 Click **Next**.  

8 Click **Finish**.  

9 If a Security Warning dialog box appears that asks if you want to install the certificate, click **Yes**.  

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

10 Click **OK**. |
| If you use Firefox:                | 1 A page appears that states this connection is untrusted.  

2 Click **I Understand the Risks**, and then click **Add Exception**.  

3 On the Add Security Exception dialog box, ensure the **Permanently store this exception** check box is checked.  

4 Click **Confirm Security Exception**. |

**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.
Contact Center Enterprise CTI Server Settings

Use the Contact Center Enterprise CTI Server Settings gadget to configure the A Side and B Side CTI servers.

All fields on this tab are populated with default system values or with values an administrator has previously entered. Change values to reflect your environment and preferences.

After changing and saving any value on the Contact Center Enterprise CTI Server Settings gadget, you must restart the Cisco Tomcat Service on both the primary and secondary Finesse servers, as described in Supported Commands. Note that if you restart the Cisco Tomcat Service, agents must sign out and sign in again.

If you must make changes to other settings (such as Contact Center Enterprise Administration & Data Server settings), you can make those changes and then restart Cisco Tomcat.

As a best practice, make changes to CTI server settings and restart the Cisco Tomcat Service during hours when agents are not signed in to the Cisco Finesse Agent Desktop.

The following table describes the fields on the Contact Center Enterprise CTI Server Settings gadget.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Side Host/IP Address</td>
<td>Either the hostname or IP address of the A Side CTI server. This field is required. This value is typically the IP address of the Peripheral Gateway (PG). The CTI server runs on the PG.</td>
</tr>
<tr>
<td>A Side Port</td>
<td>The port of the A Side CTI server. The value of this field must match the port configured during the setup of the A Side CTI server. This field is required and accepts values between 1 and 65535. You can find this value using the Unified CCE Diagnostic Framework Portico tool on the PG box. For more information about Diagnostic Framework Portico, see the Serviceability Best Practices Guide for Cisco Unified ICM, Unified CCE &amp; Unified CCH. The default value is 42027.</td>
</tr>
</tbody>
</table>
The ID of the Agent PG Routing Client (PIM).
The Agent PG Peripheral ID should be configured to the same value for the A Side and B Side CTI server.
This field is required and accepts values between 1 and 32767.
The default value is 5000.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peripheral ID</td>
<td>The ID of the Agent PG Routing Client (PIM). The Agent PG Peripheral ID should be configured to the same value for the A Side and B Side CTI server. This field is required and accepts values between 1 and 32767. The default value is 5000.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B Side Host/IP Address</th>
<th>Either the hostname or IP address of the B Side CTI server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>B Side Port</td>
<td>The port of the B Side CTI server. The value of this field must match the port configured during the setup of the B Side CTI server. This field accepts values between 1 and 65535.</td>
</tr>
</tbody>
</table>

**Actions on the Contact Center Enterprise CTI Server Settings gadget:**

- **Save:** Saves your configuration changes

  ![Save](image)

  After you change and save any value on this page, you must restart the Cisco Tomcat Service on the primary and secondary Finesse server, as described in Supported Commands. Note that if you restart the Cisco Tomcat Service, agents must sign out and sign in again.

- **Revert:** Retrieves the most recently saved server settings

  ![Revert](image)

---

**Contact Center Enterprise Administration & Data Server Settings**

Use the Contact Center Enterprise Administration & Data Server Settings gadget to configure the database settings. These settings are required to enable authentication for Finesse agents and supervisors.

![Note](image)

Finesse does not support SQL authentication for connecting to the Unified CCE administration database. Finesse requires that the administration database is configured to use Windows authentication.

After you change and save any value on the Contact Center Enterprise Administration & Data Server Settings gadget, you must restart the Cisco Tomcat Service on the primary and secondary Finesse server, as described in Supported Commands. Note that if you restart the Cisco Tomcat Service, agents must sign out and sign in again.

As a best practice, make Contact Center Enterprise Administration & Data Server settings changes and restart the Cisco Tomcat service during hours when agents are not signed in to the Cisco Finesse Agent Desktop.
The following table describes the fields on the Contact Center Enterprise Administration & Data Server Settings gadget.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Host/IP Address</td>
<td>Either the hostname or IP address of the Unified CCE Administration &amp; Data Server.</td>
</tr>
<tr>
<td>Backup Host/IP Address</td>
<td>Either the hostname or IP address of the backup Unified CCE Administration &amp; Data Server.</td>
</tr>
<tr>
<td>Database Port</td>
<td>The port of the Unified CCE Administration &amp; Data Server. The default value is 1433.</td>
</tr>
<tr>
<td>AW Database Name</td>
<td>The name of the AW Database (AWDB) (for example, ucceinstance_awdb).</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain of the AWDB.</td>
</tr>
<tr>
<td>Username</td>
<td>The username required to sign in to the AWDB.</td>
</tr>
<tr>
<td>Password</td>
<td>The password required to sign in to the AWDB.</td>
</tr>
</tbody>
</table>

**Note** Because Finesse expects the primary and backup Administration & Data Server ports to be the same, the Finesse Administration Console exposes only one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers.

For more information about these settings, see the Administration Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted and the Staging Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted.

**Actions on the Contact Center Enterprise Administration & Data Server Settings gadget:**

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

When you update any of the following fields and click Save, Finesse attempts to connect to the AWDB:

- Primary Host/IP Address
- Backup Host/IP Address
- Database Port
Cluster Settings

Use the Cluster Settings gadget to configure a secondary Finesse server. The purpose of a secondary Finesse server is to handle all agent requests if the primary server goes down.

You must complete this configuration before you install the secondary Finesse server. For more information about installing a secondary Finesse server, see the Installation and Getting Started Guide for Cisco Finesse.

The following table describes the fields on the Cluster Settings gadget.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host/IP Address</td>
<td>Either the hostname or IP address of the secondary Finesse server.</td>
</tr>
</tbody>
</table>

Actions on the Cluster Settings gadget:

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

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. 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. 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 maximum of 100 global and 100 team Not Ready reason codes.
The following table describes the fields on the Manage Reason Codes (Not Ready) gadget.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason Label</td>
<td>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. Both alphanumeric and special characters are supported. <strong>Note</strong> The Not Ready Reason Code Management gadget allows you to create multiple reason codes using the same label with a different code. However, if a label is not unique, multiple entries with the same label may appear on the Agent Desktop and agents may select the incorrect code.</td>
</tr>
<tr>
<td>Reason Code</td>
<td>A code for the Not Ready reason. The code can be any value between 1 and 65535. The combination of Reason Label and Reason Code must be unique. <strong>Note</strong> The Not Ready Reason Code Management gadget allows you to create multiple reason codes using the same code with a different label. However, if a code is not unique, the Agent Desktop may not always show the correct label.</td>
</tr>
<tr>
<td>Global?</td>
<td>Yes/No. Indicates if the reason code is available globally to all agents (Yes) or to specific teams of agents (No).</td>
</tr>
</tbody>
</table>

**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 Agent or Supervisor 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 configured codes drop-down list as shown in the following figure.

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.

If the agent also applies a Not Ready reason code, the desktop shows the pending state with the reason code (in this case, Not Ready - Lunch).

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).

**Add Not Ready Reason Code**

Perform the following procedure to add a new Not Ready reason code.

**Procedure**

1. **Step 1** In the Manage Reason Codes (Not Ready) gadget, click **New**.
   The New Reason Code area appears.
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, enter a reason code.

Note The code must be between 1 and 65535 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**

Perform the following procedure to edit the label or code for an existing 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.
The Edit Reason Code area appears.
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.

Perform the following procedure to delete a Not Ready reason code.

**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.

A question appears asking you to confirm that you want to delete the selected reason code.
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 Agent 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 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 a maximum of 100 global and 100 team Sign Out reason codes.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason Label</td>
<td>The label for the Sign Out reason code.</td>
</tr>
</tbody>
</table>
The label has a maximum length of 40 characters and should be unique for each Sign Out reason code. Both alphanumeric and special characters are supported.

**Note**  The Sign Out Reason Code Management gadget does allow you to create multiple reason codes using the same label with a different code. However, if a label is not unique, multiple entries with the same label may appear on the Agent Desktop and agents may select the incorrect code.

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>A code for the Sign Out reason. The code can be any value between 1 and 65535. The combination of Reason Label and Reason Code must be unique.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>The Manage Reason Codes (Sign Out) gadget does allow you to create multiple reason codes using the same code with a different label. However, if a code is not unique, the Agent Desktop may not always show the correct label.</td>
</tr>
</tbody>
</table>

| 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 Agent or Supervisor 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 clicks Sign Out on the desktop, any configured Sign Out codes appear in a drop-down list. The agent can then choose the code that represents why that agent is signing out.

**Add Sign Out Reason Code**

Perform the following procedure to add a new Sign Out reason code.

**Procedure**

**Step 1**  In the Manager Reason Codes (Sign Out) gadget, click **New**. The New Reason Code area appears.
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, enter a reason code.

Note The code must be between 1 and 65535 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**

Perform the following procedure to edit the label or code for an existing 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.

The Edit Reason Code area appears.
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.

Perform the following procedure to delete a Sign Out reason code.

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.
A question appears asking you to confirm that you want to delete the selected reason code.
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. Click the Global header to sort the Wrap-Up reasons by whether they are global (Yes) or not (No).

Note

Finesse supports a maximum of 100 global and 100 team Wrap-Up reasons.

Finesse supports wrap-up functionality only for incoming calls and Outbound Option Dialer Calls (Finesse does not support Outbound Option Direct Preview mode). Finesse does not support wrap-up for outgoing calls placed by agents.

To enable wrap-up, you must configure both of the following attributes in the Unified CCE Agent Desk Settings:

For more information about configuring Agent Desktop Settings, see the Configuration Manager Online Help for Unified CCE.

Note

If an agent is configured for wrap-up and selects a pending state during a call, when the call finishes that agent goes into wrap-up and not the pending state selected during the call. The agent can end wrap-up by either selecting a new state (Ready or Not Ready) or letting the wrap-up timer expire. If the agent selects a new state, the new state overrides the pending state selected during the call. If the wrap-up timer expires, the agent transitions to the pending state.
The following table describes the fields on the Manage Wrap-Up Reasons gadget.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason Label</td>
<td>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.</td>
</tr>
<tr>
<td>Global?</td>
<td>Yes/No. Indicates if the Wrap-Up reason is available globally to all agents (Yes) or to specific teams of agents (No).</td>
</tr>
</tbody>
</table>

**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 back in to see those changes reflected on their desktops.
Add Wrap-Up Reason

Cisco Finesse does not support the use of extended ASCII characters required for additional alphabets in the Wrap-Up reasons. You must use only ASCII characters in the 0-127 range. For example, if you add a Wrap-Up reason that contains the character à (ASCII 133), it does not appear correctly on the agent desktop.

Perform the following procedure to add a new Wrap-Up reason.

Procedure

Step 1 In the Manage Wrap-Up Reasons gadget, click New.
   The New Wrap-Up Reason area appears.

Step 2 In the Reason Label field, add a label for the Wrap-Up reason.
   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.
   By default, the Global? check box is selected.

Step 4 Click Save.

Edit Wrap-Up Reason

Perform the following procedure to edit an existing 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

Perform the following procedure to delete a 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.

Call Variable Layout

Use the Manage Call Variables Layout gadget on the Call Variables Layout tab of the Administration Console to define the way call variables appear on the Finesse Agent Desktop.

The Finesse Agent Desktop 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 following table describes the fields on the Manage Call Variables Layout gadget.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>A label that describes the variable for that entry (for example, Customer Name). The maximum length of this field is 50 characters.</td>
</tr>
</tbody>
</table>
The name of the call variable or ECC variable that is displayed to the agent. The maximum length of this field is 32 characters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>The name of the call variable or ECC variable that is displayed to the agent. The maximum length of this field is 32 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete?</td>
<td>Click the “X” to delete the specified row from the column.</td>
</tr>
</tbody>
</table>

**Actions on the Manage Call Variables Layout gadget:**

- **Add Row:** Adds a new row to the specified column
- **Note:** The Add Row button is disabled if 10 variables are already configured for the specified column.

- **Save:** Saves your configuration changes
- **Revert:** Retrieves and reapplies the most recently saved call variable layout

**Note**

When you modify the call variable layout of the Agent Desktop, the changes you make take effect 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.

## Configure Call Variables Layout

**Note**

Cisco Finesse does not support the use of extended ASCII characters required for additional alphabets in the call variables 1-10. You must use only ASCII characters in the 0-127 range. For example, if you set call variable 2 to contain the character à (ASCII 133), it does not appear correctly on the agent desktop.

### Procedure

**Step 1**

In the Call Header Layout area, in the Display Name field, enter the text that you want to appear in the header of the Call Control gadget on the Finesse desktop (for example, Customer Name).

**Step 2**

From the Variable drop-down list, choose the call variable or Outbound Option ECC variable that you want to appear in the header (for example, callVariable3).

**Step 3**

In the Call Body Left-Hand Layout and Call Body Right-Hand Layout areas:

a) Click the X beside any row that you want to delete.

b) Click Add Row if you want to add a new row.

c) For each row, in the Display Name field, enter the text that you want to appear on the desktop, and then choose the corresponding call variable or Outbound Option ECC variable from the Variable drop-down list.

**Step 4**

Click Submit.

**Step 5**

Click Save.
Add ECC Variables to Call Variables Layout

Note
Cisco Finesse does not support the use of extended ASCII characters required for additional alphabets in the ECC variables. You must use only ASCII characters in the 0-127 range. For example, if you add an ECC variable that contains the character à (ASCII 133), it does not appear correctly on the agent desktop.

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.
The Custom/ECC Variable Entry area appears.

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.

Phone Books

The Manage Phone Books gadget enables an administrator to 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.

Finesse can support the following number of phone books and phone book contacts:

- 10 global phone books, each with a maximum of 1,500 contacts
- 50 team phone books, each with a maximum of 1,500 contacts
- The system can support a combined total of 1,500 contacts for all types of phone books

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the phone book. The name can be a maximum length of 64 alphanumeric characters and must be unique. The following characters are not supported: &amp; &lt; &gt; &quot; \ /</td>
</tr>
<tr>
<td>Assign To</td>
<td>Indicates if the phone book is global (All Users) or team (Teams).</td>
</tr>
<tr>
<td>Last Name</td>
<td>The last name of a contact. The last name can be a maximum length of 128 characters. This field is optional.</td>
</tr>
<tr>
<td>First Name</td>
<td>The first name of a contact. The first name can be a maximum length of 128 characters. This field is optional.</td>
</tr>
<tr>
<td>Number</td>
<td>The phone number for the contact. The phone number can be 1-32 characters long and cannot be blank.</td>
</tr>
<tr>
<td>Note</td>
<td>Optional text that describes the contact. The note can be a maximum length of 128 characters.</td>
</tr>
</tbody>
</table>

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**. The Manage Phone Books area appears.

**Step 2** In the Name box, enter a name for the phone book. **Note** Phone book names can be a maximum length of 64 characters.

**Step 3** In the Assign To box drop-down list, 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**. The Edit Phone Books area appears.
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 field drop-down list, choose All Users or Teams.

Step 4  Click Save.
If you change the Assign To field from Teams to All Users, a message appears that asks you to confirm the change. Click Yes to confirm.

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.
A question appears asking you to confirm that you want to delete 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 1500 contacts. Import lists that contain more than 1500 contacts are rejected with an error message.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Max Length</th>
<th>Can Be Blank</th>
<th>Permitted Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>128</td>
<td>Yes</td>
<td>Alphanumeric characters</td>
</tr>
<tr>
<td>Last Name</td>
<td>128</td>
<td>Yes</td>
<td>The following characters are not supported: &amp; &lt; &gt; &quot; \ /</td>
</tr>
<tr>
<td>Phone Number</td>
<td>32</td>
<td>No</td>
<td>Note: The CSV file that contains the contacts to import must use either Latin or UTF-8 encoding.</td>
</tr>
<tr>
<td>Notes</td>
<td>128</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

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, as in the preceding example, to ensure that any commas or double quotes that are part of the actual fielded 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**. The Import Contacts area appears.

**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 or Unicode-8 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**.
A message is displayed asking if you want to open or save the file.

Note The default name for an export file is PhoneBookContacts.csv.

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, as desired.

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.

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. The New Contact area appears.
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. The Edit Contact area appears.
Step 4 Edit the fields that you want to change. 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 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.

A question appears asking you to confirm that you want to delete the selected contact.

Step 4 Click Yes to confirm the deletion of the selected contact.

Team Resources

Use the Manage Team Resources gadget to assign and unassign phone books, reasons, and custom desktop layouts to teams. Click the Name or ID header to sort the teams in ascending or descending order.
There are five tabs in the gadget, each enabling you to assign/unassign resources to a team. The tabs are defined in the following table.

<table>
<thead>
<tr>
<th>Tab Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Layout</td>
<td>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.</td>
</tr>
<tr>
<td>Phone Books</td>
<td>Use this tab to assign/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.</td>
</tr>
<tr>
<td>Reason Codes (Not Ready)</td>
<td>Use this tab to assign/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.</td>
</tr>
<tr>
<td>Reason Codes (Sign Out)</td>
<td>Use this tab to assign/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.</td>
</tr>
<tr>
<td>Wrap-Up Reasons</td>
<td>Use this tab to assign/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.</td>
</tr>
</tbody>
</table>

**Actions on the Manage Team Resources gadget:**

- **Add**: Assign a phone book or reason to the team.
Assign Phone Books and Reasons to Team

Procedure

Step 1 In the Manage Team Resources gadget, select a team. Tabs for each available resource appear.

Step 2 Click the tab for the resource you want to assign for the selected team. The List of <resource> area appears.

Step 3 Click Add. The Add <resource> popup appears.

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 have finished 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.

---

**Assign Custom Desktop Layout to Team**

Perform the following procedure to create and assign a custom desktop layout to a team.

**Procedure**

**Step 1** In the Manage Team Resources gadget, select a team. Tabs for each available resource appear.

**Step 2** Click the Desktop Layout tab. 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** Edit the XML as desired.

**Step 5** 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 go into 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.

---

**Unassign Phone Books and Reasons from Team**

**Procedure**

**Step 1** In the Manage Team Resources gadget, select a team. Tabs for each available resource appear.

**Step 2** Click the tab for the resource you want to unassign from the selected team.
The List of `<resource>` area appears.

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

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

---

**Finesse Layout XML**

The Finesse Layout XML defines the layout of the Finesse Desktop, including the tab names and the gadgets that appear on each tab. Tab names can appear in any language, as long as they are HTML escaped in the XML.

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

---

**Update Default Layout of Finesse Desktop**

**Note**

When you modify the layout of the Agent Desktop, the changes you make take effect on the Agent or Supervisor Desktop after 10 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.

**Procedure**

**Step 1** In the Finesse Layout XML area, enter the new layout XML file.

**Step 2** Click **Save**. Finesse validates the XML file to ensure that it is valid XML syntax and conforms to the Finesse schema.
The following is an example of a layout XML file.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<finesseLayout xmlns="http://www.cisco.com/vtg/finesse">
  <layout>
    <role>Agent</role>
    <page>
      <gadget>http://localhost/desktop/gadgets/CallControl.jsp</gadget>
    </page>
  </layout>
  <tabs>
    <tab>
      <id>home</id>
      <label>Home</label>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>Manage Call</label>
    </tab>
  </tabs>
</layout>

<layout>
  <role>Supervisor</role>
  <page>
    <gadget>http://localhost/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>Home</label>
      <gadgets>
        <gadget>http://localhost/desktop/gadgets/TeamPerformance.xml</gadget>
      </gadgets>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>Manage Call</label>
    </tab>
  </tabs>
</layout>
</finesseLayout>
```

You must ensure the XML you upload conforms to the XML schema definition for Finesse. For information about the schema definition, see XML Schema Definition.
Update Default Layout of Finesse Desktop
Serviceability

- Cisco Finesse Service Access, page 37
- CLI Access, page 37

Cisco Finesse Service Access

You can access the following Finesse services from the CLI:

- **Cisco Finesse Notification Service**: This service is used for messaging and events. If this service is not started, you cannot view call events, agent state changes, or statistics, and the Finesse Desktop will not load after sign-in.

- **Cisco Tomcat Service**: This service contains all deployed Finesse applications. A restart of the Cisco Tomcat Service requires that all agents sign out and sign back in.

The deployed applications in the Cisco Tomcat Service include:

- **Finesse Desktop application**: This application provides the user interface for agents and supervisors.

- **Finesse Rest API application**: This application provides integration with the Cisco CTI Server for the Finesse Desktop application. It also provides a programming interface that can be used by third-party applications that are written to use the Finesse REST API.

- **Finesse Administration application**: This application provides the administrative operations for Finesse.

- **Finesse Admin Rest API application**: This application provides integration with the Cisco CTI Server for the Finesse Administration application. It also provides a programming interface that can be used by third-party applications that are written to use the Finesse REST API.

CLI Access

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 also enable some system administration. Although Finesse provides access to all Cisco Unified Communications Manager CLIs, many commands are not applicable to Finesse and most have not been validated for Finesse.
You can access the CLI directly, using the monitor and keyboard at the server console or by using SSH:

1. Enter the ID for the Administrator User account (the one created during installation).
2. When prompted, enter the password for the administrator user.

## Supported Commands

Finesse supports the following CLI commands and has qualified their use.

### Log Collection

These commands prompt you to specify a secure FTP (SFTP) server location to which the files will be uploaded.

To obtain logs:

- **Install log**: `file get install desktop-install.log`
  
  Use this command to see the installation log after the system is installed.
  
  This log is written to the SFTP server and stored as a text file written to this path: `<IP Address>\<date time stamp>\install\desktop-install.log`

- **Desktop logs**: `file get activelog desktop recurs compress`
  
  Use this command to obtain logs for the Finesse web applications. This command uploads a zip file that contains the following directories:

  - **webservices**: This directory contains the logs for the Finesse backend that serves the Finesse REST APIs. The maximum size of an uncompressed desktop log file is 100 MB. This directory holds a maximum of 300 log files. After a log file reaches 100 MB, that file is compressed and a new log file is generated. Output to the last compressed desktop log file wraps to the log file created next. The log file wrap-up duration can vary, based on the number of users on the system. Timestamps are placed in the file name of each desktop log.

  - **desktop**: This directory contains logs from the Finesse agent desktop gadget container that holds the Finesse desktop gadgets. Any container-level errors with Finesse agent desktop will appear in these log files.

  - **admin**: This directory contains logs from the Finesse administration gadget container that holds the administration gadgets. Any container-level errors with the Finesse administration console appear in these log files.

  - **clientlogs**: This directory contains the client-side logs submitted from the Finesse agent desktop to the Finesse server. Each log file is no larger than 1.5 MB and contains a timestamp and the agent ID of the agent who submitted the file. A new log file is created each time an agent submits client-side logs (the data is not appended to an existing log file). The maximum size of this directory is 100 MB. When the directory reaches 100 MB, the oldest files are deleted to keep the size below 100 MB.

  - **openfireservice**: This directory contains startup and shutdown-related information logs for the Cisco Finesse Notification Service.

  - **openfire**: This directory contains limited error and information logs for the Cisco Finesse Notification Service.
These logs are stored to the following path on the SFTP server: `<IP address>\<date time stamp>\active_nnn.tgz`, where nnn is timestamp in long format.

- Servm log: `file get activelog platform/log/servm*.* compress`
  Use this command to obtain logs generated by the platform service manager that manages the starting and stopping of the Finesse services.

The desktop and servm logs are compressed to one set of files.

These logs are stored to the following path on the SFTP server: `<IP address>\<date time stamp>\active_nnn.tgz`, where nnn is timestamp in long format.

- Platform Tomcat logs: `file get activelog tomcat/logs recurs compress`
  These logs are stored to the following path on the SFTP server: `<IP address>\<date time stamp>\active_nnn.tgz`, where nnn is timestamp in long format.

- VOS install log: `file get install install.log`
  These logs are stored to the following path on the SFTP server: `<IP address>\<date time stamp>\active_nnn.tgz`, where nnn is timestamp in long format.

**Note** Log collection may fail when you use the compress flag if there are a lot of log files. If collection fails, run the command again without the compress flag.

### Cisco Security Agent

Run the following command to disable Cisco Security Agent (CSA) (mandatory): `utils csa disable`

You must run this command after installation is complete to disable Cisco Security Agent. CSA prevents some Finesse operations.

### Cisco Finesse HTTPS Redirect

Enable Cisco Finesse HTTPS Redirect to enforce HTTPS to access the Finesse desktop and administration console. If Cisco Finesse HTTPS Redirect is enabled, agents and supervisors who attempt to access the desktop with HTTP are redirected to HTTPS. Administrators who attempt to access the administration console with HTTP are also redirected to HTTPS.

If Cisco Finesse HTTPS Redirect is disabled, the desktop and the administration console can be accessed with HTTP or HTTPS.

**Note** This command does not impact the Finesse REST APIs.

To view the status of, enable, or disable Cisco Finesse HTTPS Redirect:

- To retrieve the status of Cisco Finesse HTTPS Redirect: `utils finesse application_https_redirect status`
  This command displays whether Cisco Finesse HTTPS Redirect is currently enabled or disabled on the system.

- To enable Cisco Finesse HTTPS Redirect: `utils finesse application_https_redirect enable`
You must stop the Cisco Tomcat Service before you can enable Cisco Finesse HTTPS Redirect. You can use the following command to stop this service: `utils service stop Cisco Tomcat`.

If the Cisco Tomcat Service is not stopped, the command to enable Cisco Finesse HTTPS Redirect fails. This command also fails if Cisco Finesse HTTPS Redirect is already enabled. After you enable Cisco Finesse HTTPS Redirect, start the Cisco Tomcat Service using the command `utils service start Cisco Tomcat`.

To disable Cisco Finesse HTTPS Redirect: `utils finesse application_https_redirect disable`

You must stop the Cisco Tomcat Service before you can disable Cisco Finesse HTTPS Redirect. You can use the following command to stop this service: `utils service stop Cisco Tomcat`.

If the Cisco Tomcat Service is not stopped, the command to disable Cisco Finesse HTTPS Redirect fails. This command also fails if Cisco Finesse HTTPS Redirect is already disabled. After you disable Cisco Finesse HTTPS Redirect, start the Cisco Tomcat Service using the command `utils service start Cisco Tomcat`.

---

**Finesse Services**

To view, start, or stop services:

- To retrieve the status of services: `utils service list`
  This command retrieves a list of all services and their status. Services are shown in one of the following states: STOPPED, STARTING, or STARTED. STOPPED means the service is not running. STARTING means the service is starting operation and performing any necessary initialization. STARTED means the service has successfully initialized and is operational.

- To start a service: `utils service start service name`
  This command starts the named service.

- To stop a service: `utils service stop service name`
  This command stops the named service.

- To start Cisco Tomcat: `utils service start Cisco Tomcat`

- To stop Cisco Tomcat: `utils service stop Cisco Tomcat`

- To restart Cisco Tomcat: `utils service restart Cisco Tomcat`

---

**Note**

If a Cisco Finesse service-related problem exists, we recommend a restart of a Finesse service as a last resort. Most service-related problems cannot be corrected by restarting a service. Restarting A Cisco DB is never recommended.

---

**Cisco Finesse Notification Service Logging**

To view the status of, enable, or disable Cisco Finesse Notification Service logging:
To retrieve the status of Cisco Finesse Notification Service logging: **utils finesse notification logging status**

This command displays whether Cisco Finesse Notification Service logging is currently enabled or disabled on the system.

To enable Cisco Finesse Notification Service logging: **utils finesse notification logging enable**

**Note**

You must stop the Cisco Finesse Notification Service and the Cisco Tomcat Service before you can enable Cisco Finesse Notification Service logging. You can use the following commands to stop these services: **utils service stop Cisco Finesse Notification Service** and **utils service stop Cisco Tomcat**.

If these services are not stopped, the command to enable Cisco Finesse Notification Service logging fails. This command also fails if Cisco Finesse Notification Service logging is already enabled.

To disable Cisco Finesse Notification Service logging: **utils finesse notification logging disable**

**Note**

You must stop the Cisco Finesse Notification Service and the Cisco Tomcat Service before you can disable Cisco Finesse Notification Service logging. You can use the following commands to stop these services: **utils service stop Cisco Finesse Notification Service** and **utils service stop Cisco Tomcat**.

If these services are not stopped, the command to disable Cisco Finesse Notification Service logging fails. This command also fails if Cisco Finesse Notification Service logging is already disabled.

**Upgrade**

Upgrade-related commands are grouped under **utils system upgrade**.

To initiate an upgrade: **utils system upgrade initiate**

This command allows you to install upgrades and Cisco Option Package (COP) files from both local and remote directories.

To cancel an upgrade: **utils system upgrade cancel**

**Remote Account Management**

Run the following command to enable, disable, create, and check the status of a remote access account: **utils remote_account**

A remote account generates a pass phrase that allows Cisco support personnel to access the system for the specified life of the account.

- **utils remote_account create account life**

  where _account_ is the account name and _life_ indicates the life of the account in days.
• utils remote_account disable
• utils remote_account enable
• utils remote_account status

Replication Status

To check replication status, run the following commands on the primary Finesse server:

• utils dbreplication status
  This command runs the replication status check in the background.

• utils dbreplication runtimestate
  This command returns the replication status on both the primary and secondary Finesse servers.
  • Check the RTMT counter value for replication. If all nodes in the cluster show a replication status of 2, replication is functioning correctly.
  • If the RTMT counter value for replication status is 3 or 4 for all nodes in the cluster, replication is set up, but an error occurred and replication is not functioning properly.
    ◦ Run the command utils dbreplication status and check the output.
    ◦ If mismatched rows appear in the output file, run the command utils dbreplication repair all from the primary Finesse server.

• Check the RTMT counter value for replication. If any node shows any replication value other than 1 or 2, replication is not set up correctly and you must reset replication for that node.
  • If the majority of the nodes show a replication value of 0 or 1, run the command utils dbreplication reset all from the primary Finesse server.
3rdpartygadget Account

The 3rdpartygadget account is used to upload third-party gadgets to the Finesse server. Before you can use this account, you must set the password.

This password is not migrated across upgrades. After you perform an upgrade, you must reset the password before you can make changes to any third-party gadgets.

Run the following command to set or reset the password of the 3rdpartygadget account (where password is the new password for the account):

```
utils reset_3rdpartygadget_password password
```

---

**Note**

Passwords cannot contain spaces or double quotes.

---

**Note**

If you plan to upload third-party gadgets to the Finesse server, you must have a developer support services contract or work with a Cisco partner who has a developer support services contract. For more information about uploading third-party gadgets, see the *Cisco Finesse Web Services Developer Guide*. 
CiscoUnifiedCommunicationsOSAdministration

The Cisco Unified Communications Solutions Unified OS Administration tool is available to you as follows:

1. Navigate to http://host or IP address/cmplatform where host or IP address is the hostname or IP address of your server.

2. Sign in, using the username and password for the Application User account established during the installation.

After you sign in to OS Administration, you can access other Unified Communications Solutions tools from the OS Administration Navigation drop-down list.

Use Cisco Unified Operating System Administration to perform many common system-administration functions. The following are the Unified OS Administration menus:

- **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.

---

**Warning**

Do not change IP settings without the guidance of Cisco.

- **Security**: Manage certificates and set up and manage IPSec policies
- **Software Upgrades**: Perform an upgrade and revert to a previous version
- **Services**: Use the Ping and Remote Support features
Cisco Finesse Failover Mechanisms

This chapter describes failover and redundancy mechanisms for Cisco Finesse.

- CTI Failover, page 47
- AWDB Failover, page 48
- Finesse Client Failover, page 48
- Desktop Behavior, page 49

CTI Failover

The prerequisites for CTI failover are as follows:

- Unified Contact Center Enterprise (Unified CCE) is configured in a duplex mode.
- The B Side CTI host and port are configured through the Finesse administration console.

If Finesse loses connection to the A Side CTI server, and the preceding prerequisites have been implemented, CTI failover occurs.

When Finesse is used in a duplex Unified CCE deployment, and it loses connection to the A Side CTI server, it tries to reconnect five times. If the number of connection attempts exceeds the retry threshold, Finesse then tries to connect to the B Side CTI server the same number of times. Finesse keeps repeating this process until it makes a successful connection to the CTI server.

A loss of connection to the CTI server can occur due to the following:

- Finesse misses three consecutive heartbeats from the connected CTI server.
- Finesse encounters a failure on the socket opened to the CTI server.

During failover, Finesse does not handle client requests. Any request made during this time receives a 503 "Service Unavailable" error message. In addition, Finesse does not send out events during this period. After Finesse reconnects to a CTI server, it starts responding to client requests and publishing events.

Any call control, call data, or agent state actions that occur during CTI failover are published as events to the agent desktop after failover is complete. This allows Finesse clients to reflect an accurate view of the call control, call data, and agent state.
If an agent makes or answers a call and ends that call during failover (that is, the entire call takes place during failover), the corresponding events are not published after failover is complete.

---

**Note**

An agent or supervisor who signs in after being on an active conference with other devices (which are not associated with another agent or supervisor) may experience unpredictable behavior with the Finesse desktop due to incorrect call notifications from Unified CCE. These limitations also encompass failover scenarios where a failover occurs while the agent or supervisor is participating in a conference call. For example, an agent is in a conference call when the Finesse server fails. When the agent is redirected to the other Finesse server, that agent may see unpredictable behavior on the Finesse desktop. Examples of unpredictable behavior include, but are not limited to, the following:

- The desktop does not reflect all participants in a conference call.
- The desktop does not reflect that the signed-in agent or supervisor is in an active call.
- Finesse receives inconsistent call notifications from Unified CCE.

Despite these caveats, the agent or supervisor can continue to perform normal operations on the phone.

Desktop behavior returns to normal after the agent or supervisor drops off the conference call.

---

### AWDB Failover

The prerequisites for AWDB failover are as follows:

- The secondary Administrative Workstation Database (AWDB) is configured.
- The secondary AWDB host is configured through the Finesse administration console.

Agents and supervisors are authenticated against the AWDB database. When an agent or supervisor makes a successful API request (such as a sign-in request or call control request), the credentials are cached in Finesse for 30 minutes from the time of the request. After a user is authenticated, that user continues to be authenticated until 30 minutes pass, even if both AWDBs are down. Finesse attempts to reauthenticate the user against the AWDB only after the cache expires.

If Finesse loses connection to the primary Administration & Data server, and the preceding prerequisites have been implemented, AWDB failover occurs. After Finesse loses connection to the primary Administration & Data server, it tries to reconnect to the secondary server. Finesse repeats this process for every API request until it can connect to one of the Administration & Data servers. During failover, Finesse does not process any requests, but clients can still receive events.

### Finesse Client Failover

With a two-node Finesse setup (primary and secondary Finesse servers), if the primary server goes out of service, agents who are signed in to that server are redirected to the sign-in page of the secondary server.

Client failover can occur for the following reasons:

- With a two-node Finesse setup (primary and secondary Finesse servers), if the primary server goes out of service, agents who are signed in to that server are redirected to the sign-in page of the secondary server.
Client failover can occur for the following reasons:

- The Cisco Tomcat Service goes down.
- The Finesse Webapp Service goes down.
- The Cisco Finesse Notification Service goes down.
- Finesse loses connection to both CTI servers.

## Desktop Behavior

Under certain conditions, Finesse sends a code of 255 to the CTI server (you may see a different code on the CTI server side). The actual behavior of the desktop under these conditions depends on the setting for Logout on Agent Disconnect (LOAD) in Unified CCE. By default, the CTI server places the agent in Not Ready state.

The following table lists the conditions under which Finesse sends this code to the CTI server.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Desktop Behavior</th>
<th>Server Action</th>
<th>Race Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The agent closes the browser, the browser crashes, or the agent clicks the Back button on the browser.</td>
<td>When you close the browser or navigate away from the Finesse desktop, the Finesse desktop makes a best-effort attempt to notify the server.</td>
<td>Finesse receives a presence notification of Unavailable from the client. Finesse waits 10 seconds, and then sends a forced logout request to the CTI server.</td>
<td>1 The agent closes the browser window. Finesse receives a presence notification of Unavailable for the user. Finesse tries to sign the agent out; however, that agent is already signed out.</td>
</tr>
<tr>
<td>The client refreshes the browser</td>
<td>—</td>
<td>Finesse receives a presence notification of Unavailable from the client.</td>
<td>2 If the browser crashes, it can take the Finesse server 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 in to the secondary Finesse server before the primary Finesse server 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 secondary Finesse server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 If the Finesse desktop is running over a slower network connection, Finesse may not always receive an Unavailable presence notification from the client browser. In this situation, the behavior mimics a browser crash, as described in the preceding condition.</td>
</tr>
</tbody>
</table>
The client encounters a network glitch (Finesse is in service) | Because the connection to the Finesse server temporarily goes down, the client fails over to the secondary Finesse server. | The primary Finesse server receives a presence notification of Unavailable from the client. Because Finesse is in service, it sends a forced logout request to the CTI server for the agent. | A situation can occur where the forced logout does not happen before the client signs in to the secondary Finesse server. If the agent is on a call, the primary Finesse server sends the forced logout request after the call ends. The agent will be signed out or put into Not Ready state when the call ends, even though the client is already signed in to the secondary Finesse server.

wants 10 seconds before sending a forced logout request to the CTI server to allow the browser to reconnect after the refresh.
BACKUP AND RESTORE

Cisco Finesse uses the backup and restore tools provided by the common Cisco Unified Communications platform services.

To access the Disaster Recovery System (DRS) application, direct your browser to the following URL: https://Finesse Server IP:8443/df, where Finesse Server IP is the IP address of your Finesse server.

For more information about backup and restore, see the detailed online help provided with the DRS application.
APPENDIX

XML Schema Definition

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

```xml
<?xml version="1.0" encoding="ISO-8859-1" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    targetNamespace="http://www.cisco.com/vtg/finesse"
    xmlns="http://www.cisco.com/vtg/finesse"
    elementFormDefault="qualified">
    <!-- 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:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="gadget">
        <xs:simpleType>
            <xs:restriction base="xs:anyURI">
                <xs:minLength value="1" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="role" type="role"/>
    <xs:element name="gadgets"> <!-- Grouping of a set of gadgets -->
        <xs:complexType>
            <xs:sequence 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:schema>
```
<xs:element name="page"> <!-- Grouping of a set of persistent gadgets -->
    <xs:complexType>
        <xs:sequence 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"> <!-- Id of the tab selector in the desktop -->
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="id"/> <!-- Id of the tab selector in the desktop -->
            <xs:element ref="label"/> <!-- Label of the tab selector -->
            <xs:element ref="gadgets" minOccurs="0" maxOccurs="1"/>
        </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"> <!-- Type of the role -->
    <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 maxOccurs="3">
            <!-- only support 3 roles for now -->
            <xs:element ref="layout"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>

</xs:schema>
INDEX

A
Administration Console 4
server settings 4
administrator user 37
    and Command Line Interface 37
Application User 45
    and OS Administration 45

B
best practice 4
    restarting services 4

C
call variable layout 20
Cisco Finesse User Guides vii
Cisco Security Agent 39
CLI 37, 39, 40
    administration user 37
    command to disable Cisco Security Agent 39
    commands supported for Finesse 37
    commands to start, stop, restart services 40
configuration 4, 5
    Contact Center Enterprise administration server 5
    CTI server 4
    server settings 4
Contact Center Enterprise Administration server settings 5

F
Finesse Administration Console vii, 1
Finesse layout XML 34

N
navigation 37, 45
    in Command Line Interface 37
    in the Unified OS Administration tool 45

S
server settings 4
services 4, 40
    CLI commands for 40
    restarting 4
    sign in 37, 45
        for Unified OS Administration tool 45
        to Command Line Interface 37

U
Unified OS Administration tool 45
    accessing 45
    sign in 45
    Welcome page 45

W
Welcome page 45
    Unified OS Administration tool 45