THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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, EXPRESS 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: https://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. (1721R)

© 2010–2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE

Preface ix
  Change History ix
  About This Guide x
  Audience x
  Organization x
  Related Documents xi
  Obtaining Documentation and Submitting a Service Request xi
  Field Alerts and Field Notices xii
  Documentation Feedback xii
  Conventions xii

CHAPTER 1

Getting Started 1
  User Accounts 1
  Administration Tools 1
    Cisco Finesse Administration Console 1
      Sign In to Cisco Finesse Administration Console 2
    CLI 3
    Cisco Unified Communications Operating System Administration 4
      Sign In to Cisco Unified Communications Operating System Administration 4
    Localization 4

CHAPTER 2

Manage System Settings 7
  Contact Center Enterprise CTI Server Settings 7
    Configure Contact Center Enterprise CTI Server Settings 9
  Contact Center Enterprise Administration & Data Server Settings 10
    Configure Contact Center Enterprise Administration & Data Server Settings 12
Cluster Settings 12
Configure Cluster Settings 13

CHAPTER 3
Manage Call Variables Layout 15
Call Variables 15
Configure Call Variables Layout 17
Add ECC Variables to Call Variables Layout 17

CHAPTER 4
Manage Desktop Layout 19
Finesse Desktop Layout XML 19
Default Layout XML 20
Update Default Desktop Layout 23
XML Schema Definition 24
Live Data Reports 27
Prerequisites for Live Data 27
Add Live Data Reports to Finesse 27
Add Live Data Reports to Default Desktop Layout 28
Add Live Data Reports to Custom Desktop Layout 29
Add Live Data Reports to Team Layout 30
Modify Live Data Stock Reports for Finesse 32

CHAPTER 5
Manage Phone Books 35
Phone Books and Contacts 35
Add Phone Book 37
Edit Phone Book 37
Delete Phone Book 38
Import Contacts 39
Export Contacts 40
Add Contact 41
Edit Contact 42
Delete Contact 42

CHAPTER 6
Manage Reasons 45
Not Ready Reason Codes 45
Add Not Ready Reason Code  47
Edit Not Ready Reason Code  48
Delete Not Ready Reason Code  49
Sign Out Reason Codes  50
Add Sign Out Reason Code  51
Edit Sign Out Reason Code  52
Delete Sign Out Reason Code  53
Wrap-Up Reasons  54
Add Wrap-Up Reason  55
Edit Wrap-Up Reason  56
Delete Wrap-Up Reason  57

CHAPTER 7
Manage Team Resources  59
Team Resources  59
Assign Phone Books and Reasons to Team  60
Unassign Phone Books and Reasons from Team  61
Assign Custom Desktop Layout to Team  62
Assign Workflows to Team  62
Unassign Workflows from Team  63

CHAPTER 8
Manage Workflows  65
Workflows and Workflow Actions  65
Workflow Triggers and Outbound Calls  69
Add Browser Pop Workflow Action  69
Add HTTP Request Workflow Action  71
Edit Workflow Action  72
Delete Workflow Action  73
Add Workflow  73
Edit Workflow  75
Delete Workflow  76

CHAPTER 9
Manage Security  77
HTTP and HTTPS Support  77
Cisco Finesse HTTPS Redirect  78
Download CA Certificate 110
Deploy Root Certificate for Internet Explorer 110
Set Up CA Certificate for Internet Explorer Browser 111
Set Up CA Certificate for Firefox Browser 112
Preface

This guide describes how to administer Cisco Finesse.

• Change History, on page ix
• About This Guide, on page x
• Audience, on page x
• Organization, on page x
• Related Documents, on page xi
• Obtaining Documentation and Submitting a Service Request, on page xi
• Field Alerts and Field Notices, on page xii
• Documentation Feedback, on page xii
• Conventions, on page xii

Change History

This table lists and links to changes made to this guide, and gives the dates those changes were made.

<table>
<thead>
<tr>
<th>Change</th>
<th>Date</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated multiple sections to indicate that the features listed do not support the use of extended ASCII characters.</td>
<td>April 7, 2015</td>
<td>• Configure Call Variables Layout, on page 17&lt;br&gt; • Add ECC Variables to Call Variables Layout, on page 17&lt;br&gt; • Add Wrap-Up Reason, on page 55</td>
</tr>
<tr>
<td>Updated to clarify explanation of desktop behavior when Finesse detects that the browser has closed or crashed.</td>
<td>July 28, 2014</td>
<td>Desktop Behavior, on page 98</td>
</tr>
<tr>
<td>Initial release of document for Release 10.5(1)</td>
<td>June 4, 2014</td>
<td></td>
</tr>
</tbody>
</table>
### About This Guide

The *Cisco Finesse Administration Guide* describes how to administer and maintain Cisco Finesse.

### Audience

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

For information about administering Finesse within a Unified Contact Center Express environment, see the *Unified CCX Administration Guide*.

### Organization

This guide is organized as follows:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1: <strong>Getting Started, on page 1</strong></td>
<td>Describes the tools used to administer Finesse and explains how to access them</td>
</tr>
<tr>
<td>Chapter 2: <strong>Manage System Settings, on page 7</strong></td>
<td>Describes how to configure CTI server, Administration &amp; Data server, and cluster settings</td>
</tr>
<tr>
<td>Chapter 3: <strong>Manage Call Variables Layout, on page 15</strong></td>
<td>Describes how to configure which call variables and ECC variables appear in the call control gadget of the Finesse Agent Desktop</td>
</tr>
<tr>
<td>Chapter 4: <strong>Manage Desktop Layout, on page 19</strong></td>
<td>Describes how to update the default layout of the Finesse agent desktop</td>
</tr>
<tr>
<td>Chapter</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Chapter 5: Manage Phone Books, on page 35</td>
<td>Describes how to create, edit, and delete phone books and phone book contacts</td>
</tr>
<tr>
<td>Chapter 6: Manage Reasons, on page 45</td>
<td>Describes how to add, edit, and delete Not Ready reason codes, Sign Out reason codes, and Wrap-Up reasons</td>
</tr>
<tr>
<td>Chapter 7: Manage Team Resources, on page 59</td>
<td>Describes how to assign and unassign phone books, reasons, and custom desktop layouts to teams</td>
</tr>
<tr>
<td>Chapter 8: Manage Workflows, on page 65</td>
<td>Describes how to create, edit, and delete workflows and workflow actions</td>
</tr>
<tr>
<td>Chapter 9: Manage Security, on page 77</td>
<td>Describes how to enforce access to the desktop through HTTPS, trust a self-signed certificate, and upload a CA certificate</td>
</tr>
<tr>
<td>Chapter 10: Manage Third-Party Gadgets, on page 85</td>
<td>Describes how to upload third-party gadgets to Finesse</td>
</tr>
<tr>
<td>Chapter 11: Perform Routine Maintenance, on page 89</td>
<td>Describes how to access Finesse services, collect logs, manage remote accounts, manage third-party gadget accounts, and check replication</td>
</tr>
<tr>
<td>Chapter 12: Cisco Finesse Failover Mechanisms, on page 95</td>
<td>Describes failover and redundancy mechanisms for Cisco Finesse</td>
</tr>
<tr>
<td>Chapter 13: Backup and Restore, on page 101</td>
<td>Describes backup and restore mechanisms for Cisco Finesse</td>
</tr>
</tbody>
</table>

### Related Documents

<table>
<thead>
<tr>
<th>Document or resource</th>
<th>Link</th>
</tr>
</thead>
</table>

### Obtaining Documentation and Submitting a Service Request

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

### Field Alerts and Field Notices

Cisco can modify its products or determine key processes to be important. These changes are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Sign in [www.cisco.com](http://www.cisco.com) and then access the tool at [https://www.cisco.com/cisco/support/notifications.html](https://www.cisco.com/cisco/support/notifications.html).

### Documentation Feedback

To provide comments about this document, send an email message to the following address: [contactcenterproducts_docfeedback@cisco.com](mailto:contactcenterproducts_docfeedback@cisco.com).

We appreciate your comments.

### Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface font</strong></td>
<td>Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example:</td>
</tr>
<tr>
<td></td>
<td>• Choose <strong>Edit &gt; Find</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Finish</strong>.</td>
</tr>
<tr>
<td><strong>italic font</strong></td>
<td>Italic font is used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• To introduce a new term. Example: A <em>skill group</em> is a collection of agents who share similar skills.</td>
</tr>
<tr>
<td></td>
<td>• A syntax value that the user must replace. Example: IF (<em>condition</em>, <em>true-value</em>, <em>false-value</em>)</td>
</tr>
<tr>
<td></td>
<td>• A book title. Example: See the <em>Cisco Unified Contact Center Enterprise Installation and Upgrade Guide</em>.</td>
</tr>
<tr>
<td><strong>window font</strong></td>
<td>Window font, such as Courier, is used for the following:</td>
</tr>
<tr>
<td></td>
<td>• Text as it appears in code or that the window displays. Example:</td>
</tr>
<tr>
<td></td>
<td>&lt;html&gt;&lt;title&gt;Cisco Systems, Inc.&lt;/title&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| `< >`      | 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. |
Getting Started

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

- User Accounts, on page 1
- Administration Tools, on page 1
- Localization, on page 4

User Accounts

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

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

- **Application User account**: Use this account to access the Cisco Finesse administration console.

Administration Tools

Cisco Finesse Administration Console

The Cisco Finesse administration console is a web-based interface used to configure system settings in Cisco Finesse. The administration console contains tabs that you click to access the various administration features. The tab names and the tasks that you can perform on each tab are as follows:

- **Settings**: Configure CTI server, Administration & Data server, and cluster settings.

- **Call Variables Layout**: Manage the call variables and ECC variables that appear on the agent desktop call control gadget.

- **Desktop Layout**: Make changes to the default desktop layout for agents and supervisors.

- **Phone Books**: Add, edit, or delete phone books or phone book contacts.

- **Reasons**: Add, edit, or delete Not Ready reason codes, Sign Out reason codes, or Wrap-Up reasons.

- **Team Resources**: Assign desktop layouts, phone books, reason codes, and wrap-up reasons to specific teams.
• **Workflows:** Create and manage workflows and workflow actions.

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

---

**Note**

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

---

## Sign In to Cisco Finesse Administration Console

**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 Finesses 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 Finesses. 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*.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you use Internet Explorer:</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>A page appears that states there is a problem with the website's security certificate.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Continue to this website (not recommended)</strong>. This action opens the sign in page for the administration console. A certificate error appears in the address bar of your browser.</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Certificate Error</strong>, and then click <strong>View Certificates</strong> to open the Certificate dialog box.</td>
</tr>
<tr>
<td>3.</td>
<td>On the Certificate dialog box, click <strong>Install Certificate</strong>. This action opens the Certificate Import Wizard.</td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>Next</strong>.</td>
</tr>
</tbody>
</table>
### Option | Description
---|---
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.

**Related Topics**

- User Accounts, on page 1
- Manage Security, on page 77

---

### CLI

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

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

**Related Topics**

- User Accounts, on page 1
Cisco Unified Communications Operating System Administration

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

- **Show**: View information on cluster nodes, hardware status, network configuration, installed software, system status, and IP preferences.
- **Settings**: Display and change IP settings, network time protocol (NTP) settings, SMTP settings, time, and version.

**Important**

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

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

Sign In to Cisco Unified Communications Operating System Administration

**Procedure**

**Step 1**

Direct your browser to http://host or IP address/cmplatform, where host or IP address is the hostname or IP address of your server.

**Step 2**

Sign in with the username and password for the Administrator User account.

**Note**

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

**Related Topics**

User Accounts, on page 1

Localization

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

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

**Note**

You cannot uninstall a language pack after it is installed.
Table 1: Supported Languages for Desktop User Interface

<table>
<thead>
<tr>
<th>Language</th>
<th>Locale File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Danish</td>
<td>da_DK</td>
</tr>
<tr>
<td>Dutch</td>
<td>nl_NL</td>
</tr>
<tr>
<td>English</td>
<td>en_US</td>
</tr>
<tr>
<td>Finnish</td>
<td>fi_FI</td>
</tr>
<tr>
<td>French</td>
<td>fr_FR</td>
</tr>
<tr>
<td>German</td>
<td>de_DE</td>
</tr>
<tr>
<td>Italian</td>
<td>it_IT</td>
</tr>
<tr>
<td>Norwegian</td>
<td>nb_NO</td>
</tr>
<tr>
<td>Portuguese</td>
<td>pt_BR</td>
</tr>
<tr>
<td>Spanish</td>
<td>es_ES</td>
</tr>
<tr>
<td>Swedish</td>
<td>sv_SE</td>
</tr>
<tr>
<td>Japanese</td>
<td>ja_JP</td>
</tr>
<tr>
<td>Chinese (simplified)</td>
<td>zh_CN</td>
</tr>
<tr>
<td>Chinese (traditional)</td>
<td>zh_TW</td>
</tr>
<tr>
<td>Korean</td>
<td>ko_KR</td>
</tr>
<tr>
<td>Polish</td>
<td>pl_PL</td>
</tr>
<tr>
<td>Russian</td>
<td>ru_RU</td>
</tr>
<tr>
<td>Turkish</td>
<td>tr_TR</td>
</tr>
</tbody>
</table>

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://hostname of Finesse server/desktop?locale=fr_FR`)

The following items are localized on the desktop:

- labels for field names, buttons, and drop-down lists
- prompts
- messages
Localization

- tool tips
- page titles
- gadget tab names (Finesse gadgets only)

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

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 variables and ECC variables are Unicode enabled and independent of the desktop locale. However, these Unicode characters may not display correctly in the Unified CCE Script Editor, which can cause problems with Unified CCE scripts (especially if Unified CCE is installed on a Native Language Windows Operating System (such as Chinese, Japanese, or Russian).

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.

Finesse does not support the following for localization:
- Finesse administration console
- Tab labels for third-party gadgets deployed in the Finesse gadget container

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 defined 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

Locale-based searching and sorting may not work as expected.
CHAPTER 2

Manage System Settings

You can configure CTI server, Administration & Data server, and cluster settings on the Settings tab of the Cisco Finesse administration console.

- Contact Center Enterprise CTI Server Settings, on page 7
- Contact Center Enterprise Administration & Data Server Settings, on page 10
- Cluster Settings, on page 12

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.

Note

After you make any changes to the values on the Contact Center Enterprise CTI Server Settings gadget, you must restart Cisco Tomcat. 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.

If you restart Cisco Finesse Tomcat, agents must sign out and sign in again. Changes to the CTI server settings and restarting the Cisco Finesse Tomcat Service must be done during hours when agents are not signed in to the Finesses desktop.

Contact Center Enterprise CTI Server Settings

Contact Center Enterprise CTI Server Settings

<table>
<thead>
<tr>
<th>A Side Host/IP Address: 192.168.1.133</th>
<th>B Side Host/IP Address: 192.168.1.133</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Side Port: 42027</td>
<td>B Side Port: 43027</td>
</tr>
<tr>
<td>Peripheral ID: 5001</td>
<td></td>
</tr>
</tbody>
</table>

*Indicates required fields
Although the B Side Host/IP Address and B Side Port fields are not shown as required, an A Side and B Side CTI server are mandatory for a production deployment of Unified CCE and Cisco Finesse.

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 <em>Serviceability Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise</em>. The default value is 42027.</td>
</tr>
<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>
<tr>
<td>B Side Host/IP Address</td>
<td>Either the hostname or IP address of the B Side CTI server.</td>
</tr>
<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>

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

**Related Topics**

*View, Start, or Stop Services*, on page 90
Configure Contact Center Enterprise CTI Server Settings

Access the administration console on the primary Finesse server to configure the A Side and B Side CTI servers.

---

**Note**

After you restart Finesse, it can take approximately 6 minutes for all server-related services to restart. Therefore, you should wait 6 minutes before you attempt to access the Finesse administration console.

---

**Note**

If you are using HTTPS, the first time you access the administration console, you see a browser security warning. To eliminate browser security warnings each time you sign in, you can trust the self-signed certificate provided with Finesse or obtain and upload a CA certificate.

---

**Procedure**

**Step 1**

Sign in to the administration console on the primary Finesse server:

http://FQDN hostname, or IP address of Finesse server/cfadmin

**Step 2**

Sign in with the Application User credentials defined during installation.

**Step 3**

In the Contact Center Enterprise CTI Server Settings area, enter the CTI server settings as described in the following table. Refer to your configuration worksheet if necessary.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Side Host/IP Address</td>
<td>Enter the hostname or IP address of the A Side CTI server. 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>Enter the port number 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.</td>
</tr>
<tr>
<td>Peripheral ID</td>
<td>Enter 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 servers.</td>
</tr>
<tr>
<td>B Side Host/IP Address</td>
<td>Enter the hostname or IP address of the B Side CTI server.</td>
</tr>
<tr>
<td>B Side Port</td>
<td>Enter 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.</td>
</tr>
</tbody>
</table>

**Step 4**

Click Save.
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
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.

Finesse requires that the administration database is configured to use NTLM. If the administration database is configured to use only NTLMv2, Finesse cannot connect to the administration database.

Primary Administration & Data Server is configured on side A and Secondary Administration & Data Server is configured on side B. Make sure Finesse server on both sides connect to Primary Administration & Data Server on side A and fall back to Secondary Administration & Data Server on side B only when Primary Administration & Data Server goes down.

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. If you restart the Cisco Tomcat Service, agents must sign out and sign in again. To avoid this, you can 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 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.</td>
</tr>
<tr>
<td>AW Database Name</td>
<td>Autobots database name</td>
</tr>
</tbody>
</table>
The default value is 1433.

**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.

<table>
<thead>
<tr>
<th>AW Database Name</th>
<th>The name of the AW Database (AWDB) (for example, ucce_instance_awdb).</th>
</tr>
</thead>
<tbody>
<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></td>
<td><strong>Note</strong> This user refers to the Administrator Domain user that the AWDB uses to synchronize with the logger. The AWDB server must use Windows authentication and the configured username must be a domain user.</td>
</tr>
<tr>
<td>Password</td>
<td>The password required to sign in to the AWDB.</td>
</tr>
</tbody>
</table>

For more information about these settings, see the *Administration Guide for Cisco Unified 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
- AW Database Name

If Finesse cannot connect to the AWDB, an error message appears and you are asked if you still want to save. If you click Yes on the error dialog box, the settings are saved. If you click No, the settings are not saved. You can change the settings and try again or click Revert to retrieve the previously saved settings.

When you update the Username or Password fields and click Save, Finesse attempts to authenticate against the AWDB. If authentication fails, an error message appears and you are asked if you still want to save. Click Yes to save the settings or click No to change the settings. Click Revert to retrieve the previously saved settings.

**Note** Finesse will not come into service in case of AWDB errors when connecting Cisco Finesse 11.5(1) and higher versions to Unified CCE 11.5(1) and higher versions.

**Related Topics**

- View, Start, or Stop Services, on page 90
Configure Contact Center Enterprise Administration & Data Server Settings

Configure the Contact Center Enterprise Administration & Data Server settings to enable authentication for Finesse agents and supervisors.

Procedure

**Step 1**
If you are not already signed in, sign in to the administration console.

**Step 2**
In the Contact Center Enterprise Administration & Data Server Settings area, enter the Administration & Data Server settings as described in the following table. Refer to your configuration worksheet if necessary.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Host/IP Address</td>
<td>Enter the hostname or IP address of the Unified CCE Administration &amp; Data Server.</td>
</tr>
<tr>
<td>Backup Host/IP Address</td>
<td>Enter the hostname or IP address of the backup Unified CCE Administration &amp; Data Server.</td>
</tr>
<tr>
<td>Database Port</td>
<td>Enter the port of the Unified CCE Administration &amp; Data Server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Because Finesse expects the primary and backup Administration &amp; 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 &amp; Data Servers.</td>
</tr>
<tr>
<td>AW Database Name</td>
<td>Enter the name of the AW Database (AWDB) (for example, ucceinstance_awdb).</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain of the AWDB.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username required to sign in to the AWDB.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password required to sign in to the AWDB.</td>
</tr>
</tbody>
</table>

**Step 3**
Click Save.

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 *Cisco Finesse Installation and Upgrade Guide*.
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

**Related Topics**
- [View, Start, or Stop Services](#), on page 90

---

**Configure Cluster Settings**

Configure the cluster settings for the secondary Finesse node. The secondary Finesse node handles agent requests if the primary server goes down.

**Procedure**

1. **Step 1**  
   If you are not already signed in, sign in to the administration console with the Application User credentials.

2. **Step 2**  
   In the Cluster Settings area, in the Host/IP Address field, enter the hostname or IP address of the secondary Finesse server.

3. **Step 3**  
   Click Save.
Configure Cluster Settings
CHAPTER 3

Manage Call Variables Layout

On the Call Variables Layout tab on the Cisco Finesse administration console, you can define how call variables appear on the Finesse agent desktop.

- Call Variables, on page 15
- Configure Call Variables Layout, on page 17
- Add ECC Variables to Call Variables Layout, on page 17

Call Variables

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
- BStatus
- 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>
<tr>
<td>Variable</td>
<td>The name of the call variable or ECC variable that is displayed to the agent. The maximum length of this field is 32 characters.</td>
</tr>
<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 dialog box 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.
**Manage Desktop Layout**

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

**Important**

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

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

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

**Finesse Desktop Layout XML**

The Finesse Layout XML defines the layout of the Finesse desktop, including tab names and the gadgets that appear on each tab.

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

- **Finesse Default Layout XML**: Expands to show the layout XML for the default Finesse desktop.
- **Restore Default Layout**: Restores the Finesse desktop to the default layout.
- **Save**: Saves your configuration changes.
- **Revert**: Retrieves and applies the most recently saved desktop layout.

Default Layout XML

The Finesse default desktop layout XML for Unified CCE and Packaged CCE contains optional gadgets and notes that describe how to modify the layout for your deployment type.

For Unified CCE deployments:

Live Data gadgets are not supported for Unified CCE and must either be removed or remain commented out.

For Packaged CCE deployments:

The Agent Queue Statistics gadget is not supported and must either be removed from the layout or commented out (<gadget>/desktop/gadgets/QueueStatistics.jsp</gadget>).

Optional Live Data gadgets are provided in the layout XML but are commented out. Remove the comment tags from the reports you want to appear on the desktop.

```xml
<finesseLayout xmlns="http://www.cisco.com/vtg/finesse">
  <layout>
    <!-- Layout XML content -->
  </layout>
</finesseLayout>
```
<!-- The following Gadget (Agent Queue Statistics) is *not* supported in Packaged CCE deployment.
If you are using Packaged CCE you must comment out or remove this gadget.

<gadget>/desktop/gadgets/QueueStatistics.jsp</gadget>

<--

<!-- The following Gadgets are for LiveData. They are *ONLY* supported in a Packaged CCE Deployment.
If you are using Packaged CCE and wish to show LiveData Reports, then do the following:
1) Uncomment out each Gadget you wish to show.
2) Replace all instances of "my-cuic-server" with the Fully Qualified Domain Name of your Intelligence Center Server.
3) [OPTIONAL] Adjust the height of the gadget by changing the "gadgetHeight" parameter.

IMPORTANT NOTES:
- In order for these Gadgets to work, you must have performed all documented pre-requisite steps.
- The use of HTTP/HTTPS *must* match what your Users use for the Finesse Desktop (HTTP or HTTPS).
- If you wish to use HTTP, then HTTP must be enabled on both Finesse and Intelligence Center.
- Do *NOT* change the viewId (unless you have built a custom report and know what you are doing).
- The "teamName" will be automatically replaced with the Team Name of the User logged into Finesse.

-->
The following Tab and Gadgets are for LiveData. They are *ONLY* supported in a Packaged CCE Deployment. If you are using Packaged CCE and wish to show LiveData Reports, then do the following:

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

**IMPORTANT NOTES:**
- In order for these Gadgets to work, you must have performed all documented pre-requisite steps.
- The use of HTTP/HTTPS *must* match what your Users use for the Finesse Desktop (HTTP or HTTPS).
- If you wish to use HTTP, then HTTP must be enabled on both Finesse and Intelligence Center.
- Do *NOT* change the viewId (unless you have built a custom report and know what you are doing).
- The "teamName" will be automatically replaced with the Team Name of the User logged into Finesse.

If you are showing the tab, then also uncomment this section.

```xml
<!--
<tab>
  <id>moreReports</id>
  <label>finesse.container.tabs.agent.moreReportsLabel</label>
</tab>

<!-- HTTPS Version of LiveData Gadgets -->
<?-- "Agent Skill Group" Report -->
<!-- <gadget id=""https://my-cuic-server:8444/cuic/gadget/LiveData/
    LiveDataGadget.jsp?gadgetHeight=310&
    viewId=9A8784B10000141000001C50A0006C4&
    filterId=agent.id=CL"></gadget> -->

<!-- HTTP Version of LiveData Gadgets -->
<?-- "Agent Skill Group" Report -->
<!-- <gadget id=""http://my-cuic-server:8081/cuic/gadget/LiveData/
    LiveDataGadget.jsp?gadgetHeight=310&
    viewId=9A8784B10000141000001C50A0006C4&
    filterId=agent.id=CL"></gadget> -->
```
If you are showing the tab, then also uncomment this section as well.
</gadgets>
</tab>
</tabs>
</layout>

<role>Supervisor</role>
<page>
  <gadget>/desktop/gadgets/CallControl.jsp</gadget>
</page>
<tabs>
  <tab>
    <id>home</id>
    <label>finesse.container.tabs.supervisor.homeLabel</label>
    <columns>
      <column>
        <gadgets>
          <gadget>/desktop/gadgets/TeamPerformance.jsp</gadget>
          <gadget>/desktop/gadgets/QueueStatistics.jsp</gadget>
        </gadgets>
      </column>
    </columns>
  </tab>
  <tab>
    <id>manageCall</id>
    <label>finesse.container.tabs.supervisor.manageCallLabel</label>
  </tab>
</tabs>
</layout>
</finesseLayout>

Update Default Desktop Layout

When you modify the layout of the Finesse desktop, the changes you make take effect on the 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 the desktop.

Note

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

Procedure

Step 1

In the Finesse Layout XML area, make changes to the XML as required.

Example:

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

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

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

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

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

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

```xml
<tab>
    <id>tab-id</id>
    <label>Tab Label</label>
    <columns>
        <column>
            <gadgets>
                <gadget>/gadget/1/url.xml</gadget>
                <gadget>/gadget/2/url.xml</gadget>
            </gadgets>
        </column>
        <column>
            <gadgets>
                <gadget>/gadget/3/url.xml</gadget>
                <gadget>/gadget/4/url.xml</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```

Step 2  Click Save.

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

Step 3  After you save your changes, if you want to revert to the last saved desktop layout, click Revert. If you want to revert to the default desktop layout, click Restore Default Layout.

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

Related Topics
- Upload Third-Party Gadgets, on page 86
- Add Live Data Reports to Custom Desktop Layout, on page 29

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"
```
<!-- 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 minOccurs="0" maxOccurs="unbounded">
      <!-- No limit to number of gadget URIs for now -->
      <xs:element ref="gadget"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="column">
  <!-- Grouping of a set of gadgets within a column -->
  <xs:complexType>
    <xs:sequence minOccurs="0" maxOccurs="unbounded">
      <!-- No limit to number of gadget URIs for now -->
      <xs:element ref="gadgets"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="columns">
  <!-- Grouping of a set of columns -->
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="column" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="page">
  <!-- Grouping of a set of persistent gadgets -->
  <xs:complexType>
    <xs:sequence minOccurs="0" maxOccurs="unbounded">
      <!-- No limit to number of gadget URIs for now -->
      <xs:element ref="gadget"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="tab">
  <xs:complexType>
    <xs:sequence>
      <!-- Id of the tab selector in the desktop -->
      <xs:element ref="id"/>
      <!-- Label of the tab selector -->
      <xs:element ref="label"/>
      <xs:choice>
        <xs:element ref="gadgets" minOccurs="0" maxOccurs="1"/>
        <xs:element ref="columns" minOccurs="0" maxOccurs="1"/>
      </xs:choice>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="tabs">
  <!-- Grouping of tabs -->
  <xs:complexType 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:element ref="role"/>
  <!-- List of page gadgets -->
  <xs:element ref="page"/>
  <!-- Grouping of tabs for this particular role -->
  <xs:element ref="tabs"/>
</xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="finesseLayout">
  <!-- Layout of the desktop -->
  <xs:complexType maxOccurs="3">
    <!-- only support 3 roles for now -->
    <xs:element ref="layout"/>
  </xs:sequence>
</xs:complexType>
</xs:element>
Live Data Reports

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

Note
Finesse supports Live Data reports only with Packaged Contact Center Enterprise.

Prerequisites for Live Data

Before you add Live Data reports to the desktop, you must meet the following prerequisites:

- You must have the Live Data reports configured and working in Cisco Unified Intelligence Center.
- You must use either HTTP or HTTPS for both Cisco Unified Intelligence Center and Finesse. You cannot use HTTP for one and HTTPS for the other. The default setting for both after a fresh installation is HTTPS. If you want to use HTTP, you must enable it on both Cisco Unified Intelligence Center and Finesse. For information about enabling HTTP for Cisco Unified Intelligence Center, see the at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.
- Ensure that user synchronization is enabled for Cisco Unified Intelligence Center. For more information, see the.
- If your deployment uses HTTPS, you must upload security certificates to the Finesse and Cisco Unified Intelligence Center servers. Both Finesse and Cisco Unified Intelligence Center are installed with self-signed certificates. However, if you use the self-signed certificates, agents and supervisors must accept certificates in the Finesse desktop when they sign in before they can use the Live Data gadget. To avoid this requirement, you can provide a CA certificate instead. You can obtain a CA certificate from a third-party certificate vendor or produce one internal to your organization.

Related Topics
Certificates for Live Data, on page 107
Cisco Finesse HTTPS Redirect, on page 78
Administration Console User Guide for Cisco Unified Intelligence Center

Add Live Data Reports to Finesse

The following sections describe how to add the Live Data reports to the Finesse desktop. The procedure that you follow depends on several factors, described in the following table.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>When to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Live Data reports to default desktop layout</td>
<td>Use this procedure if you want to add Live Data reports to the Finesse desktop after a fresh installation or after an upgrade if you have not customized the default desktop layout.</td>
</tr>
<tr>
<td>Add Live Data reports to custom desktop layout</td>
<td>Use this procedure if you have customized the Finesse desktop layout.</td>
</tr>
</tbody>
</table>
Add Live Data Reports to Default Desktop Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to the default desktop layout. Use this procedure after a fresh installation of Finesse. If you upgraded Finesse but do not have a custom desktop layout, click Restore Default Layout on the Manage Desktop Layout gadget and then follow the steps in this procedure.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Sign in to the Finesse administration console.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the Desktop Layout tab.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Remove the comment characters (&lt;!-- and --&gt;) from each report that you want to add to the desktop layout. Make sure you choose the reports that match the method your agents use to access the Finesse desktop (HTTP or HTTPS).</td>
</tr>
<tr>
<td>Step 4</td>
<td>Replace my-cuic-server with the fully-qualified domain name of your Cisco Unified Intelligence Server.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Optionally, change the gadget height.</td>
</tr>
</tbody>
</table>

Example:

The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows:

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=400&viewId=99E6C8E210000141000000D80A00006C4&filterId=agent.id=CL%20teamName</gadget>
```

If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

| Step 6 | Click Save. |

**Note**

After you add a gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of columns, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without needing to scroll down.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.
Add Live Data Reports to Custom Desktop Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to a custom desktop layout.

**Procedure**

**Step 1**  
Sign in to the Finesse administration console.

**Step 2**  
Click the **Desktop Layout** tab.

**Step 3**  
Click **Finesse Default Layout XML** to show the default layout XML.

**Step 4**  
Copy the XML code for the report you want to add from the Finesse default layout XML. If your agents use HTTP to access Finesse, copy the XML code for the HTTP report. If they use HTTPS, copy the XML code for the HTTPS report.

**Example:**

To add the Agent Report for HTTPS, copy the following:

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=99E6C8E21000014100000D8A0006C4&filterId=agent.id=CL%20teamName</gadget>
```

**Step 5**  
Paste the XML within the tab tags where you want it to appear.

**Example:**

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

```xml
<layout>
    <role>Agent</role>
    <page>
        <gadget>/desktop/gadgets/CallControl.jsp</gadget>
    </page>
    <tabs>
        <tab>
            <id>home</id>
            <label>finesse.container.tabs.agent.homeLabel</label>
            <gadgets>
                <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=99E6C8E21000014100000D8A0006C4&filterId=agent.id=CL%20teamName</gadget>
            </gadgets>
        </tab>
        <tab>
            <id>manageCall</id>
            <label>finesse.container.tabs.agent.manageCallLabel</label>
        </tab>
    </tabs>
</layout>
```

**Step 6**  
Replace `my-cuic-server` with the fully-qualified domain name of your Cisco Unified Intelligence Server.
Add Live Data Reports to Team Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to the desktop layout of a specific team.

Procedure

Step 1  Sign in to the Finesse administration console.
Step 2  Click the Desktop Layout tab.
Step 3  Click Finesse Default Layout XML to show the default layout XML.
Step 4  Copy the XML code for the report you want to add from the Finesse default layout XML. If your agents use HTTP to access Finesse, copy the XML code for the HTTP report. If they use HTTPS, copy the XML code for the HTTPS report.

Example:
To add the Agent Report for HTTPS, copy the following:

\[
\text{<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=99E6C8E210000141000000D80A0006C4&filterId=agent.id=CL\%20teamName</gadget>}
\]

Step 5  Click the Team Resources tab.
Step 6  Select the team from the list of teams for which you want to add the report.

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

Step 8  Check the Override System Default check box.

Step 9  Paste the XML within the tab tags where you want it to appear.

**Example:**

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

```xml
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadgets>
        <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=99E6C8E21000141000000D80A0006C4&filterId=agent.id=CL20teamName</gadget>
      </gadgets>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
  </tabs>
</layout>
```

Step 10  Replace my-cuic-server with the fully-qualified domain name of your Cisco Unified Intelligence Server.

Step 11  Optionally, change the gadget height.

**Example:**

The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows:

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=400&viewId=99E6C8E21000141000000D80A0006C4&filterId=agent.id=CL20teamName</gadget>
```

If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

Step 12  Click Save.
After you add a gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of columns, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without needing to scroll down.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

---

**Modify Live Data Stock Reports for Finesse**

This procedure describes how to modify the Live Data stock reports in Cisco Unified Intelligence Center and add the modified report to the Finesse desktop layout.

---

**Note**

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

---

**Procedure**

**Step 1**
Copy the gadget URL for the report you want to modify from the Finesse default layout XML and paste it into a text editor.

**Example:**
If you want to modify the Agent Report for HTTPS, copy the following URL and paste it into a text editor:

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=99E6CBE21000001410000000D80A0006C4&filterId=agent.id=CL%20teamName</gadget>
```

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

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

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

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

```xml
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htm?viewId=5C90012F1000014000000080A4E5B33&linkType=htmlType&viewType=Grid
```

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

**Step 5**
Replace my-cuic-server with the FQDN of the Cisco Intelligence Center Server.

**Step 6**
Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click **Save**.
Note  After you add the gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of columns, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without the need to scroll.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.
Modify Live Data Stock Reports for Finesse
Manage Phone Books

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

- Phone Books and Contacts, on page 35
- Add Phone Book, on page 37
- Edit Phone Book, on page 37
- Delete Phone Book, on page 38
- Import Contacts, on page 39
- Export Contacts, on page 40
- Add Contact, on page 41
- Edit Contact, on page 42
- Delete Contact, on page 42

Phone Books and Contacts

Finesse supports the following number of phone books:

- 10 global phone books
- 50 team phone books

The system supports a total of 1500 contacts.

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 must be unique, and can be a maximum length of 64 alphanumeric characters.</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.
Step 3 Click **Yes** to confirm the deletion of the selected phone book.

---

**Import Contacts**

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

The import list must be in the specified comma separated values (CSV) format, and can contain a maximum of 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></td>
</tr>
<tr>
<td>Phone Number</td>
<td>32</td>
<td>No</td>
<td>Note</td>
</tr>
<tr>
<td>Notes</td>
<td>128</td>
<td>Yes</td>
<td>The CSV file that contains the contacts to import must use Latin encoding.</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.
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 filed data are not mistaken for field delimiters. If your data does not include these characters, you can omit the double quotes in files you prepare for importing.

**Procedure**

**Step 1**
In the Manage Phone Books gadget, select the phone book into which you want to import a list of contacts.

**Step 2**
Click **Import**.

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 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.
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.

**Related Topics**  
[Import Contacts](#), on page 39

---

## 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.

The List of Contacts for Marketing Team 1

<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
<th>Number</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adams</td>
<td>Evette</td>
<td>1-555-1414</td>
<td>VP Sales East</td>
</tr>
<tr>
<td>Adams</td>
<td>Keith</td>
<td>1-555-2998</td>
<td>Product Owner</td>
</tr>
<tr>
<td>Adams</td>
<td>Alfredo</td>
<td>1-555-1342</td>
<td>Mainline</td>
</tr>
<tr>
<td>Adams</td>
<td>Dusty</td>
<td>1-555-0344</td>
<td>Truck Driver</td>
</tr>
<tr>
<td>Adams</td>
<td>Corey</td>
<td>1-555-1514</td>
<td>QA Engineer</td>
</tr>
<tr>
<td>Adams</td>
<td>Linwood</td>
<td>1-555-0350</td>
<td>VP Sales</td>
</tr>
<tr>
<td>Adams</td>
<td>DeWitt</td>
<td>1-555-2144</td>
<td>Fireman</td>
</tr>
<tr>
<td>Adams</td>
<td>Murray</td>
<td>1-555-1286</td>
<td>Lawyer</td>
</tr>
<tr>
<td>Adams</td>
<td>Jan</td>
<td>1-555-0108</td>
<td>Policeman</td>
</tr>
</tbody>
</table>

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.
Manage Reasons

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

The reason codes you configure in Finesse are not automatically populated in Unified CCE. To populate them across the solution, you must configure the reason codes in both Finesse and Unified CCE.

Certain reason codes are reserved and cannot be used.

For Unified CCE systems, these reserved reason codes are as follows: -1, -2, -3, 0, 999, 32767, 50001, 50002, 50003, 50004, 50005, 50010, 50020, 50030, 50040, and 50042.

Note

- Not Ready Reason Codes, on page 45
- Sign Out Reason Codes, on page 50
- Wrap-Up Reasons, on page 54

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 total of 200 Not Ready reason codes. This includes a maximum of 100 global Not Ready reason codes, and 100 Not Ready team reason codes. The team reason codes can be mapped to any team, and the same reason code can be mapped to multiple teams.
The following table describes the fields on the Manage Reason Codes (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.</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 and must be unique.</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>

**Note**

In previous releases, Finesse did allow you to create multiple Not Ready reason codes with the same code. If you upgraded from a previous release, you may have Not Ready reason codes with duplicate values in your database. After you complete the upgrade, find these duplicate codes and edit them to give them unique values. You can find the duplicate codes by clicking on the Reason Code header to sort the codes by their value.

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

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

**Note**

When you add, edit, or delete a Not Ready reason code, the changes you make take effect on the Finesse desktop after three seconds. However, agents who are signed in when the changes are made must sign out and sign back in to see those changes reflected on their desktops.
When an agent signs into the Finesse desktop, the agent state is set to Not Ready. The agent can then choose to go to Ready status or choose from one of the configured Not Ready reason codes from the agent state drop-down list 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**

**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 Finesse desktop. Use the Manage Reason Codes (Sign Out) gadget to view, add, edit, or delete Sign Out reason codes. Click the Reason Label or Reason Code headers to sort the Sign Out reason codes by label or by reason code, in ascending or descending order. Click the 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 total of 200 Sign Out reason codes. This includes a maximum of 100 global Sign Out reason codes, and 100 Sign Out team reason codes. The team reason codes can be mapped to any team, and the same reason code can be mapped to multiple teams.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason Label</td>
<td>Reason Code</td>
</tr>
<tr>
<td>End of Shift</td>
<td>10</td>
</tr>
<tr>
<td>Vacation Time</td>
<td>22</td>
</tr>
<tr>
<td>Paid Time Off</td>
<td>30</td>
</tr>
</tbody>
</table>
Add Sign Out Reason Code

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

Procedure

Step 1
In the Manage Reason Codes (Sign Out) gadget, click New.

The New Reason Code area appears.

Note

In previous releases, Finesse did allow you to create multiple Sign Out reason codes with the same code. If you upgraded from a previous release, you may have Sign Out reason codes with duplicate values in your database. After you complete the upgrade, find these duplicate codes and edit them to give them unique values. You can find the duplicate codes by clicking on the Reason Code header to sort the codes by their value.

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

• New: Add a new Sign Out reason code

• Edit: Edit an existing Sign Out reason code

• Delete: Delete a Sign Out reason code

• Refresh: Reload the list of Sign Out reason codes from the server

Note

When you add, edit, or delete a Sign Out reason code, the changes you make take effect on the Finesse desktop after three seconds. However, agents who are signed in when the changes are made must sign out and sign 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 Manage Reason Codes (Sign Out) gadget, click New.

The New Reason Code area appears.

Reason Label

The label for the Sign Out reason code.
The label has a maximum length of 40 characters and should be unique for each Sign Out reason code. Both alphanumeric and special characters are supported.

Reason Code

A code for the Sign Out reason.
The code can be any value between 1 and 65535 and must be unique.

Global?

Yes/No. Indicates if the reason code is available globally to all agents (Yes) or to specific teams of agents (No).
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

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:

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

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

For more information about configuring Agent Desktop Settings, see the Configuration Manager Online Help for Unified CCE.
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.</td>
</tr>
<tr>
<td></td>
<td>This label must be unique for each Wrap-Up reason and has a maximum length of</td>
</tr>
<tr>
<td></td>
<td>39 bytes (which equals 39 US English characters). Both alphanumeric and special</td>
</tr>
<tr>
<td></td>
<td>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**

**Note**

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.

*Note* Wrap-Up reason labels are limited to 39 bytes.

**Step 3**
If the Wrap-Up reason is global, select the Global? check box. If the Wrap-Up reason is specific to a team, clear the Global? check box.

*Note* By default, the Global? check box is selected.

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

---

**Edit Wrap-Up Reason**

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.
CHAPTER 7

Manage Team Resources

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

- Team Resources, on page 59
- Assign Phone Books and Reasons to Team, on page 60
- Unassign Phone Books and Reasons from Team, on page 61
- Assign Custom Desktop Layout to Team, on page 62
- Assign Workflows to Team, on page 62
- Unassign Workflows from Team, on page 63

Team Resources

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

The Manage Team Resources gadget contains six tabs, each enabling you to assign or unassign resources to a team. The tabs are defined in the following table.
<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>
<tr>
<td>Workflows</td>
<td>Use this tab to assign/unassign workflows to the team. Only workflows that are defined in the Manage Workflows gadget are available for assignment.</td>
</tr>
</tbody>
</table>

Actions on the Manage Team Resources gadget:

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

---

**Note**

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

---

## Assign Phone Books and Reasons to Team

**Procedure**

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

   Tabs for each available resource appear.

2. **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.

---

**Unassign Phone Books and Reasons from Team**

**Procedure**

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

**Related Topics**  
Manage Desktop Layout, on page 19

Assign Workflows to Team

**Procedure**

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

**Step 2**  
Click the Workflows tab.  
The List of Workflows area appears.

**Step 3**  
Click **Add**.  
The Add Workflow popup appears.

**Step 4**  
Select one or more workflows from the list to assign them to the team.  
Workflows you assign are highlighted in blue in the Add Workflows popup and added to the List of Workflows area.

**Step 5**  
Workflows are executed in the order in which they are listed. Use the up and down arrows to move a selected workflow to the desired position in the list.

**Step 6**  
When you has finished assigning workflows, click **Save**.

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

---

### Unassign Workflows from Team

**Procedure**

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

**Step 2**  
Click the Workflows tab.  
The List of Workflows area appears.

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

**Step 4**  
Click **Save**.
Unassign Workflows from Team
CHAPTER 8

Manage Workflows

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

- Workflows and Workflow Actions, on page 65
- Add Browser Pop Workflow Action, on page 69
- Add HTTP Request Workflow Action, on page 71
- Edit Workflow Action, on page 72
- Delete Workflow Action, on page 73
- Add Workflow, on page 73
- Edit Workflow, on page 75
- Delete Workflow, on page 76

Workflows and Workflow Actions

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

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

Finesse supports the following number of workflows and workflow actions:

- 100 workflows per Finesse system
- 100 actions per Finesse system
- 20 workflows per team
- 5 conditions per workflow
- 5 actions per workflow
- 5 variables per action

Click the column headers to sort workflows and workflow actions in ascending or descending order.
The following table describes the fields on the Manage Workflows gadget.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the workflow. The name must be unique and can be a maximum length of 40 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the workflow. The description can be a maximum length of 128 characters.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the workflow action. The name must be unique and can be a maximum length of 64 characters.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of workflow. Possible values are Browser Pop, HTTP Request.</td>
</tr>
</tbody>
</table>

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

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

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

Each workflow must contain only one trigger. Triggers are based on Finesse dialog events. Dialog events include the following:

- When a call arrives
- When a call is answered

**Note**
If you set a workflow to trigger when a call is answered, the workflow runs when an agent answers an incoming call or makes an outgoing call, or when a customer answers an Outbound Option call.

- When a call ends
- When making a call
- While previewing an Outbound Option call

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

- To determine whether a workflow should execute, its trigger set and conditions are evaluated against each dialog event received.
- The workflow engine processes workflow events for the first call that matches any configured workflow's trigger set and conditions. No other workflows run until this call has ended. If the agent accepts a second call while still on the first call, workflows do not run on the second call even after the first call has ended.

**Note**
Outbound Preview calls are an exception to this rule. You can have a workflow run while the agent previews the call as well as when the agent accepts the call.

- After a workflow for a particular trigger type (for example, Call Arrives) executes, it never triggers again for the same dialog ID.

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

**Note**
Workflows that trigger when a call arrives, when a call is answered, or when making a call run whenever the browser is refreshed. When an agent refreshes the browser, the workflow engine sees the call as newly arrived or newly made. If an HTTP request action is part of the workflow, the HTTP request is sent when the agent refreshes the browser. Applications that receive the HTTP requests must account for this scenario. Otherwise, undesired results may occur.

An example of a workflow is a Call Arrival event that triggers an action that collects information from the dialog event (for example, the ANI or customer information) and displays a web page containing customer information.
You can filter trigger events by the value of the data that comes in the event. You can configure a workflow to execute if any conditions are met or if all conditions are met.

Individual conditions consist of the following:

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

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

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

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

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

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

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

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

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

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

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

If the user has multiple calls when the user refreshes the browser, the Workflow Engine treats the first dialog received from the Finesses server as the first displayed call. This call is not necessarily the same call that was the first displayed call before the browser refresh. Dialogs received for any other call are ignored because they are not considered first displayed calls. If dialogs for more than one call are received before the Workflow Engine is loaded after the browser refresh, no dialogs are evaluated because none are considered first displayed calls.
Workflows run for both Finesse agents and supervisors. The team to which the supervisor belongs (as distinguished from the team that the supervisor manages) determines which workflows run for the supervisor. You may want to put the supervisors in their own team to keep agent workflows from being run for them.

**Workflow Triggers and Outbound Calls**

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

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

<table>
<thead>
<tr>
<th>Workflow Trigger</th>
<th>Preview Outbound Call</th>
<th>Progressive or Predictive Outbound Call</th>
</tr>
</thead>
<tbody>
<tr>
<td>While previewing a call</td>
<td>When the agent previews the call (before the agent accepts or rejects the call).</td>
<td>Does not trigger.</td>
</tr>
<tr>
<td>When a call arrives</td>
<td>When the agent accepts the call.</td>
<td>When the call arrives on the agent desktop.</td>
</tr>
<tr>
<td>When a call is answered</td>
<td>When the customer answers the call. If the agent conferences in another agent or transfers the call, the workflow triggers for the agent who is the recipient of the conference or transfer.</td>
<td>When the customer answers the call. If the agent conferences in another agent or transfers the call, the workflow triggers for the agent who is the recipient of the conference or transfer.</td>
</tr>
<tr>
<td>When a call is made</td>
<td>When the customer call is initiated.</td>
<td>When the customer call is initiated or when failover occurs during the call.</td>
</tr>
<tr>
<td>When a call ends</td>
<td>When the customer call ends.</td>
<td>When the customer call ends.</td>
</tr>
</tbody>
</table>

**Add Browser Pop Workflow Action**

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

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

**Step 1**
In the Manage Workflow Actions gadget, click **New**.
The New Action area appears.

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

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

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

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

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

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

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

**Example:**

```
http://www.google.com/search?q=callVariable1&callVariable2
```

For every variable you select, you can enter test data in the Sample Data box. A sample URL is automatically built in the Browser URL box below the Sample Data area. To test the URL, click Open to open the URL in your browser.
Finessedoes not validate the URL you enter.

**Step 7**
Click Save.

---

**Add HTTP Request Workflow Action**

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

**Procedure**

**Step 1**
In the Manage Workflow Actions area, click **New**.
The New Action area appears.

**Step 2**
In the Name box, enter a name for the action.
A workflow action name can contain a maximum of 64 characters.

**Step 3**
From the Type drop-down list, select **HTTP Request**.

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

**Step 5**
From the Method drop-down list, select the method to use.
You can select either PUT or POST.

**Step 6**
From the Location drop-down list, select the location.
If you are making the HTTP request to a Finesse API, select **Finesse**. If you are making a request to any other API, select **Other**.

**Step 7**
In the Content Type box, enter the content type.
The default content type is application/xml, which is the content type for Finesse APIs. If you are using a different API, enter the content types for that API (for example, application/JSON).

**Step 8**
In the URL box, enter the URL to which to make the request. To add variables to the URL, click the tag icon at the right of the box and select one or more variables from the drop-down list.

**Example:**

`/finesse/api/User/dialogId`  

**Note**
The preceding example is the URL for a Finesse API. If you want to make a request to another API, you must enter the entire URL (for example, http://googleapis.com).

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

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

Step 10 Click Save.

---

**Edit Workflow Action**

**Procedure**

**Step 1** In the Manage Workflow Actions gadget, select the action that you want to edit.

**Step 2** Click Edit.

The Edit Action area appears.

**Step 3** Edit the fields that you want to change.

**Step 4** Click Save.
Delete Workflow Action

Procedure

Step 1  In the Workflow Actions gadget, select the action that you want to delete.
The Delete Action area appears.

Step 2  Click Delete.
A question appears asking you to confirm that you want to delete the selected action.

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

Add Workflow

Procedure

Step 1  In the Manage Workflows gadget, click New.
The New Workflow area appears.
**Step 2**  
In the Name box, enter the name of the workflow.  
**Note**  
The name is limited to 40 characters.

**Step 3**  
In the Description box, enter a description of the workflow.  
**Note**  
The description is limited to 128 characters.

**Step 4**  
In the When to perform Actions drop-down list, select the event that triggers the workflow.

**Step 5**  
In the How to apply Conditions box, select if all conditions are met, or if any conditions are met, and then click **Add Condition** to add up to five conditions.  
**Example:**  
For example, you can specify that the action is taken when CallVariable 1 is equal to 123 and CallVariable 2 begins with 2.

**Step 6**  
In the Ordered List of Actions area, click **Add** to open the Add Actions area. Click an action in this area to add it to the Ordered List of Actions.

**Step 7**  
Use the up and down arrows next to the Ordered List of Actions to move actions into the order in which they should be performed.
Step 8  Click Save.

Step 9  Assign the workflow to one or more teams.

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

Related Topics
Assign Workflows to Team, on page 62

Edit Workflow

Procedure

Step 1  In the Manage Workflows gadget, select the workflow you want to edit.

Step 2  Click Edit.

The Edit Workflow area appears.

Step 3  Edit the fields that you want to change.

Step 4  Click Save.
Delete Workflow

Procedure

Step 1 In the Manage Workflows gadget, select the workflow that you want to delete. The Delete Workflow area appears.

Step 2 Click Delete.
A question appears asking you to confirm that you want to delete the selected workflow.

Step 3 Click Yes to confirm the deletion of the selected workflow.
Manage Security

- HTTP and HTTPS Support, on page 77
- Cisco Finesse HTTPS Redirect, on page 78
- Trust Self-Signed Certificate, on page 78
- Obtain and Upload CA Certificate, on page 80
- Add Certificate for HTTPS Gadget, on page 82
- Reset Security or Admin Password, on page 83

HTTP and HTTPS Support

The Cisco Finesse administration console and agent desktop support both HTTP and secure HTTP (HTTPS). To access the administration console using HTTPS, enter the following URL in your browser (where FQDN, hostname, or IP address is the FQDN, hostname, or IP address of your primary Finesse server):

https://FQDN, hostname, or IP address/cfadmin

To access the administration console using HTTP, enter the following URL in the address bar of your browser (where FQDN is the fully-qualified domain name of your primary Finesse server):

http://FQDN, hostname, or IP address/cfadmin

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

- http://FQDN, hostname, or IP address
- https://FQDN, hostname, or IP address

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

By default, HTTPS access is enabled. You can run the Cisco Finesse HTTPS Redirect CLI command to disable HTTPS and allow HTTP access for both the Finesse administration console and the agent desktop.

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

This command does not impact the Finesse REST APIs.

In a two-node setup, if you enable or disable HTTPS Redirect only on the primary Finesse server, the setting does not replicate to the secondary Finesse server. You must enter the required commands on both the primary and secondary Finesse server.

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`.

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 are not using HTTPS or if you uploaded a CA certificate, you can skip this procedure.
Procedure

Step 1
In your browser, enter the URL for the administration console (https://FQDN of the primary Finesse server/cfadmin) or the agent desktop (https://FQDN of the primary Finesse server/desktop).

Step 2
Perform the steps in the following table for the browser you are using.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you use Internet Explorer:</td>
<td>1. A page appears that states there is a problem with the website's security certificate. Click <strong>Continue to this website (not recommended)</strong>. This action opens the sign in page for the administration console (or agent desktop). A certificate error appears in the address bar of your browser.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Certificate Error</strong>, and then click <strong>View Certificates</strong> to open the Certificate dialog box.</td>
</tr>
<tr>
<td></td>
<td>3. On the Certificate dialog box, click <strong>Install Certificate</strong>. This action opens the Certificate Import Wizard.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you use Internet Explorer 11 with Windows 8.1, you must add Finesse to your trusted sites before the Install Certificate option appears (Internet Options &gt; Security &gt; Trusted Sites &gt; Sites).</td>
</tr>
<tr>
<td></td>
<td>After you click <strong>Install Certificate</strong>, under <strong>Store Location</strong>, select <strong>Current User</strong> to install the certificate for the current user only, or select <strong>Local Machine</strong> to install the certificate for all Windows users who use this computer.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>5. Select <strong>Place all certificates in the following store</strong>, and then click <strong>Browse</strong>.</td>
</tr>
<tr>
<td></td>
<td>6. Select <strong>Trusted Root Certification Authorities</strong>, and then click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Finish</strong>.</td>
</tr>
<tr>
<td></td>
<td>9. If a Security Warning dialog box appears that asks if you want to install the certificate, click <strong>Yes</strong>.</td>
</tr>
<tr>
<td></td>
<td>A Certificate Import dialog box that states the import was successful appears.</td>
</tr>
<tr>
<td></td>
<td>10. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>11. Enter your credentials, and then click <strong>Sign In</strong>.</td>
</tr>
<tr>
<td>If you use Firefox:</td>
<td>1. A page appears that states this connection is untrusted.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>I Understand the Risks</strong>, and then click <strong>Add Exception</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. On the Add Security Exception dialog box, ensure the <strong>Permanently store this exception</strong> check box is checked.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Confirm Security Exception</strong>.</td>
</tr>
</tbody>
</table>
Obtain and Upload CA Certificate

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The page that states this connection is untrusted automatically closes and the administration console (or agent desktop) loads.</td>
</tr>
</tbody>
</table>

5. Enter your credentials, and then click **Sign In**.

6. For the agent desktop only, an error appears that states Finesse cannot connect to the Cisco Finesse Notification Service and prompts you to add a security exception for the certificates issued by the Finesse server.

   Click **OK**.

---

**Note**

This procedure only applies if you are using HTTPS.

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

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

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

https://hostname of primary Finesse server/cmplatform

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

**Note**

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

**Procedure**

**Step 1**

Generate a CSR.

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

b) From the Certificate Name drop-down list, select **tomcat**.

c) Click **Generate CSR**.

**Step 2**

Download the CSR.

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

**Step 3**
Generate and download a CSR for the secondary Finesse server.

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

https://hostname of secondary Finesse server/cmplatform

**Step 4**
Use the CSRs to obtain the CA root certificate, intermediate certificate, and signed application certificate from the Certificate Authority.

**Note** To set up the certificate chain correctly, you must upload the certificates in the order described in the following steps.

**Step 5**
When you receive the certificates, select Security > Certificate Management > Upload Certificate.

**Step 6**
Upload the root certificate.

a) From the Certificate Name 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 Name drop-down list, select tomcat-trust.
b) In the Root Certificate field, enter the name of the root certificate that you uploaded in the previous step. Do not include the extension (for example, TEST Root CA 2048).
c) In the Upload File field, click Browse and browse to the intermediate certificate file.
d) Click Upload File.

**Step 8**
Upload the application certificate.

a) From the Certificate Name drop-down list, select tomcat.
b) In the Root Certificate field, enter the name of the intermediate certificate that you uploaded in the previous step. Include the .pem extension (for example, TEST-SSL-CA.pem).
c) In the Upload File field, click Browse and browse to the application certificate file.
d) Click Upload File.

**Step 9**
After the upload is complete, sign out 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 Tomcat``` to restart the Cisco Finesse Tomcat service.

**Step 13**
Upload the application certificate to the secondary Finesse server.

You do not need to upload the root and intermediate certificates to the secondary Finesse server. After you upload these certificates to the primary server, they are replicated to the secondary server.

**Step 14**
Access the CLI on the secondary Finesse server and restart the Cisco Finesse Notification Service and the Cisco Tomcat Service.

**Related Topics**

Cisco Unified Communications Operating System Administration, on page 4
Add Certificate for HTTPS Gadget

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

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

Note

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

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

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

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

Procedure

Step 1
Download the tomcat.pem certificate from the third-party gadget host.

a) Sign into Cisco Unified Operating System Administration on the third-party gadget host (http://host or IP address/cmplatform, where host or IP address is the hostname or IP address of the third-party gadget host).

b) Click Security > Certificate Management.

c) Click Find.

d) Click tomcat.pem.

e) Click Download and save the file on your desktop.

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://host or IP address/cmplatform, where host or IP address is the hostname or IP address 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 Tomcat on the primary Finesse server.

Step 4
After synchronization is complete, restart Cisco Tomcat on the secondary Finesse server.
Reset Security or Admin Password

If you need to reset the security or admin password, you must perform the following steps on the console of the system using VSphere. You cannot ssh to the system to run the command.

Procedure

Step 1  
Sign in to the platform window with the following username and password: `pwrecovery/pwreset`  
The following messages appear:  
Welcome to Platform password reset.  
Admin and Security password reset are possible.  
Press any key when ready.

Step 2  
Press any key to continue.  
The following messages appear:  
If you have a CD or DVD in the disk drive, remove it now.  
Press any key to continue.

Step 3  
If there is a disk in the disk drive, remove it. When you are ready, press any key to continue.  
The system checks to ensure that you have removed the disk from the drive.  
The following message appears:  
Insert a valid CD or DVD into the disk drive.

Step 4  
Connect the CD/DVD drive and point it to the ISO image.  
The system checks to ensure you have inserted the disk.  
After the system verifies that you have inserted a disk, you are prompted to choose one of the following options:  
Enter 'a' for admin password reset.  
Enter 's' for security password reset.  
Enter 'q' for quit.

Step 5  
Select the appropriate option and provide the new password.  
The system resets the password.
Reset Security or Admin Password
CHAPTER 10

Manage Third-Party Gadgets

- 3rdpartygadget Account, on page 85
- Upload Third-Party Gadgets, on page 86
- Third-Party Gadget Limitations, on page 87

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.

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.

To set (or reset) the 3rdpartygadget account password, access the CLI and run the following command:

```plaintext
utils reset_3rdpartygadget_password
```

You are prompted to enter a password. After you enter a password, you are prompted to confirm the password. The password for the 3rdpartygadget account must be between 5 and 32 characters long and cannot contain spaces or double quotes (").

Note

If the third-party gadget hosted in Cisco Finesse is sending a REST request to the web server via Shindig using the SHA256 certificate, then the keylength should be 1024.

Note

Third-party gadgets are migrated across upgrades and included in DRS backup and restore.
Upload Third-Party Gadgets

After you set the password for the 3rdpartygadget account, you can use SFTP to upload third-party gadgets to the Finesseserver, as illustrated in the following example.

**Note**

Finesse allows you to upload third-party gadgets to your own web server, however, you must ensure that the Finesseserver has access to your web server.

```bash
my_workstation:gadgets user$ sftp 3rdpartygadget@<finesse>
3rdpartygadget@<finesse>'s password:
Connected to <finesse>.
sftp> cd /files
sftp> put HelloWorld.xml
Uploading HelloWorld.xml to /files/HelloWorld.xml
HelloWorld.xml
sftp> exit
```

After you upload a gadget, it is available under the following URL:

http://<finesse>/3rdpartygadget/files/

**Note**

For Unified CCX deployments you must specify port 8082.

To access the gadget uploaded in the previous example, use the following URL:

http://<finesse>/3rdpartygadget/files/HelloWorld.xml

When you add a gadget to the desktop layout, that gadget can be referenced using a relative path. For more information on adding third party gadgets to the Finessedesktop layout, see the section Manage Desktop Layout in the Cisco Finesse Administration Guide.

To include the gadget that was uploaded in the previous example in the desktop layout, add the following XML (highlighted) to the layout:

```xml
<finesseLayout xmlns="http://www.cisco.com/vtg/finesse">
  <layout>
    <role>Agent</role>
    <page>
      <gadget>/desktop/gadgets/CallControl.jsp</gadget>
      <gadget>/3rdpartygadget/files/HelloWorld.xml</gadget>
    </page>
    ...
  </layout>
  <layout>
    <role>Supervisor</role>
    <page>
      <gadget>/desktop/gadgets/CallControl.jsp</gadget>
      <gadget>/3rdpartygadget/files/HelloWorld.xml</gadget>
    </page>
    ...
  </layout>
</finesseLayout>
```
You cannot delete, rename or change permissions of a folder while using SFTP in 3rd party gadget accounts for Unified CCX deployments. In order to perform these actions, SELinux has to be in permissive mode. This can be accomplished by executing the CLI command:

```
utils os secure permissive
```

Note

Because of browser caching and caching in the Finesse web server, you may need to clear the browser cache or restart the Cisco Tomcat service before gadget changes take effect. If you make a change to a gadget and the change is not reflected on the Finess desktop, clear your browser cache.

If you do not see the changes after you clear the browser cache, use the following CLI command to restart the Cisco Tomcat service:

```
admin:utils service restart Cisco Tomcat
```

### Third-Party Gadget Limitations

Third-party gadgets must be .xml files. You cannot use .jsp files.
Perform Routine Maintenance

Access the CLI to perform routine maintenance tasks such as viewing, stopping, or starting services, logging, managing remote accounts, managing third-party gadget accounts, and checking replication.

Use the credentials for the Administrator User account to access the CLI.

- Cisco Finesse Services, on page 89
- Log Collection, on page 90
- Cisco Finesse Notification Service Logging, on page 92
- Remote Account Management, on page 93
- Replication Status, on page 93

Cisco Finesse Services

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**: 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 and Finesse administration application. Which APIs are available to a user depends on the role associated with that user's credentials. This application 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 Diagnostic Portal application**: This application provides performance-related information for Finesse.

If a Cisco Finesse service-related problem exists, restart a Finesse service as a last resort. Most service-related problems cannot be corrected by restarting a service. Restart A Cisco DB only if the service is down.
To restart the Cisco Finesse Notification Service, you must stop and start services in the following order:

1. Stop the Cisco Tomcat service.
2. Stop the Cisco Finesse Notification Service.
4. Start the Cisco Tomcat service.

**View, Start, or Stop Services**

**Procedure**

**Step 1**
Sign into the CLI using the credentials for the Administrator User account.

**Step 2**
To view a list of all services and their states, enter the following command: `utils service list`. 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 initialization. STARTED means the service has successfully initialized and is operational.

**Step 3**
To start a service, enter the following command: `utils service start service name`.

**Example:**
For example, to start Cisco Tomcat, enter the command `utils service start Cisco Tomcat`.

**Step 4**
To stop a service, enter the following command: `utils service stop service name`.

**Example:**
For example, to stop Cisco Tomcat, enter the command `utils service stop Cisco Tomcat`.

**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. The maximum size of this directory is approximately 4.5 GB. 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.

• **finesse-dp:** This directory contains start-up, error, and informational logs generated by the Finesse Diagnostic Portal application.

• **jmx:** This directory contains the JMX counters data generated by the JMX logger process. It contains important jmx counters exposed by Finesse and openfire.

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.
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 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.

  
  **Note**
  
  Ensure the Cisco Finesse Notification Service is running before you run the command to retrieve the status of Cisco Finesse Notification Service logging. If the service is not running, this command fails.

- To enable Cisco Finesse Notification Service logging: `utils finesse notification logging enable`

  **Note**
  
  Ensure that the Cisco Finesse Notification Service is running before you run the command to enable Cisco Finesse Notification Service logging. If the service is not running, this command fails. This command also fails if Cisco Finesse Notification Service logging is already enabled.

  If you enable logging and then restart the Cisco Finesse Notification Service, logging is automatically disabled.

- To disable Cisco Finesse Notification Service logging: `utils finesse notification logging disable`

  **Note**
  
  Ensure that the Cisco Finesse Notification Service is running before you run the command to disable Cisco Finesse Notification Service logging. If the service is not running, this command fails. This command also fails if the Cisco Finesse Notification Service logging is already disabled.

Related Topics

- Log Collection, on page 90
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 passphrase that allows Cisco support personnel to get access to the system for the specified life of the account.

- `utils remote_account create account life`
  
  `account` is the account name. `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 command on the primary Finesses server:

- `utils dbreplication runtimestate`
  
  This command returns the replication status on both the primary and secondary Finesses 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.

- If the majority of the nodes show a value of 0 or 1, run the command `utils dbreplication reset all` from the primary Finesses server.

- If any node shows any replication value other than 1 or 2, replication is not set up correctly.

- To fix replication, contact Cisco Technical Support.
CHAPTER 12

Cisco Finesse Failover Mechanisms

This chapter describes failover and redundancy mechanisms for Cisco Finesse.

• CTI Failover, on page 95
• AWDB Failover, on page 96
• Finesse Client Failover, on page 97
• Desktop Behavior, on page 98

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.
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 Finesses 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 Finesses 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.
- Finesses 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 Finesses administration console.
- Finesses can connect to the secondary AWDB host.
- The Distributor service is running on the secondary AWDB host.

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 Finesses 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. Finesses attempts to reauthenticate the user against the AWDB only after the cache expires.

If Finesses loses connection to the primary Administration & Data server, and the preceding prerequisites have been implemented, AWDB failover occurs. After Finesses loses connection to the primary Administration & Data server, it tries to reconnect to the secondary server.

Finesses repeats this process for every API request until it can connect to one of the Administration & Data servers. During failover, Finesses does not process any requests, but clients can still receive events.

If Finesses cannot connect to either of the Administration & Data servers and the cache has expired, the systems returns errors as follows:

- Agents and supervisors who attempt to sign in to the Finesses desktop receive an “Invalid user ID or password” error message.
- Administrators cannot update or retrieve settings in the Finesses administration console.
• Users who are already signed in to Finesse receive an “Operation timed out” error message.

• Users who make API requests receive an 401 “Unauthorized” HTTP error message.

If Finesse loses connection to one AWDB and then receives requests, these requests may time out before Finesse can detect that the connection is down and connect to the alternate AWDB. In this scenario, the user (administrator, agent, or supervisor) may need to retry the operation for it to succeed.

Related Topics
Contact Center Enterprise Administration & Data Server Settings, on page 10

Finesse Client Failover

With a two-node Finesse setup (primary and secondary Finesse servers), if the server that an agent is connected to goes out of service, the agent receives a notification that the connection with the server was lost. The Finesse desktop does the following:

• The Finesse desktop continues to check whether the current Finesse server recovers its state.

• The Finesse desktop checks if the other Finesse server is available and in service.

If the other Finesse server is available, the desktop automatically signs the agent into the other server. If the current Finesse server recovers its state, the desktop notifies the agent that it has reconnected.

The Finesse smarter failover logic has three triggers to detect desktop failure:

• The Finesse desktop receives a SystemInfo event that the current server is OUT_OF_SERVICE.

• The BOSH connection is disconnected.

• The “finesse” XMPP user presence changes to unavailable.

No matter which trigger is detected, the desktop reconnection logic is as follows:

1. Poll SystemInfo for current server every 20 seconds and the other Finesse server between 10-45 seconds.

2. If SystemInfo is IN_SERVICE, check the BOSH connection.

3. If BOSH is disconnected, make a BOSH connection request

4. If BOSH is connected and the server is IN_SERVICE, refresh the data.

While polling SystemInfo every 20 seconds, the desktop also checks the availability of the alternate server every 10-45 seconds. The smarter failover logic is biased toward staying with the current server. If the failover logic detects that the alternate server is available, it checks the current server one more time. If the current server has recovered, the desktop reconnects to the current server. If the current server is still down, the desktop connects the agent to the alternate server. In this case, the agent does not automatically reconnect to the failed server after it recovers but instead remains connected to the alternate server.

If the BOSH connection is the source of failure, the JabberWerx library makes three attempts to reconnect before changing the state of the desktop to disconnected. These attempts occur before the smarter failover logic begins.

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.

---

**Note**

After Finesse failover, the pending state of an agent will not be displayed once the agent fails over to the secondary Finesse node. The pending state change is reflected on the desktop only after the call ends.

---

**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.

---

**Note**

Finesse takes up to 120 seconds to detect when an agent closes the browser or the browser crashes and Finesse waits 60 seconds before sending a forced logout request to the CTI server. Under these conditions, Finesse can take up to 180 seconds to sign out the agent.

---

The following table lists the conditions under which Finesse sends this code to the CTI server:
**Scenario** | **Desktop Behavior** | **Server Action**
--- | --- | ---
The agent closes the browser, the browser crashes, or the agent clicks the Back button in the browser. | When you close the browser or navigate away from the Finesse desktop, the Finesse desktop makes a best-effort attempt to notify the server. | 1. Finesse receives a presence notification of *Unavailable* from the client. Finesse waits 60 seconds, and then sends a forced logout request to the CTI server.  

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 into 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.  

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.
### Scenario

The client encounters a network glitch (Finesse is in service)

### Desktop Behavior

Because the connection to the Finesse server temporarily goes down, the client fails over to the secondary Finesses server.

### Server Action

The primary Finesse server takes up to 120 seconds to detect that the client is gone. Finesse is in service, so it waits 60 seconds and 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 Finesses server. If the agent is on a call, the primary Finesses 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 Finesses server.
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/drf, 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.

- Restore First Node in HA Setup with Rebuild, on page 101

Restore First Node in HA Setup with Rebuild

In a high availability (HA) setup, if a hard-drive failure or other critical hardware or software failure occurs, you may need to rebuild the primary Finesse node (publisher node). Perform the following steps to restore the publisher node to its last backed up state.

Procedure

| Step 1 | Perform a fresh installation of Finesse. Make sure to install the same version of Finesse, using the same administrator credentials, network configuration, and security password that you used for the initial installation. |
| Step 3 | From the Restore menu, select Restore Wizard. |
| Step 4 | Select a backup device. Choose the location where your backup is stored. |
| Step 5 | Select the backup file to use. |
| Step 6 | When prompted to choose the nodes to restore, choose the first node. You can also select node2 from the drop-down list in the Select the server from which database data needs to be restored area to restore the recent data from the secondary Finesse (subscriber) node. |
| Step 7 | After the restore process is complete, restart the node. |
| Step 8 | Run the following command on the primary Finesse server: 

```bash
utils dbreplication stop all
```

| Step 9 | Run the following CLI command on the primary Finesse server to set up replication: 

```bash
utils dbreplication reset all
```
The dbreplication reset command can take some time to complete.

Run the CLI command `utils dbreplication runtimestate` on the primary Finesse node. If the RTMT counter value for replication status is 2 on all nodes, replication is functioning properly.

**Note**

Step 10

Restart both nodes.

**Note**

In an HA setup, if a hard-drive failure or critical software failure occurs that requires a rebuild of the secondary Finess node (subscriber node), you can reinstall the secondary node using the same version of Finess, administrator credentials, network configuration, and security password that you used for the initial installation. After the installation is complete, check that the dbreplication is functioning and allow the data to propagate from the primary to the secondary node. However, if you need to restore third-party gadgets to the secondary node, you must either upload them again or run the restore process on the secondary node.

Always check the dbreplication status after any restore, using the CLI command `utils dbreplication runtimestate`. 
Supported Cisco Unified Communications OS Services

The following sections list the Cisco Unified Communications OS services that are supported by Cisco Finesse. For more information about the CLI commands, see the Command Line Interface Guide for Cisco Unified Communications Solutions.

Note

Other commands listed in the Command Line Interface Guide for Cisco Unified Communications Solutions are not tested or qualified for Finesse. Some of those commands may return only platform-specific information. Others may not work for Finesse. Finesse supports only the commands from the guide that are listed here.

Some of these commands may warn about invalidating a software license. Because Finesse is not a licensed server, you can disregard these warnings.

File Commands

- file check
- file delete
- file get
- file list
- file search
- file tail
- file view

Show Commands

- show account
- show date
- show disk usage
- show hardware
• show logins
• show myself
• show network
• show network ipprefs
• show open
• show packages
• show perf
• show status
• show tech all
• show tech dberrcode
• show tech gateway
• show tech locales
• show tech params
• show tech prefs
• show tech repltimeout
• show tech runtime
• show tech systables
• show tech systems
• show tech version
• show timezone
• show trace
• show version

**Utils Commands**

• utils core active list
• utils core inactive list
• utils csa enable
• utils csa disable
• utils csa status
• utils dbreplication clusterreset
• utils dbreplication dropadmindb
• utils dbreplication forcedataasyncsub
• utils dbreplication reset
• utils dbreplication runtime state
• utils dbreplication setrepltimeout
• utils dbreplication stop
• utils diagnose test
• utils firewall ipv4
• utils iostat
• utils network arp
• utils network capture eth0
• utils network connectivity
• utils network host
• utils network ping
• utils network traceroute
• utils ntp
• utils ntp config
• utils ntp restart
• utils ntp server add
• utils ntp server delete
• utils ntp server list
• utils ntp status
• utils ntp start
• utils remote_account
• utils reset_application_ui_administrator_name
• utils reset_application_ui_administrator_password
• utils service
• utils system
• utils system boot
• utils system restart
• utils system upgrade
• utils vmtools status
Note Cisco SNMP integration with Finesse is restricted to platform MIBs. Finesse does not have any application-specific MIBs.

Note The SNMP configuration has to be done individually on both the Finesse primary and secondary nodes if you are upgrading from Finesse version 10.0(1) to 10.5(1) and are using an IP address to connect to the Finesse server.
Certificates for Live Data

You must set up security certificates for Finesse and Cisco Unified Intelligence Center with HTTPS.

You can:

• Use the self-signed certificates provided with Finesse and Cisco Unified Intelligence Center.
• Obtain and install a Certification Authority (CA) certificate from a third-party vendor.
• Produce a certificate internally.

As is the case when using other self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

---

Note

As is the case when using other self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

---

Add Self-Signed Certificates for Live Data

Both Finesse and Unified Intelligence Center are installed with self-signed certificates. If you choose to work with these self-signed certificates (rather than producing your own CA certificate or obtaining a CA certificate from a third-party certificate vendor), you must first export the certificates from the Unified Intelligence Center Publisher and Subscriber. You must then import the certificates into Finesse, importing the Publisher certificate to the Finesse Primary node and the Subscriber certificate to the Finesse Secondary node.

As is the case when using other self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.
Procedure

**Step 1**  
Sign into Cisco Unified Operating System Administration on Cisco Unified Intelligence Center (https://<hostname of Cisco Unified Intelligence Center server>/cmplatform).

**Step 2**  
From the Security menu, select Certificate Management.

**Step 3**  
Click Find.

**Step 4**  
Do one of the following:

- If the tomcat certificate for your server is not on the list, click Generate New. When the certificate generation is complete, reboot your server. Then restart this procedure.
- If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)

**Step 5**  
Click Download .pem file and save the file to your desktop.

You must download the certificates that contain the hostnames Cisco Unified Intelligence Center publisher and Cisco Unified Intelligence Center subscriber.

**Step 6**  
Sign in to Cisco Unified Operating System Administration on the primary Finesse server (http://hostname of Finesse server/cmplatform).

**Step 7**  
From the Security menu, select Certificate Management.

**Step 8**  
Click Upload Certificate.

**Step 9**  
From the Certificate Name drop-down list, select tomcat-trust.

**Step 10**  
Click Browse and browse to the location of the .pem files (Cisco Unified Intelligence Center publisher and subscriber certificates).

**Step 11**  
Click Upload File.

**Step 12**  
Restart Cisco Tomcat on the Finesse server.

---

## Obtain and Upload CA Certificate for Live Data

You must perform the following steps on both the Cisco Unified Intelligence Center publisher server and the Finesse primary server. Use the Certificate Management utility from Cisco Unified Communications Operating System Administration.

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

https://hostname of Finesse or Cisco Unified Intelligence Center server/cmplatform

**Procedure**

**Step 1**  
Generate a CSR.

a) Select Security > Certificate Management > Generate CSR.

b) From the Certificate Name drop-down list, select tomcat.

c) Click Generate CSR.
Step 2  Download the CSR.
   a) Select **Security > Certificate Management > Download CSR.**
   b) From the Certificate Name drop-down list, select **tomcat**.
   c) Click **Download CSR.**

Step 3  Use the CSR to obtain the signed application certificate and the CA root certificate from the Certificate Authority.

Step 4  When you receive the certificates, select **Security > Certificate Management > Upload Certificate.**

Step 5  Upload the root certificate.
   a) From the Certificate Name 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 6  Upload the application certificate.
   a) From the Certificate Name drop-down list, select **tomcat**.
   b) In the Root Certificate field, enter the name of the CA root certificate.
   c) In the Upload File field, click **Browse** and browse to the application certificate file.
   d) Click **Upload File.**

Step 7  After the upload is complete, access the CLI on the primary Finesse server.

Step 8  Enter the command **utils service restart Cisco Finesse Notification Service** to restart the Cisco Finesse Notification service.

Step 9  Enter the command **utils service restart Cisco Tomcat** to restart the Cisco Tomcat service.

Step 10 Upload the root certificate and application certificate to the Cisco Unified Intelligence Center publisher server.

Step 11 After the upload is complete, access the CLI on the Cisco Unified Intelligence Center server.

Step 12 Enter the command **utils service restart Intelligence Center Openfire Service** to restart the Intelligence Center Openfire service.

Step 13 Enter the command **utils service restart Intelligence Center Reporting Service** to restart the Intelligence Center Reporting service.

---

**Produce Certificate Internally**

**Set Up Microsoft Certificate Server**

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

**Procedure**

---

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

Step 2  In the left pane, click **Roles**.

Step 3  In the right pane, click **Add Roles**.
The Add Roles Wizard opens.

Step 4  On the Select Server Roles screen, check the **Active Directory Certificate Services** check box, and then click **Next**.

Step 5  On the Introduction to Active Directory Certificate Services screen, click **Next**.

Step 6  On the Select Role Services screen, check the **Certification Authority** check box, and then click **Next**.

Step 7  On the Specify Setup Type screen, select **Enterprise**, and then click **Next**.

Step 8  On the Specify CA Type screen, select **Root CA**, and then click **Next**.

Step 9  Click **Next** on the Set Up Private Key, Configure Cryptography for CA, Configure CA Name, Set Validity Period, and Configure Certificate Database screens to accept the default values.

Step 10  On the Confirm Installations Selections screen, verify the information, and then click **Install**.

---

**Download CA Certificate**

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

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the Windows 2008 domain controller, run the CLI command <code>certutil -ca.cert ca_name.cer</code>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Save the file. Note where you saved the file so you can retrieve it later.</td>
</tr>
</tbody>
</table>

---

**Deploy Root Certificate for Internet Explorer**

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

**Note**

To avoid certificate warnings, each user must use the fully qualified domain name (FQDN) of the Finesse server to access the desktop.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the Windows 2008 domain controller, click <strong>Start</strong> &gt; <strong>Administrative Tools</strong> &gt; <strong>Group Policy Management</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Right-click Default Domain Policy and select <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Group Policy Management Console, go to <strong>Computer Configuration</strong> &gt; <strong>Policies</strong> &gt; <strong>Window Settings</strong> &gt; <strong>Security Settings</strong> &gt; <strong>Public Key Policies</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click Trusted Root Certification Authorities and select <strong>Import</strong>.</td>
</tr>
</tbody>
</table>
**Set Up CA Certificate for Internet Explorer Browser**

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

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

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Windows Explorer, double-click the <code>ca_name.cer</code> file (in which <code>ca_name</code> is the name of your certificate) and then click <strong>Open</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click <strong>Install Certificate</strong> &gt; <strong>Next</strong> &gt; <strong>Place all certificates in the following store</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Browse</strong> and select <strong>Trusted Root Certification Authorities</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Finish</strong>.</td>
</tr>
</tbody>
</table>

A message appears that states you are about to install a certificate from a certification authority (CA).

**Step 7**

Click **Yes**.

A message appears that states the import was successful.

**Step 8**

To verify the certificate was installed, open Internet Explorer. From the browser menu, select **Tools** > **Internet Options**.

**Step 9**

Click the **Content** tab.

**Step 10**

Click **Certificates**.

**Step 11**

Click the **Trusted Root Certification Authorities** tab.

**Step 12**

Ensure that the new certificate appears in the list.

**Step 13**

Restart the browser for certificate installation to take effect.

**Note**

If using Internet Explorer 11, you may receive a prompt to accept the certificate even if signed by private CA.
Set Up CA Certificate for Firefox Browser

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

Note
To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the Firefox browser menu, select <strong>Options</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Advanced</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Click the <strong>Certificates</strong> tab.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>View Certificates</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>Click <strong>Authorities</strong>.</td>
</tr>
<tr>
<td>6</td>
<td>Click <strong>Import</strong> and browse to the <strong>ca_name.cer</strong> file (in which <strong>ca_name</strong> is the name of your certificate).</td>
</tr>
<tr>
<td>7</td>
<td>Check the <strong>Validate Identical Certificates</strong> check box.</td>
</tr>
<tr>
<td>8</td>
<td>Restart the browser for certificate installation to take effect.</td>
</tr>
</tbody>
</table>