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, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: 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)

© 2010–2020 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE
Preface xi
Change History xi
About This Guide xiii
Audience xiii
Related Documents xiii
Communications, Services, and Additional Information xiii
Field Notice xiv
Documentation Feedback xiv
Conventions xiv

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 4
Cisco Unified Communications Operating System Administration 4
  Sign In to Cisco Unified Communications Operating System Administration 5
Certificate Management 5
  Server-Side Certificate Management 5
  Obtain and Upload CA Certificate 5
  Produce Certificate Internally 7
Client-Side Certificate Acceptance 8
  Client Requirements 8
Deploy Root Certificate for Internet Explorer 8
  Set Up CA Certificate for Internet Explorer and Edge Browsers 9
Configure Call Variables Layouts 39
   Call Variables Popover 40
Add ECC Variables to Call Variables Layout 41
Assign Call Variables Layouts 41
Manipulate Call Variables Layouts with a Workflow 41

CHAPTER 5  Manage Desktop Layout 43
   Gadgets and Components 44
Finesse Desktop Layout XML 44
Default Layout XML 45
Update Default Desktop Layout 47
Drag-and-Drop and Resize Gadget or Component 48
Customize Desktop Properties 49
Horizontal Header 51
Customize Title and Logo in the Header 51
alternateHosts Configuration 52
Headless Gadget Configuration 53
Customize Icons in Left Navigation Bar 53
   Customize Icons for Gadgets 54
      List of Icons 56
XML Schema Definition 66
Live Data Reports 69
   Prerequisites for Live Data 69
Add Live Data Reports to Finesse 70
   Add Live Data Reports to Default Desktop Layout 70
   Add Live Data Reports to Custom Desktop Layout 72
   Add Live Data Reports to Team Layout 73
Modify Live Data Stock Reports for Finesse 74
Configure Live Data Reports with Multiple Views 75

CHAPTER 6  Manage Phone Books 79
   Phone Books and Contacts 79
Add Phone Book 80
Edit Phone Book 81
CHAPTER 7  Manage Reasons  85
Not Ready Reason Codes  85
   Add Not Ready Reason Code  87
   Edit Not Ready Reason Code  87
   Delete Not Ready Reason Code  87
Sign Out Reason Codes  88
   Add Sign Out Reason Code  89
   Edit Sign Out Reason Code  89
   Delete Sign Out Reason Code  90
Predefined System Reason Codes  90
Manage Reason Code Conflicts During Upgrade  92
Wrap-Up Reasons  93
   Add Wrap-Up Reason  94
   Edit Wrap-Up Reason  95
   Delete Wrap-Up Reason  95
   Force Wrap-Up Reason  95

CHAPTER 8  Manage Team Resources  97
Team Resources  97
Assign Phone Books and Reasons to Team  98
Unassign Phone Books and Reasons from Team  99
Assign Custom Desktop Layout to Team  99
   Customize Desktop Properties at Team Level  100
Assign Workflows to Team  102
Unassign Workflows from Team  102

CHAPTER 9  Manage Workflows  103
<table>
<thead>
<tr>
<th>Chapter 10</th>
<th>Manage Security</th>
<th>113</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS Support</td>
<td>113</td>
<td></td>
</tr>
<tr>
<td>HSTS</td>
<td>113</td>
<td></td>
</tr>
<tr>
<td>Reset Security or Admin Password</td>
<td>114</td>
<td></td>
</tr>
<tr>
<td>Cross-Origin Resource Sharing (CORS)</td>
<td>115</td>
<td></td>
</tr>
<tr>
<td>Gadget Source Whitelisting</td>
<td>115</td>
<td></td>
</tr>
<tr>
<td>Security Enhancements</td>
<td>115</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 11</th>
<th>Manage Finesse IP Phone Agent</th>
<th>117</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finesse IP Phone Agent</td>
<td>117</td>
<td></td>
</tr>
<tr>
<td>One Button Sign In</td>
<td>118</td>
<td></td>
</tr>
<tr>
<td>Finesse IP Phone Service Subscription Options</td>
<td>119</td>
<td></td>
</tr>
<tr>
<td>Set Up Application User, Web Access, and HTTPS Server Parameters</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td>Configure Finesse IP Phone Service in Unified CM</td>
<td>121</td>
<td></td>
</tr>
<tr>
<td>Finesse IP Phone Agent Certificate Management</td>
<td>122</td>
<td></td>
</tr>
<tr>
<td>CA-Signed Certificate</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td>Self-Signed Certificate</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td>Export CUCM Certificate</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td>Import CUCM Certificate</td>
<td>124</td>
<td></td>
</tr>
<tr>
<td>Export Cisco Finesse Certificate</td>
<td>124</td>
<td></td>
</tr>
<tr>
<td>Import Certificate into CUCM Trust Store</td>
<td>125</td>
<td></td>
</tr>
<tr>
<td>Add Service Parameters for One Button Sign In</td>
<td>125</td>
<td></td>
</tr>
<tr>
<td>Subscribe Agent Phones to Manual Subscription Service</td>
<td>127</td>
<td></td>
</tr>
<tr>
<td>Set Up Agent Access to the Self Care Portal</td>
<td>127</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 12

Manage Third-Party Gadgets 129
3rdpartygadget Account 129
Upload Third-Party Gadgets 130
Cisco Webex Experience Management 131
Configure Experience Management Gadgets for Finesse Desktop 131

CHAPTER 13

Perform Routine Maintenance 133
Cisco Finesse Services 133
View, Start, or Stop Services 134
Log Collection 134
Collect Logs using Cisco Unified Real-Time Monitoring Tool 137
Syslog Support for Critical Log Messages 138
Cisco Finesse Notification Service Logging 139
Remote Account Management 140

CHAPTER 14

Cisco Finesse Failover Mechanisms 141
CTI Failover 141
AWDB Failover 143
Finesse Desktop Failover 143
Desktop Behavior 145
Finesse IP Phone Agent Failover 149
Guidelines for Optimal Desktop Failover 150
Failover Planning 153

CHAPTER 15

Backup and Restore 155
Backup and Restore 155
Important Considerations 156
SFTP Requirements 156
Master and Local Agents 157
Master Agent Duties 157
Local Agent Duties 157
Backup Tasks 158
Manage Backup Devices 158
Manage Backup Schedules 158
Perform Manual Backup 159
Check Backup Status 159
Restore the Nodes in HA Setup with Rebuild 160

CHAPTER 16

Supported Cisco Unified Communications OS Services 163

APPENDIX A

Cisco Finesse CLI 167
Commands Supported for Cisco Finesse 167
Cisco Finesse Services 167
Cisco Finesse Trace Logging 168
Toaster Notifications 169
Finesse IPPA Inactivity Timeout 169
Configuring Queue Statistics 170
Cross-Origin Resource Sharing (CORS) 171
Gadget Source Whitelisting 174
Supported Content Security Policy Directives 175
Finesse System Commands 176
Desktop Properties 177
WebProxy Service 182
  utils webproxy cache clear 182
  set webproxy access-log-level 183
  set webproxy log-severity 184
  show webproxy access-log-level 185
  show webproxy log-severity 185
Service Properties 185
Log Collection Schedule 188
Upgrade 189
Shutdown 190
Replication Status 190
View Property 191
Update Property 191
Signout from Media Channels 191
APPENDIX B

Certificates for Live Data 193
  Certificates and Secure Communications 193
  Export Self-Signed Live Data Certificates 193
  Import Self-Signed Live Data Certificates 194
  Obtain and Upload Third-party CA Certificate 195

APPENDIX C

Certificates for Cisco Identity Service 197
  Export Cisco Identity Service Certificates 197
  Import Cisco IdS Certificates 198
Preface

- Change History, on page xi
- About This Guide, on page xiii
- Audience, on page xiii
- Related Documents, on page xiii
- Communications, Services, and Additional Information, on page xiii
- Field Notice, on page xiv
- Documentation Feedback, on page xiv
- Conventions, on page xiv

Change History

This table lists the changes that are made to this guide. Most recent changes appear at the top.

<table>
<thead>
<tr>
<th>Change</th>
<th>See</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added Content Security Policy directives.</td>
<td>Supported Content Security Policy Directives</td>
<td>July 2020</td>
</tr>
<tr>
<td>Added CLI to drop participants from conference call.</td>
<td>Service Properties</td>
<td></td>
</tr>
<tr>
<td>Added hostname, IP address and domain name change details.</td>
<td>Manage IP Address and Hostname</td>
<td>April 2020</td>
</tr>
<tr>
<td>Added new DTMF desktop behaviour CLI.</td>
<td>Desktop Properties</td>
<td></td>
</tr>
<tr>
<td>Added new service property configuration CLI for port 5223.</td>
<td>Service Properties</td>
<td></td>
</tr>
</tbody>
</table>


- Added desktop chat search. Desktop Chat Server Settings
- Added Cloud Connect server settings. Cloud Connect Server Settings
- Added keyboard shortcuts. Keyboard Shortcuts
- Added edit call variables. Call Variables
<table>
<thead>
<tr>
<th>Change</th>
<th>See</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added new editors and updated the details of default desktop layout.</td>
<td>Default Layout XML</td>
<td></td>
</tr>
<tr>
<td>Added drag-and-drop and resize details.</td>
<td>Drag-and-Drop and Resize Gadget or Component</td>
<td></td>
</tr>
<tr>
<td>Added desktop property customization.</td>
<td>Customize Desktop Properties</td>
<td></td>
</tr>
<tr>
<td>Changed the phone book limits.</td>
<td>Phone Books and Contacts</td>
<td></td>
</tr>
<tr>
<td>Added new reason code—50006.</td>
<td>Predefined System Reason Codes</td>
<td></td>
</tr>
<tr>
<td>Added text and XML editors for team resources.</td>
<td>Assign Custom Desktop Layout to Team</td>
<td></td>
</tr>
<tr>
<td>Added desktop properties customization at the team level.</td>
<td>Customize Desktop Properties at Team Level</td>
<td></td>
</tr>
<tr>
<td>Updated HTTPS support details.</td>
<td>HTTPS Support</td>
<td></td>
</tr>
<tr>
<td>All the references to <a href="http://FQDN">http://FQDN</a> of Finesse Server/ are changed to</td>
<td>All the references to <a href="https://FQDN">https://FQDN</a> of Finesse Server/</td>
<td></td>
</tr>
<tr>
<td>Added security enhancement details.</td>
<td>Security Enhancements</td>
<td></td>
</tr>
<tr>
<td>Added Finesse IP Phone agent certificate management.</td>
<td>Finesse IP Phone Agent Certificate Management</td>
<td></td>
</tr>
<tr>
<td>Added Cisco Webex Experience Management details.</td>
<td>Cisco Webex Experience Management</td>
<td></td>
</tr>
<tr>
<td>Added 3rdpartygadget directory, webproxy service logs, and call variables logging.</td>
<td>Log Collection</td>
<td></td>
</tr>
<tr>
<td>Added guidelines for desktop failover.</td>
<td>Guidelines for Optimal Desktop Failover</td>
<td></td>
</tr>
<tr>
<td>Added failover planning.</td>
<td>Failover Planning</td>
<td></td>
</tr>
<tr>
<td>Changed queue statistics support for users.</td>
<td>Configuring Queue Statistics</td>
<td></td>
</tr>
<tr>
<td>Added new desktop property configuration CLIs.</td>
<td>Desktop Properties</td>
<td></td>
</tr>
<tr>
<td>Added new webproxy service CLIs.</td>
<td>WebProxy Service</td>
<td></td>
</tr>
<tr>
<td>Added new service property configuration CLIs.</td>
<td>Service Properties</td>
<td></td>
</tr>
<tr>
<td>Added new CLIs for log collection schedules.</td>
<td>Log Collection Schedule</td>
<td></td>
</tr>
<tr>
<td>Added CLI to update CUIC gadget URL.</td>
<td>Upgrade</td>
<td></td>
</tr>
<tr>
<td>Added show property for admin security banner message.</td>
<td>View Property</td>
<td></td>
</tr>
</tbody>
</table>
## Change

<table>
<thead>
<tr>
<th>Change</th>
<th>See</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added update property for admin security banner message.</td>
<td>Update Property</td>
<td></td>
</tr>
<tr>
<td>Added export and import Cisco IdS certificates.</td>
<td>Certificates for Cisco Identity Service</td>
<td></td>
</tr>
<tr>
<td>Removed Context Service Settings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SocialMiner product name change.</td>
<td>All the references to SocialMiner are changed to the Customer Collaboration Platform.</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.


## Related Documents

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

## Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
• To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
• To obtain general networking, training, and certification titles, visit Cisco Press.
• To find warranty information for a specific product or product family, access Cisco Warranty Finder.

**Cisco Bug Search Tool**

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

### Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices
- End of Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at https://cway.cisco.com/mynotifications.

### Documentation Feedback

To provide comments about this document, send an email message to the following address: 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, folder names, and submenu names.</td>
</tr>
<tr>
<td></td>
<td>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 (condition, true-value, false-value)</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><strong>&lt; &gt;</strong></td>
<td>Angle brackets are used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• For arguments where the context does not allow italic, such as ASCII output.</td>
</tr>
<tr>
<td></td>
<td>• A character string that the user enters but that does not appear on the window such as a password.</td>
</tr>
</tbody>
</table>
CHAPTER 1

Getting Started

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

• User Accounts, on page 1
• Administration Tools, on page 1
• Certificate Management, on page 5
• QoS Settings, on page 12
• Localization, on page 12

User Accounts

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

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

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

Administration Tools

Cisco Finesse Administration Console

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

• Settings: Administration & Data server, Configure CTI server, Cluster Settings, IP Phone Agent Settings, and Desktop Chat server.

• Call Variables Layout: Manage the call and ECC variables that appear on the agent desktop call control gadget, team performance gadget, and call popover.

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

• Phone Books: Add, edit, or delete phone books or phone book contacts.
• **Reasons:** Add, edit, or delete Not Ready reason codes, Sign Out reason codes, or Wrap-Up reasons. (Reason Codes are disabled for Packaged CCE deployments).

• **Team Resources:** Assign desktop layouts, phone books, reason codes, and wrap-up reasons to specific teams.

• **Workflows:** Create and manage workflows and workflow actions.

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

---

**Note**

Finesse administration tasks are performed only on the primary Finesse server.

---

**Response Caching**

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


---

### Sign In to Cisco Finesse Administration Console

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

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

**Procedure**

---

**Step 1**

Direct your browser to https://<FQDN>:8445/cfadmin, where *FQDN* is the fully qualified domain name of your primary Finesse server.

**Note**

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

**Step 2**

The first time you access the administration console using HTTPS, you are prompted to trust the self-signed certificate provided with Finesse. The following table describes the steps for each supported browser.

**Note**

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer:</td>
<td>a. A page appears that states this site is untrusted.</td>
</tr>
<tr>
<td></td>
<td>b. Click More information &gt; Go on to the webpage.</td>
</tr>
</tbody>
</table>
On the Sign In page, in the ID field, enter the Application User ID that was used during the installation.

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

Step 5
Click Sign In.

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

**Note**
After 30 minutes of inactivity, Finesse automatically signs you out of the administration console and you must sign in again.

**Sign In Using IPv6**

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

- For HTTPS access, enter:
  
  https://<FQDN>:8445/cfadmin

The remaining steps of the sign in procedure remain the same for IPv6.
Account Locked after Five Failed Sign in Attempts

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

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

Note

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

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

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

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

CLI

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

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

Cisco Unified Communications Operating System Administration

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

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

  Important

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

- **Security**: Manage certificates and set up and manage IPSec policies.
- **Software Upgrades**: Perform and upgrade or revert to a previous version.
- **Services**: Use the Ping and Remote Support features.
Sign In to Cisco Unified Communications Operating System Administration

Procedure

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

Step 2 Sign in with the username and password for the Administrator User account.

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

Certificate Management

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

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

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

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

Server-Side Certificate Management

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

Obtain and Upload CA Certificate

Note This procedure only applies if you are using HTTPS and is optional. If you are using HTTPS, you can choose to either obtain and upload a CA certificate or use the self-signed certificate provided with Finesse.
To eliminate browser security warnings each time you sign in, obtain an application and root certificate signed by a CA. Use the Certificate Management utility from Cisco Unified Communications Operating System Administration.

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

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

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

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

---

**Procedure**

**Step 1** Generate a CSR.

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

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

**Note** To avoid certificate exception warnings, you must access the servers using the FQDN name. Do not select "Multi-server (SAN)" as multi-server certificates is not supported with Cisco Finesse.

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

**Step 2** Download the CSR.

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

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

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

To open Cisco Unified Operating System Administration for the secondary server in your browser, enter:

https://FQDN of secondary Finesse server:8443/cmplatform

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

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

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

**Step 6** Upload the root certificate.

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

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

c) Click **Upload File**.

**Step 7** Upload the intermediate certificate.
Produce Certificate Internally

Set up Microsoft Certificate Server for Windows Server 2012 R2

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

Before you begin

Microsoft .Net Framework 3.5 Service Pack 1 must be installed. See the Windows Server 2012 documentation for instructions.

Procedure

Step 1
In Windows, open the Server Manager.

Step 2
In the Quick Start window, click Add Roles and Features.

Step 3
In the Set Installation Type tab, choose Role-based or feature-based installation and click Next.

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

Step 5
In the Server Roles tab, check the Active Directory Certificate Services box and click Add Features in the pop-up window.

Step 6
In the Features and AD CS tabs, click Next to accept default values.

Step 7
In the Role Services tab, verify that the Certification Authority box is checked and click Next.

Step 8
In the Confirmation tab, click Install.

Step 9
After the installation is complete, click the Configure Active Directory Certificate Service on the destination server link.
Step 10 Verify the credentials (for the domain Administrator user) and click Next.

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

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

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

Step 14 In the Private Key, Cryptography, CA Name, Validity Period, and Certificate Database tabs, click Next to accept default values.

Step 15 Review the information in the Confirmation tab and click Configure.

---

Download CA certificate

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

Procedure

Step 1 On the Windows domain controller, run the CLI command certutil -ca.cert ca_name.cer, in which ca_name is the name of your certificate.

Step 2 Save the file. Note where you saved the file so you can retrieve it later.

---

Client-Side Certificate Acceptance

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

Client Requirements


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

---

Deploy Root Certificate for Internet Explorer

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

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

Step 1 On the Windows domain controller, navigate to Administrative Tools > Group Policy Management.

Note Users who have strict Group Policy defined on the Finesse Agent Desktop have to disable Cross Document Messaging from Group Policy Management to ensure proper functioning of Finesse on Internet Explorer 11.

Step 2 Right-click Default Domain Policy and select Edit.

Step 3 In the Group Policy Management Console, click Computer Configuration > Policies > Window Settings > Security Settings > Public Key Policies.

Step 4 Right-click Trusted Root Certification Authorities and select Import.

Step 5 Import the ca_name.cer file.


Step 7 From the Configuration Model list, select Enabled.

Step 8 Sign in as a user on a computer that is part of the domain and open Internet Explorer.

Step 9 If the user does not have the certificate, run the command gpupdate.exe /target:computer /force on the user’s computer.

Set Up CA Certificate for Internet Explorer and Edge Browsers

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

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

Procedure

Step 1 In Windows Explorer, double-click the ca_name.cer file and then click Open.

Note Here the ca_name is the name of your certificate.

Step 2 In the Certificate Import Wizard, select Current User.

Step 3 Click Install Certificate > Next > Place all certificates in the following store.

Step 4 Click Browse and choose Trusted Root Certification Authorities.

Step 5 Click OK > Next > Finish.

Step 6 Click Yes on the install a certificate from a CA prompt.

Step 7 To verify the certificate was installed, from the browser menu on IE, choose Tools > Internet Options.

Step 8 In the Content tab, click Certificates.

Step 9 In the Trusted Root Certification Authorities tab, ensure that the new certificate appears in the list.

Step 10 Restart the browser for certificate installation to take effect.
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 FQDN of the Finess server to access the desktop.

**Procedure**

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

Set Up CA Certificate for Chrome Browser

**Procedure**

1. In Chrome browser, go to **Settings**.
2. In **Advanced Settings > Privacy and Security**, click **Manage Certificates**.
3. Click **Trusted Root Certification Authorities** tab.
4. Click **Import** and browse to the `ca_name.cer` file.
5. In the **Trusted Root Certification Authorities** tab ensure the new certificate appears in the list
6. Restart the browser for the certificate to install.

Trust Self-Signed Certificate

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

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

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

---

**Add Certificate for HTTPS Gadget**

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

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

**Note**

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

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

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

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

**Procedure**

**Step 1**

Download the certificate from the third-party gadget host.

a) Sign in to Cisco Unified Operating System Administration on the third-party gadget host (https://FQDN:8443/cmplatform, where FQDN is the fully qualified domain name of the third-party gadget host).

b) Click Security > Certificate Management.

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 Finesses server.

a) Sign in to Cisco Unified Operating System Administration on the primary Finesses server (https://FQDN:8443/cmplatform, where FQDN is the fully qualified domain name of the Finesses 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.
QoS Settings

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

Localization

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

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

Note

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

Table 1: Supported Languages for Desktop User Interface

<table>
<thead>
<tr>
<th>Language</th>
<th>Locale File</th>
<th>Language</th>
<th>Locale File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulgarian</td>
<td>Bg_BG</td>
<td>Portuguese</td>
<td>pt_BR</td>
</tr>
<tr>
<td>Catalan</td>
<td>Ca_ES</td>
<td>Romanian</td>
<td>Ro_RO</td>
</tr>
<tr>
<td>Czech</td>
<td>Cs_CZ</td>
<td>Spanish</td>
<td>es_ES</td>
</tr>
<tr>
<td>Croatian</td>
<td>Hr_HR</td>
<td>Swedish</td>
<td>sv_SE</td>
</tr>
<tr>
<td>Danish</td>
<td>da_DK</td>
<td>Slovak</td>
<td>Sk_SK</td>
</tr>
<tr>
<td>Dutch</td>
<td>nl_NL</td>
<td>Slovenian</td>
<td>Sl_SI</td>
</tr>
<tr>
<td>English</td>
<td>en_US</td>
<td>Serbian</td>
<td>Sr_RS</td>
</tr>
<tr>
<td>Finnish</td>
<td>fi_FI</td>
<td>Japanese</td>
<td>ja_JP</td>
</tr>
<tr>
<td>French</td>
<td>fr_FR</td>
<td>Chinese (simplified)</td>
<td>zh_CN</td>
</tr>
<tr>
<td>German</td>
<td>de_DE</td>
<td>Chinese (traditional)</td>
<td>zh_TW</td>
</tr>
<tr>
<td>Hungarian</td>
<td>Hu_HU</td>
<td>Korean</td>
<td>ko_KR</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: https://FQDN/desktop?locale=fr_FR)

The following items are localized on the desktop:

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

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

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

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

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrap-Up Reasons</td>
<td>Limited to 40 bytes of UTF-8 data.</td>
</tr>
<tr>
<td>Call Variables 1-10</td>
<td>Limited to 40 bytes of UTF-8 data.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If Finesse sends a set call data request that exceeds 40 bytes of data, the request fails.</td>
</tr>
</tbody>
</table>
Limit Variable

UTF-8 data is limited to the maximum size in bytes for ECC variables specified in Unified CCE.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECC Variables</td>
<td>UTF-8 data is limited to the maximum size in bytes for ECC variables specified in Unified CCE.</td>
</tr>
</tbody>
</table>

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

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

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

Finesse does not support the following for localization:

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

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

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

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

Manage System Settings

You can configure the following on the Settings tab of the Cisco Finesse administration console:

- Administration and Data server settings
- CTI server settings
- Cluster settings
- Finesse IP Phone agent settings
- Desktop Chat server settings
- Cloud Connect server settings

If Cisco Finesse Tomcat is down, then Finesse administration console displays 502—Bad Gateway error message.

Note

For information about Finesse IPPA settings, see Manage Finesse IP Phone Agent.

- Contact Center Enterprise Administration and Data Server Settings, on page 15
- Contact Center Enterprise CTI Server Settings, on page 18
- Cluster Settings, on page 21
- Desktop Chat Server Settings, on page 22
- Cloud Connect Server Settings, on page 24
- Keyboard Shortcuts, on page 25

Contact Center Enterprise Administration and Data Server Settings

Use the Unified CCE Administration & Data Server Settings gadget to configure the database settings. These settings are required to enable authentication for Finesse agents and supervisors.
To connect to the Unified CCE administration database, Finesse supports connections using SQL or Windows authentication.

The Finesse JDBC driver is configured to use NTLMv2. Therefore, Finesse can connect to the administration database even if the administration database is configured to use only NTLMv2.

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, restart the Cisco Finesse Tomcat Service on the primary and secondary Finesse server. If you restart the Cisco Finesse 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 Finesse Tomcat service during hours when agents are not signed in to the Cisco Finesse desktop.

The following table describes the fields on the Unified CCE Administration & Data Server Settings gadget:

**Table 2: Field Descriptions**

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

**Note**

Finesse expects the primary and backup Administration & Data Server ports to be the same, hence the Finesse administration console exposes one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers.
For more information about these settings, see the Administration Guide for Cisco Unified Contact Center Enterprise and the Staging Guide for Cisco Unified ICM/Contact Center Enterprise.

**Actions on the Unified CCE 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**, 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.

---

**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.**

---

### Configure Contact Center Enterprise Administration and Data Server Settings

Configure the Unified CCE 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 Unified CCE Administration & Data Server Settings area, enter the Administration & Data Server settings as described in the preceding table. For more information, see Table 2: Field Descriptions, on page 16. Refer to your configuration worksheet if necessary.

**Step 3**  Click Save.

What to do next

The CTI test functionality documented in the Configure Unified CCE CTI Server Settings topic depends on AWDB connectivity to determine the CTI version. Or else, the test will not go through.

Contact Center Enterprise CTI Server Settings

Use the Contact Center Enterprise CTI Server Settings gadget to configure the A 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.

For configuring secure connection select the Enable SSL encryption check box.

Test the CTI connection for given configuration using the Test Connection button.

---

**Note**

After you make any changes to the values on the Contact Center Enterprise CTI Server Settings gadget, you must restart all the nodes of Cisco Finesse Tomcat. To make changes to other settings (such as Contact Center Enterprise Administration & Data Server settings), you can make those changes and then restart Cisco Finesse Tomcat.

If you restart Cisco Finesse Tomcat, agents must sign out and sign in again. As a best practice, make changes to CTI server settings and restart the Cisco Finesse Tomcat Service during hours when agents are not signed in to the Finesse desktop.

The secure encryption and Test Connection functionality is supported only from Unified CCE 12.0.

---

**Note**

Although the B Side Host/IP Address and B Side Port fields are not shown as required, A and B Side CTI servers 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:
### Field | Explanation
--- | ---
**A Side Host/IP Address** | 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.

**A Side Port** | The value of this field must match the port configured during the setup of the A Side CTI server. This field is required and accepts values between 1 and 65535. You can find this value using the Unified CCE Diagnostic Framework Portico tool on the PG box. For more information about Diagnostic Framework Portico, see the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise*. The default value is 42027.

**Peripheral ID** | The ID of the Agent PG Routing Client (PIM). The Agent PG Peripheral ID should be configured to the same value for the A and B Side CTI server. This field is required and accepts values between 1 and 32767. The default value is 5000.

**B Side Host/IP Address** | The hostname or IP address of the B Side CTI server.

**B Side Port** | 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.

**Enable SSL encryption** | Check this box to enable secure encryption.

### Actions on the Contact Center Enterprise CTI Server Settings gadget:
- **Save**: Saves your configuration changes.
- **Revert**: Retrieves the most recently saved server settings.
- **Test Connection**: Tests the CTI connection.

### CTI Test Connection
When you click **Test Connection**:

1. Input validation is done on the request attributes.
   - Host/IP Address must not be empty. Port and Peripheral IDs must be within the valid range.
2. Validation is done to check if the provided Host/IP is resolved by Finesse box.
3. Validation is done to check if AW Database is reachable and if a valid path ID is configured for the provided Peripheral ID.

4. Socket connection is established to the provided Host/IP and port. The connection might fail if there is no route to the provided IP. If SSL encryption box is checked, this step also checks for successful TLS handshake. For TLS handshake to be successful, mutual trust has to be established between Finesse and CTI server.


5. After successful socket connection, a CTI initialization request is sent to check if the provided host is a CTI host.

If the CTI response is a success for the CTI initialization request and peripheral provided is configured with Unified CCE, it is confirmed to be a CTI host.

6. CTI connection is closed by sending a CTI session close request.

---

**Note**

If Test Connection is successful for Side A or B of the CTI cluster and the other side fails, it is a valid configuration as CTI server works in active-passive mode and connects to the active node. Inactive CTI node will refuse connection on the CTI port. However, Administrator has to ensure that the failed side also has a valid entry for CTI host and port field. System cannot verify this due to server restrictions.

If Test Connection is successful on Side A and B of the CTI cluster, then there is an error in the system configuration. Verify that the Side A and B of the CTI node have valid entries for port and host.

Test connection API success result does not guarantee peripheral to be online. It only validates if the peripheral provided is configured with Unified CCE.

Test connection API with insecure connection parameter will function as intended for earlier versions of Unified CCE deployments.

---

**Configure Contact Center Enterprise CTI Server Settings**

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

---

**Note**

After you restart Finesse, it can take approximately 6 minutes for all server-related services to restart. Therefore, wait for 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, 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:
https://FQDN 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 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.

---

**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>Hostname</td>
<td>The hostname 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
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

**Step 1**  
Sign into the administration console with the Application User credentials.

**Step 2**  
In the Cluster Settings area, in the Hostname field, enter the hostname of the secondary Finesse server.

**Step 3**  
Click Save.

Desktop Chat Server Settings

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

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

IM&P has a clustered design, where users are distributed across multiple nodes in the cluster. The Desktop Chat initially discovers the IM&P nodes that a user has configured, caches this information and communicates with the actual server for subsequent login, until the browser cache is cleared. To spread the initial discovery load, it is advisable to configure the nodes in a round robin fashion if the deployment has more than one Finesse cluster. For example, if there are 5 IM&P nodes configure Finesse cluster A with node 1 & 2, Finesse cluster B with nodes 3 & 4, and so on.

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Chat Server</td>
<td>Enter the IM&amp;P primary server URL of Desktop Chat.</td>
</tr>
<tr>
<td>Secondary Chat Server</td>
<td>Enter the IM&amp;P secondary server URL of Desktop Chat.</td>
</tr>
</tbody>
</table>
**Actions on the Desktop Chat Server gadget:**

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

---

**Important**

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

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

---

**Note**

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

---

**Desktop Chat Search**

**Note**

To enable this feature in Cisco Finesse, install Finesse 12.0(1)ES4 COP or higher.

By default, the desktop chat user search displays all the users from LDAP. You can refine this search to display the users from the corresponding customer whose Agent or Supervisor initiated the search, based on the Organization Unit (OU) defined in Cisco Unified Communications Manager IM and Presence Service. This is supported on Cisco Unified Communications Manager IM and Presence Service, Release 12.5(1)SU2 ES build version 12.5.1.12900-26 onwards. Contact Cisco TAC for more details.

In Cisco Unified Communications Manager IM and Presence Service, the administrator must map the **Client User Fields** to the **Appropriate LDAP User Fields** in the **Searchable LDAP Attributes** table.

**Searchable LDAP Attributes (Client-to-LDAP Field Attribute Mappings)**

The setting depends on the type of LDAP server that you select, and must exactly match each logical entity on the LDAP server (for example, firstname, lastname, fullname, and so on). Map each Client User to LDAP field attributes for XMPP user search, as follows:

- Active Directory provides default values in the Client User and LDAP user fields. You can edit each field as you require to suit your configuration.

- Generic Directory Server does not provide default values. You must specify which LDAP attributes to map to each Client User Field for XMPP user search.
Configure Desktop Chat Server Settings

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Sign in to the administration console with the Application User credentials.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Desktop Chat Server Settings area, enter the IM&amp;P primary and secondary server URL of the Desktop Chat.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

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

Cloud Connect Server Settings

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


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

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>(mandatory) The Cloud Connect administrator username required to sign in to Cloud Connect.</td>
</tr>
</tbody>
</table>
### Configure Cloud Connect Server Settings

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Sign in to the administration console on the primary Finesseserver using the URL: <a href="https://FQDN">https://FQDN</a> of Finesseserver:8445/cfadmin.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Settings &gt; Cloud Connect Server Settings.</td>
</tr>
</tbody>
</table>
| Step 3 | Enter the Username, Password, and Publisher Address of the Cloud Connect server.  
      | (optional) Enter the Subscriber Address for multinode deployment.       |
| Step 4 | Click Save.                                                            |

### Keyboard Shortcuts

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

#### Keyboard Shortcut Conflicts

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

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

Keyboard shortcut conflict can occur in the following scenarios:
### Conflict Scenario

<table>
<thead>
<tr>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conflicts can occur between keyboard shortcuts at the page level and gadget level.</td>
</tr>
<tr>
<td>Conflicts can occur when two gadgets have the same keyboard shortcut, and both are in the same tab.</td>
</tr>
<tr>
<td>Conflicts can occur when there are multiple instances of the same gadget and focus is on the active tab*.</td>
</tr>
</tbody>
</table>

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

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

---

### Note

- After deploying the third-party gadgets, the administrator must sign in as an agent and a supervisor to check if there are any keyboard shortcut conflicts and resolve them.

- The third-party gadget providers can use the keyboard shortcuts JavaScript library as a guideline to provide a consistent desktop user experience.

- The ECE (Enterprise Chat and Email) keyboard shortcuts are available only if ECE gadget is configured in the Unified CCE deployment. If it is not configured, the third-party gadget developers can use the ECE shortcut keys that are listed in Keyboard Shortcuts List. For more information, see the Cisco Finesse Agent and Supervisor Desktop User Guide at [https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html](https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html).
CHAPTER 3

Manage IP Address and Hostname

Note
To enable this feature in Cisco Finesse, install Finesse 12.5(1)ES2 COP or higher.

• IP Address or Hostname or Domain Name Change, on page 27
• Change IP Address or Hostname Task List, on page 27
• Change IP Address Only, on page 32
• Change Domain Name, on page 33
• Post-Change Tasks and Verification, on page 35

IP Address or Hostname or Domain Name Change

Note
Before you change the IP address or hostname or domain name, update the DNS server with a new host entry.

You can change the IP address or hostname or domain name of the Cisco Finesse cluster nodes in your deployment. These changes can be done for a variety of reasons such as:

• to resolve a duplicate IP address or hostname.
• to move the server from one segment to another.

Note
Hostname supports 24 alphanumeric characters.

Change IP Address or Hostname Task List

The following table lists the tasks to perform before you change the IP address or hostname for Cisco Finesse cluster nodes.
Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Pre-Change Tasks.</td>
<td>Perform system health checks before the IP address or hostname change.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Change IP Address or Hostname using Unified Operating System GUI or Change IP Address or Hostname Using CLI.</td>
<td>Change IP address or hostname for the Cisco Finesse cluster node using either the Unified OS GUI or Command Line Interface (CLI).</td>
</tr>
<tr>
<td><strong>Step 3</strong> Post-Change Tasks and Verification.</td>
<td>Verify system health checks after the IP address or hostname change.</td>
</tr>
</tbody>
</table>

Pre-Change Tasks

Perform the following system health checks for the Cisco Finesse cluster nodes before you change the IP address or hostname or domain name.

Note

If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Procedure

**Step 1** Check the active ServerDown alerts to ensure that all servers are active and available on the Cisco Finesse cluster nodes.

- Check by using RTMT—Select Alert Central from the tree hierarchy or choose System > Tools > Alert > Alert Central and verify the alerts.
- Check by using CLI—Enter `file search activelog syslog/CiscoSyslog ServerDown` command and verify the application event log.

Sample Output:

```
admin:file search activelog syslog/CiscoSyslog ServerDown
Searching path: /var/log/active/syslog/CiscoSyslog
Searching file: /var/log/active/syslog/CiscoSyslog
Search completed
```

**Step 2** Check the DB replication status on all the Cisco Finesse cluster nodes to ensure that all servers are replicating database changes successfully.

- Check by using RTMT—Choose CallManager > Service > Database Summary and verify the replication status.
- Check by using CLI—Enter `show perf query class "Number of Replicates Created and State of Replication"` command and verify the application event log.

Sample Output:

```
admin: show perf query class "Number of Replicates Created and State of Replication"
==&gt;query class :
```
- Perf class (Number of Replicates Created and State of Replication) has instances and values:
  ReplicateCount -> Number of Replicates Created = 344
  ReplicateCount -> Replicate State = 2

Note: All nodes must show the Replicate State as 2. The value 2 refers that the replication state is good.

Step 3
Check network connectivity and DNS server configuration by running the `utils diagnose module validate_network` command on all Cisco Finesse cluster nodes.

Sample Output:
```
admin:utils diagnose module validate_network
Log file: platform/log/diag1.log
Starting diagnostic test(s)
---------------------------
test - validate_network : Passed
Diagnostics Completed
The final output will be in Log file: platform/log/diag1.log
Please use 'file view activelog platform/log/diag1.log' command to see the output
```

Step 4
Run a manual Disaster Recovery System (DRS) backup to ensure that all Cisco Finesse cluster nodes and active services are backed up successfully. For more information, see Disaster Recovery chapter in the Administration Guide for Cisco Unified Communications Manager at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Disaster Recovery

Important: If you have DRS backup, then you can restore your system from the backup files in case of any failure.

Note: The DRS backup files are invalid after successful change of hostname, IP address, or domain name.

Change IP Address or Hostname using Unified Operating System GUI

You can use Cisco Unified Operating System Administration to change the IP address or hostname of the Cisco Finesse cluster nodes in your deployment.

Before you begin
- Perform the system health checks on your deployment. For more information, see Pre-Change Tasks, on page 28.
- Ensure that Single Sign-On is disabled.

Procedure

Step 1
In Cisco Unified OS Administration, choose Settings > IP > Ethernet.

Step 2
Change the Hostname and IP Address. If required, change the Default Gateway.

Step 3
Click Save.
Node services automatically restart with the new changes. Restarting services ensures the proper update and service-restart sequence for the changes to take effect.

Changing the hostname triggers an automatic self-signed certificate regeneration.

**Note** Do not proceed if the new hostname does not resolve to the correct IP address.

**Step 4**

Restart the Cisco Finesse cluster nodes using CLI `utils system restart`.

a) Enter `y` and press Enter to restart the system.

**Sample Output:**

```
admin:utils system restart
*** WARNING ***
Please make sure database replication setup is complete. Use the command 'utils dbreplication runtimestate' to get the current status.
If database replication setup is in progress, restarting the server may leave database replication unable to complete.
Do you really want to restart ?
Enter (yes/no)? yes
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...  
- Service Manager shutting down services... Please Wait
```

What to do next

Post-Change Tasks and Verification, on page 35.

---

**Change IP Address or Hostname Using CLI**

You can use the CLI to change the IP address or hostname of the Cisco Finesse cluster nodes in your deployment.

**Note** If the certificates are invalid or have expired, you must renew the certificates before using the CLI set network hostname.

**Before you begin**

- Perform the system checks on your deployment. For more information, see Pre-Change Tasks, on page 28.
- Ensure that Single Sign-On is disabled.

**Procedure**

- **Step 1** Sign in to the CLI of the Cisco Finesse cluster node that you want to change.
- **Step 2** Enter `set network hostname`.
- **Step 3** Follow the prompts to change the hostname, IP address, and default gateway.
a) Enter the new hostname and press Enter.
b) Enter yes, if you also want to change the IP address. Otherwise, press Enter and move to Step 4.
c) Enter the new IP address.
d) Enter the subnet mask.
e) Enter the address of the gateway.

**Step 4**
Verify that all your input is correct and enter yes to start the process.

**Note**  
Do not proceed if the new hostname does not resolve to the correct IP address.

**Sample Output:**

```
admin:set network hostname

*** W A R N I N G ***
Do not close this window without first canceling the command.
This command will automatically restart system services.
The command should not be issued during normal operating hours.

Note: Please verify that the new hostname is a unique name across the cluster and, if DNS services are utilized, any DNS configuration is completed before proceeding.

Security Warning: This operation will regenerate all CUCM Certificates including any third party signed Certificates that have been uploaded.
Enter the hostname:: samplehostname
Would you like to change the network ip address at this time [yes]:: yes
Warning: Do not close this window until command finishes.
cr-l-c: To quit the input.

*** W A R N I N G ***

Note: Please verify that the new ip address is unique across the cluster.

Enter the ip address:: 10.10.10.9
Enter the ip subnet mask:: 255.255.255.224
Enter the ip address of the gateway:: 10.10.10.1
Hostname: samplehostname
IP Address: 10.10.10.9
IP Subnet Mask: 255.255.255.224
Gateway: 10.10.10.1

Do you want to continue [yes/no]? yes

calling 1 of 6 component notification script: ahostname_callback.sh
Info(0): Process node query returned using finesse25:
name

finesse25
update server table from:'finesse25', to: 'samplehostname'
Rows: 1

updating database, please wait 90 seconds

updating database, please wait 60 seconds

updating database, please wait 30 seconds

calling 2 of 6 component notification script: clm_notify_hostname.sh
calling 3 of 6 component notification script: dfm_notify_hostname_change.py
calling 4 of 6 component notification script: idsLocalPrefsUpdateFile.sh
Going to trigger /usr/bin/python /usr/local/cm/lib/dblupdatefiles-plugin.py -f=samplehostname,finesse25

calling 5 of 6 component notification script: regenerate_all_certs.sh
```
calling 6 of 6 component notification script: update_idsenv.sh
calling 1 of 3 component notification script: afupdateip.sh
calling 2 of 3 component notification script: ahostname_callback.sh
Info(0): Processnode query returned using 192.168.1.25:
name
----
calling 3 of 3 component notification script: clm_notify_hostname.sh

Step 5

Restart the Cisco Finesse cluster node using CLI **utils system restart**.

a) Enter `y` and press `Enter` to restart the system.

**Sample Output:**

```
admin:utils system restart

*** WARNING ***
Please make sure database replication setup is complete. Use the command 'utils dbreplication runtimestate' to get the current status.
If database replication setup is in progress, restarting the server may leave database replication unable to complete.
Do you really want to restart ?
Enter (yes/no)? yes
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
- Service Manager shutting down services... Please Wait
```

What to do next

*Post-Change Tasks and Verification, on page 35.*

## Change IP Address Only

You can use the CLI to change the IP address of the Cisco Finesse cluster nodes in your deployment.

**Before you begin**

- Perform the system health checks on your deployment. For more information, see *Pre-Change Tasks, on page 28.*
- Ensure that Single Sign-On is disabled.

**Procedure**

**Step 1**

Sign in to the CLI of the Cisco Finesse cluster node that you want to change.

**Step 2**

Enter `set network ip eth0 addr mask gw`.

**Table 4: Syntax Description**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>Specifies Ethernet interface 0.</td>
</tr>
</tbody>
</table>
Manage IP Address and Hostname

### Change Domain Name

You can use the CLI to change the domain name of the Cisco Finesse cluster nodes in your deployment.

---

**Parameters**

<table>
<thead>
<tr>
<th><strong>addr</strong></th>
<th>Specifies the server IP address that you want to assign.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mask</strong></td>
<td>Specifies the server network mask that you want to assign.</td>
</tr>
<tr>
<td><strong>gw</strong></td>
<td>Specifies the default gateway of the server that you want to assign.</td>
</tr>
</tbody>
</table>

**Sample Output:**

```
admin: set network ip eth0 10.53.57.101 255.255.255.224 10.53.56.1
*** WARNING ***
This command will restart system services
Note: Please verify that the new ip address is unique across the cluster and, if DNS services are utilized, any DNS configuration is completed before proceeding.
Continue (y/n)?
```

**Step 2**

**a)** Enter `y` and press **Enter** to start the process.

**Sample Output:**

```
admin: set network ip eth0 10.53.57.101 255.255.255.224 10.53.56.1
*** WARNING ***
This command will restart system services
Note: Please verify that the new ip address is unique across the cluster and, if DNS services are utilized, any DNS configuration is completed before proceeding.
Continue (y/n)?
```

**Step 3**

**a)** Enter `y` and press **Enter** to restart the system.

**Sample Output:**

```
admin: utils system restart
*** WARNING ***
Please make sure database replication setup is complete. Use the command 'utils dbreplication runtimestate' to get the current status.
If database replication setup is in progress, restarting the server may leave database replication unable to complete.
Do you really want to restart?
Enter (yes/no)? yes
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
- Service Manager shutting down services... Please Wait
```

---

**What to do next**

Post-Change Tasks and Verification, on page 35.
Before you begin

- Perform the system health checks on your deployment. For more information, see Pre-Change Tasks, on page 28.
- Ensure that Single Sign-On is disabled.

Procedure

Step 1
Sign into the CLI of the Cisco Finesse cluster node that you want to change.

Step 2
Enter `set network domain name`.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the system domain name that you want to assign..</td>
</tr>
</tbody>
</table>

a) Enter y and press Enter to start the process.

Sample Output:

```
admin:set network domain sampledomainname
*** WARNING ***
Adding/deleting or changing domain name on this server will break database replication. Once you have completed domain modification on all systems that you intend to modify, please reboot all the servers in the cluster. This will ensure that replication keeps working correctly. After the servers have rebooted, please confirm that there are no issues reported on the Cisco Unified Reporting report for Database Replication.

The server will now be rebooted. Do you wish to continue.

Security Warning : This operation will regenerate host certificates.
Continue (y/n)? y
```

Step 3
Restart the Cisco Finesse cluster nodes using CLI `utils system restart`.

a) Enter y and press Enter to restart the system.

Sample Output:

```
admin:utils system restart
*** WARNING ***
Please make sure database replication setup is complete. Use the command 'utils dbreplication runtimestate' to get the current status.
If database replication setup is in progress, restarting the server may leave database replication unable to complete.
Do you really want to restart ?
Enter (yes/no)? yes
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
```
Stopping Service Manager...
- Service Manager shutting down services... Please Wait

What to do next
- Enter `utils service list` to verify list of all services and their states.
- Enter `show network eth0 detail` to verify the new domain name.
- Post-Change Tasks and Verification, on page 35.

Post-Change Tasks and Verification
Verify if the IP address, hostname, or domain name changes that were made to your deployment are implemented successfully.

Note
If you do not receive the results that you expect when you perform these tasks, do not continue with this procedure. Resolve any problems that you find, and then continue.

Procedure

Step 1
Check the active ServerDown alerts to ensure that all servers in the Cisco Finesse cluster nodes are active and available. For more information, see Step 1, on page 28 of the Pre-Change Tasks, on page 28.

Step 2
Check the DB replication status on all the Cisco Finesse cluster nodes to ensure all servers are replicating database changes successfully. For more information, see Step 2, on page 28 of the Pre-Change Tasks, on page 28.

Step 3
Check network connectivity and DNS server configuration by running the `utils diagnose module validate_network` command on all the Cisco Finesse cluster nodes.

Step 4
Start a manual DRS backup to ensure that all the Cisco Finesse cluster nodes and active services are backed up successfully.

Step 5
Enable SSO and perform the following tasks.
  a) Re-generate the SAML certificate.
  b) Re-establish trust relationship between Identity Provider (IdP) and Cisco Identity Service (IdS).
  c) If the components are registered earlier, then
     - Re-register all the SSO components.
     - Perform the SSO Test to check if all the SSO components are registered. Verify that the test is successful for each component.

Step 6  Regenerate and upload the following certificates that contain new hostname or domain name.
   • CA-signed certificate to Cisco Finesse.
   • Cisco Finesse tomcat certificate to CTI server and third-party server (if required).
   • Cisco Finesse tomcat-trust certificate to Cisco Unified Intelligence Center (CUIC) and Live Data.
   • Cisco Finesse tomcat certificate to Customer Collaboration Platform as tomcat-trust.

Step 7  Update Cross-Origin Resource Sharing (CORS) requests for Cisco Finesse, CUIC, and Live Data.

Step 8  Enable Shindig whitelist to add Cisco Finesse new FQDN for Cisco Finesse, CUIC, and Live Data.

Step 9  Verify and update Finesse desktop layout with new FQDN for resource loading.

Step 10 Update Unified CCE inventory with Cisco Finesse IP address.

From Step 6 to Step 10, after you complete each step, you must restart the services to reflect new changes, and then proceed to the next step.
Manage Call Variables Layouts

Call Variables Layouts

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

• Each layout has a name (required) and description (optional).

• You can change the name and description of the default Call Variables Layout.

• You cannot delete the default Call Variables Layout.

• Finesse appends (Default) to the name of the default Call Variables Layout.

• To display a custom Call Variables Layout, in the Unified CCE routing script set the user(Layout ECC variable to the name of a configured Call Variables Layout. In this case, if no custom layouts match the user.Layout value (or no custom layouts are configured), Finesse displays the default layout.

• Finesse retains the custom layout as specified by the user.Layout ECC variable on CTI server failover. During PG failover, Finesse changes the active call layout to the default layout while retaining the call variables and time indicators.

Call Variables

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

• BACampaign
• BAAccountNumber
• BAResponse
• BStatus
• BADialedListID
• BATimeZone
• BABuddyName

Columns can be empty.

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

• queueNumber
• queueName
• callKeyCallId
• callKeyPrefix
• callKeySequenceNum
• wrapUpReason

---

**Note**

The callKeyPrefix indicates the day when the call was routed.

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

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

---

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

---

**Edit Call Variables**

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

Procedure

Step 1 From the Manage Call Variables Layouts gadget:
  • Click **New** to create a new Call Variables Layout.
  • Choose a layout from the list and click **Edit** to modify an existing Call Variables Layout (or click **Delete** to remove it).

Step 2 Under **Create New Layout** (or under Edit <layout name> when editing an existing layout):
  • Enter a name for the Call Variables Layout (maximum 40 characters).
  • Enter a description of the Call Variables Layout (maximum 128 characters).

Step 3 Under Call Header Layout:
  • Enter the display name that you want to appear in the header of the Call Control gadget on the Finesse desktop. For example, Customer Name (maximum 50 characters).
  • From the drop-down list, choose the call variable or Outbound Option ECC variable that you want to appear in the header. For example, callVariable3 (maximum 32 characters).

Step 4 In the Call Body Left-Hand Layout and Call Body Right-Hand Layout areas:
  a) Click **Add Row** to add a new row (or click the “X” to delete a row).
  b) For each row:
     • Enter the display name that you want to appear on the desktop. For example, Customer Name (maximum 50 characters).
Enter the corresponding call variable or Outbound Option ECC variable from the drop-down list (maximum 32 characters).

Step 5  Select up to five call variables using the check box. The selected call variables are displayed in agent call popover and supervisor active call details.

Note  If you do not select any call variables, the first two call variables from the Call Body Left-Hand layout area will be displayed in the agent call popover and supervisor active call details. If there are no call variables in the Left-hand layout area, then the call variables in the Right-Hand Layout will be selected.

Step 6  Turn on the toggle switch to enable the edit option for a specific call variable. By default, this option is turned off.

Note  • Call variable (callVariable1 to callVariable10) values are editable.
       • ECC variable values are editable.
       • Amongst BA variables (campaign-based outbound calls), only BAResponse value is editable.

Step 7  Click **Save** to save the changes, or **Cancel** to discard the changes.

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

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

---

**Call Variables Popover**

In the call layout popover configuration, you can configure the call header and up to five call variables in the Call Variables Layout. These variables are displayed in the agent's call popover and active call details in the Team Performance gadget for a supervisor.

If you do not select any call variables, the first two call variables from the Call Body Left-Hand layout area will be displayed in the agent call popover and supervisor active call details. If there are no call variables in the Left-hand layout area, then the call variables in the Right-Hand Layout will be selected.

In upgrade scenarios, by default, the first two call variables will be displayed in the agent call popover and supervisor active call details. You can modify the configuration of the popover variables to improve the agent and supervisor experience.
Add ECC Variables to Call Variables Layout

**Procedure**

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

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

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

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

Assign Call Variables Layouts

**Procedure**

**Step 1** In CCE Configuration Manager, create an ECC variable called **user.Layout** in the Expanded Call Variable list.

**Note** If a user.layout and a user.Layout are specified, Finesse will prioritize user.layout over user.Layout. If the layout specified in the user.Layout or user.layout is not found, Finesse uses the Default layout.

**Step 2** Add **user.Layout** to the CCE routing script. Use a Set Variable node in an appropriate place in the script to set the value of user.Layout to the name of the call variables layout to display. The layout name should match the name of a call variables layout that was created on the Call Variables Layout tab in Finesse Administration.

Manipulate Call Variables Layouts with a Workflow

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

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

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

Cisco Finesse Administration Guide, Release 12.5(1)
Manipulate Call Variables Layouts with a Workflow
CHAPTER 5

Manage Desktop Layout

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

Important

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

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

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

• Gadgets and Components, on page 44
• Finesse Desktop Layout XML, on page 44
• Default Layout XML, on page 45
• Update Default Desktop Layout, on page 47
• Drag-and-Drop and Resize Gadget or Component, on page 48
• Customize Desktop Properties, on page 49
• Horizontal Header, on page 51
• Customize Title and Logo in the Header, on page 51
• alternateHosts Configuration, on page 52
• Headless Gadget Configuration, on page 53
• Customize Icons in Left Navigation Bar, on page 53
• XML Schema Definition, on page 66
• Live Data Reports, on page 69
Gadgets and Components

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

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

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

Third-party gadgets are hosted on the Cisco Finesse server using the 3rdpartygadget web application or on an external web server. Gadgets can make REST requests to services hosted on external servers using the Cisco Finesse JavaScript Library API. To avoid browser cross-origin issues, REST requests are proxied through the backend Shindig web application. Third-party gadgets must implement their own authentication mechanisms for third-party REST services.

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

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

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

Components are listed in the desktop layout using the <component> tag. Currently, the layout validations prevent custom components from being created. Hence, only default components are allowed in the desktop layouts. The default desktop functionalities are currently registered as components to provide flexibility and to reduce the load on the server.

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

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

Actions on the Manage Desktop Layout gadget are as follows.

- Edit the code using any of the following editors:
  - Text Editor
  - XML Editor

- View Default Layout - Displays the Cisco Finesse default layout.
• **Restore Default Layout** - Restores the Cisco Finesse desktop to the default layout.
• **Save** - Saves your configuration changes.
• **Revert** - Retrieves and applies the most recently saved desktop layout.

### Default Layout XML

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

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

---

**Note**

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

Both the editors support the following features:

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

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

Optional Live Data gadgets in the layout XML are commented out. After you install and configure Live Data, remove the comment tags from the reports that you want to appear on the desktop.

Following are the updates available in the default layout XML for Finesse desktop:

- Sample configurations for customizing desktop properties are added to the default layout (**Desktop Layout**) and team-specific layout (**Team Resources > Desktop Layout**).

  For upgraded layouts, sample configurations for customizing desktop properties do not appear by default. The administrator must copy the XML from the **View Default Layout** and add to the respective custom layouts.

- Horizontal Header is available in the layout configuration and the Header can be customized.

- Title and Logo of Finesse desktop can be customized.

- Desktop Chat, TeamMessage, Dialer, Agent Identity, and Non-Voice State Control are added as part of the header component.

  For upgraded layouts, TeamMessage and Desktop Chat will not appear by default. The XML must be copied from the default layout and added to the respective custom layouts. See *Cisco Finesse Installation & Upgrade Guide*. 

---
• Vertical tabs in Finesse desktop are moved to collapsible left navigation bar for which the icons can be customized.

• Support for inbuilt java script components has been added.

• The ID attribute (optional) is the ID of the HTML DOM element used to display the gadget or component. The ID should start with an alphabet and can contain alpha numeric characters along with hyphen(-) and underscore(_). It can be set through the Finesse Administrative portal and has to be unique across components and gadgets.

• The managedBy attribute (optional) for Live Data gadgets defines the gadgets which manage these Live Data gadgets. The value of managedBy attribute for Live Data gadgets is team-performance. This means that the rendering of the gadget is managed by the Team Performance gadget. These gadgets are not rendered by default, but will be rendered when the options Show State History and Show Call History are selected in the Team Performance gadget.

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

• The Hidden attribute (optional) is used to support headless gadgets. When an attribute is set to "hidden=true", then the gadget is loaded by the container, but will not be displayed. The default value set for the attribute is "false".

• maxRows is changed from being a query parameter to an attribute.

  Example of maxRows being a query parameter:
  
  <gadget id="team-performance" maxRows="5">/desktop/scripts/js/teamPerformance.js</gadget>

  Example of maxRows being an attribute:

  <gadget id="team-performance" maxRows="5">/desktop/scripts/js/teamPerformance.js</gadget>

  During an upgrade it will be removed from the URL of the team performance gadget and added as an attribute. The maxRows attribute (optional) is used to adjust the height of the Team Performance gadget. If there are multiple instances of the Team Performance gadget, each instance height can be set by using this attribute. During an upgrade the height of the team performance gadget will be retained. By default the maxRows attribute value is set to 10 rows.

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

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Component ID</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title and Logo</td>
<td>cd-logo</td>
<td>&lt;url&gt;/desktop/scripts/js/logo.js&lt;/url&gt;</td>
</tr>
<tr>
<td>Voice State Control</td>
<td>agent-voice-state</td>
<td>&lt;url&gt;/desktop/scripts/js/agentvoicestate.component.js&lt;/url&gt;</td>
</tr>
<tr>
<td>Non-voice state control</td>
<td>nonvoice-state-menu</td>
<td>&lt;url&gt;/desktop/scripts/js/nonvoice-state-menu.component.js&lt;/url&gt;</td>
</tr>
<tr>
<td>TeamMessage</td>
<td>broadcastmessagepopover</td>
<td>&lt;url&gt;/desktop/scripts/js/teammessage.component.js&lt;/url&gt;</td>
</tr>
</tbody>
</table>
Update Default Desktop Layout

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

Note

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

The version tag of Desktop Layout XML cannot be edited.

Procedure

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

Example:

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

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

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

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

```xml
<gadgets>
  <gadget>https://<ipAddress>/gadgets/<gadgetname>.xml</gadget>
</gadgets>
```
Replace `<ipAddress>` with the IP address of the server where the gadget resides.

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

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

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

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

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

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

---

**Drag-and-Drop and Resize Gadget or Component**

The administrator can configure the drag-and-drop and resize gadget or component features for the agents and supervisors to customize their Finesse desktop.

- The drag-and-drop feature allows the agents or supervisors to drag (and drop) the gadget or the component to the required position on the desktop layout.
- The resize feature allows the agents or supervisors to shrink or expand the gadget or the component to a custom size on the desktop layout.
By default, the drag-and-drop and resize features are disabled. The administrator must set the enableDragDropAndResizeGadget desktop property value as true to enable these features.

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

• Default layout (Desktop Layout)—In the Text Editor, remove the comment (<!— and -->) from the enableDragDropAndResizeGadget code snippet and enter the value as true to add these features to the desktop layout. For more information, see Customize Desktop Properties, on page 49.

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

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

• Team-specific layouts (Manage Team Resources > Desktop Layout)—Select a specific team and then in the Text Editor, remove the comment (<!— and -->) from the enableDragDropAndResizeGadget code snippet and enter the value as true to add these features to the team desktop layout. For more information, see Customize Desktop Properties at Team Level, on page 100.

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

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

• For upgraded layouts, sample configuration for customizing desktop property (enableDragDropAndResizeGadget) does not appear by default in the Desktop Layout. The administrator must copy the XML from the View Default Layout and add to the respective custom layouts.

• For new layouts, sample configuration for customizing desktop property (enableDragDropAndResizeGadget) appears by default in the Desktop Layout.

• The administrator can also use the CLI and set the utils finesse set_property desktop enableDragDropAndResizeGadget to true to enable these features. For more information, see Desktop Properties.

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

• These features are not applicable for gadgets that do not have a defined title. For more information, see Gadget Limitations section in Cisco Finesse Web Services Developer Guide at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.


**Customize Desktop Properties**

You can customize the Finesse desktop properties.
Procedure

**Step 1**  
Click Desktop Layout.

**Step 2**  
Select from the following editors:
- Text Editor
- XML Editor

**Step 3**  
Enter the desktop property name in the config key tag.

**Step 4**  
Enter the possible value of the desktop property in the value tag.

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

```xml
<!-- <config key="enableDragDropAndResizeGadget" value="false"/> -->
<!-- <config key="wrapUpCountDown" value="true"/> -->
<!-- <config key="desktopChatAttachmentEnabled" value="true"/> -->
<!-- <config key="forceWrapUp" value="true"/> -->
```

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

The following table lists the supported desktop properties:

<table>
<thead>
<tr>
<th>Config Key</th>
<th>Value</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enableDragDropAndResizeGadget</td>
<td>true/false</td>
<td>false</td>
</tr>
<tr>
<td>enableShortCutKeys</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>forceWrapUp</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>wrapUpCountDown</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>showWrapUpTimer</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>desktopChatAttachmentEnabled</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>desktopChatMaxAttachmentSize</td>
<td>Range: 1—10 (MB)</td>
<td>5</td>
</tr>
<tr>
<td>desktopChatUnsupportedFileTypes</td>
<td>Unsupported file formats include comma-separated valid file extensions. For example: .exe, .sh</td>
<td>.exe, .msi, .sh, .bat</td>
</tr>
<tr>
<td>showAgentHistoryGadgets</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>showActiveCallDetails (for Supervisor Only)</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>pendingDTMFThresholdCount</td>
<td>Range: 1—20</td>
<td>20</td>
</tr>
<tr>
<td>dtmfRequestTimeoutInMs</td>
<td>Range: 1000—200000 (1 to 200 seconds)</td>
<td>5000 (5 seconds)</td>
</tr>
</tbody>
</table>
To enable the following Finesse desktop properties in Cisco Finesse, Release 12.5(1), install Cisco Finesse Release 12.5(1) ES1 COP or higher.

- pendingDTMFThresholdCount
- dtmfRequestTimeoutInMs

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

**Step 5**

Click **Save**.

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

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

---

**Horizontal Header**

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

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

---

**Note**

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

---

**Customize Title and Logo in the Header**

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

**Procedure**

**Step 1**

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

Step 3 Enter the product name in the config value tag with title key.

Step 4 Upload the logo file just like any third-party gadget.
For more information, see section Upload Third-Party Gadgets in Cisco Finesse Admin Guide.

Step 5 Enter the URL of the logo file in the config value tag with logo key.

**Example:**
```xml
<configs>
  <!-- The Title for the application which can be customised.-->
  <config value="product.full-name" Key="title"/>
  <!-- The logo file for the application-->
  <!--<config key="logo" value="/3rdpartygadgets/<some_sample_image>"/>-->
</configs>
```

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

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

---

**alternateHosts Configuration**

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

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

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

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

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

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

When the gadget is specified with a relative URL, for example: `<gadget>/3rdpartygadgets/relative_path</gadget>`, the `alternateHosts` attribute does not apply and is ignored by the Cisco Finesse desktop.
If the host serving the gadget fails after the Cisco Finesse desktop was successfully loaded, the desktop must be refreshed in order to load the gadget from an alternate host. The gadget does not implement its own failover mechanism.

**Headless Gadget Configuration**

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

**Customize Icons in Left Navigation Bar**

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

**Procedure**

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

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

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

**Example:**

```xml
<tab>
    <id>myHistory</id>
    <icon>/3rdpartygadgets/some_sample_image</icon>
    <label>finesse.container.tabs.agent.myHistoryLabel</label>
    <columns>
        <column>
            <!-- The following gadgets are used for viewing the call history and state history of an agent. -->
            <gadgets>
                <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=280&amp;viewId=5FA44C6F930C4A64A6775B21A17EED6A&amp;filterId=agentTaskLog.id=CL%20teamName</gadget>
                <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=280&amp;viewId=5FA44C6F930C4A64A6775B21A17EED6A&amp;filterId=agentTaskLog.id=CL%20teamName</gadget>
            </gadgets>
        </column>
    </columns>
</tab>
```
The file size that can be uploaded in the left navigation bar as custom icons is 25 pixels by 25 pixels. The maximum width of the tab title in the left navigation bar must be 80 pixels or less. The file types supported are .svg, .png, .gif, and .jpeg/jpg.

Customize Icons for Gadgets

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

Procedure

Step 1 Click Desktop Layout.
Step 2 Select from the following editors:

• Text Editor
• XML Editor
Step 3
Enter the value of the icon in the icon tag. Get the icon name from the List of Icons, on page 56. The icon name is located on the right of the icon image. For example, search.

Note
Icon name is case sensitive. Enter the icon name exactly as displayed in the List of Icons, on page 56.

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

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

The following are the icons for Actions.

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

The following are the icons for Audio.
The following are the icons for Camera.

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

The following are the icons for Chat.

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

Cisco Finesse Administration Guide, Release 12.5(1)
The following are the icons for Collaboration.

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

The following are the icons for Contacts.
The following are the icons for Content.

- attachment
- link
- document
- create-page
- move-page
- notes
- image
- folder
- export
- import

The following are the icons for Editor.

- contact
- add-contact
- remove-contact
- directory
- contact-card
- star
The following are the icons for Email.

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

The following are the icons for Hardware.
The following are the icons for Media.

- image
- sound
- music
- graph
- text
- tables
- zip

The following are the icons for Navigation.
The following are the icons for Network.

- wifi
- proximity
- proximity-not-connected
- bluetooth
- bluetooth-contained
- bluetooth-outline
- ethernet
- no-signal
- signal-1
- signal-2

The following are the icons for Notifications and Alerts.
The following are the icons for Phone.

- calls
- other-phone
- call-log
- work
- desk-phone
- voicemail
- callback
- redial
- DND
- swap-calls

The following are the icons for Sources.

- incoming-call
- outgoing-call
- missed-call
- rtpx
- rtpx-rtpx-duplex
- speed-dial
- off-hook
- alerting
- parked
### List of Icons

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

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>settings</td>
<td>animation</td>
<td>reset</td>
</tr>
<tr>
<td>sliders</td>
<td>accessibility</td>
<td>backup-data</td>
</tr>
<tr>
<td>user</td>
<td>setup-assistant</td>
<td>bug</td>
</tr>
<tr>
<td>admin</td>
<td>tools</td>
<td>lock-contain</td>
</tr>
<tr>
<td>activities</td>
<td>hue</td>
<td>ground</td>
</tr>
<tr>
<td>profile-settings</td>
<td>brightness</td>
<td>storage</td>
</tr>
<tr>
<td>ringer-settings</td>
<td>volume</td>
<td>data-usage</td>
</tr>
<tr>
<td>language</td>
<td>call-rate</td>
<td>numbered-inputs</td>
</tr>
<tr>
<td>wallpaper</td>
<td>vibrate</td>
<td>numbered-outputs</td>
</tr>
<tr>
<td>manage-cables</td>
<td>time</td>
<td></td>
</tr>
</tbody>
</table>

The following are the icons for Video Controls.
The following are the icons for Miscellaneous Icons.

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

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

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
  <!-- definition of version element -->
  <xs:element name="version">
    <xs:simpleType>
      <xs:restriction base="xs:double">
        <xs:pattern value="[0-9.]+" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <!-- The below elements are for common desktop header and configs -->
  <!-- Copied from:
  <!-- If the common-desktop XSD changes, this too needs to be updated -->
  <!-- Only difference is that, column has been renamed to headercolumn, since column is
already there in finesse desktop layout -->
  <xs:complexType name="configs">
    <xs:sequence>
      <xs:element name="config" type="config" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="config">
    <xs:attribute name="key">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:pattern value="[a-zA-Z]*" />
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="value" type="xs:string" />
  </xs:complexType>
  <xs:complexType name="header">
    <xs:choice>
      <xs:sequence>
        <xs:element name="leftAlignedColumns" type="listOfColumns" minOccurs="1" maxOccurs="1" />
        <xs:element name="rightAlignedColumns" type="listOfColumns" minOccurs="0" maxOccurs="1" />
      </xs:sequence>
    </xs:choice>
  </xs:complexType>
  <xs:complexType name="component">
    <xs:sequence>
      <xs:element name="url" type="xs:string" minOccurs="1" maxOccurs="1" />
      <xs:element name="stylesheet" type="xs:string" minOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="id" use="required">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:pattern value=".+
```
<xs:simpleType name="role">
    <xs:restriction base="xs:string">
        <xs:enumeration value="Agent" />
        <xs:enumeration value="Supervisor" />
        <xs:enumeration value="Admin" />
    </xs:restriction>
</xs:simpleType>

<!-- definition of simple elements -->
<xs:element name="id">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:pattern value="[a-zA-Z](\[-_:.a-zA-Z0-9\])*" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>
<xs:element name="label">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="1" />
            <xs:pattern value="[^\r\n\s]*" />
            <!-- This regex restricts the label string from carriage returns or newline characters -->
        </xs:restriction>
    </xs:simpleType>
</xs:element>
<xs:element name="icon" type="xs:anyURI" />
<xs:element name="gadget">
    <xs:complexType>
        <xs:simpleContent>
            <xs:extension base="restrictWhiteSpaces">
                <!-- <xs:attribute name="staticMessage" type="xs:string"/> -->
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>
</xs:element>
</xs:complexType>
</xs:element>
<xs:simpleType>
  <xs:restriction base="xs:string">
    <xs:patter value="[a-zA-Z]([-_a-zA-Z0-9]*)" />
  </xs:restriction>
</xs:simpleType>

<xs:attribute name="alternateHosts" type="xs:string" />
<xs:attribute name="managedBy" type="xs:string" />
<xs:attribute name="hidden" type="xs:boolean" />
</xs:extension>

<xs:complexType>
  <xs:attribute name="role" type="role" />
  <xs:attribute name="gadgets">
    <!-- Grouping of a set of gadgets -->
    <xs:complexType>
      <xs:sequence minOccurs="0" maxOccurs="unbounded">
        <!-- No limit to number of gadget URIs for now -->
        <xs:element ref="gadget" />
        <!-- URI of the gadget xml -->
      </xs:sequence>
    </xs:complexType>
  </xs:attribute>
</xs:complexType>

<xs:element name="restrictWhiteSpaces">
  <xs:restriction base="xs:anyURI">
    <xs:minLength value="1" />
    <xs:pattern value="\S+" />
    <!-- This regex restricts anyURI from containing whitespace within -->
  </xs:restriction>
</xs:simpleType>

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

<xs:element name="columns">
  <!-- Grouping of a set of columns -->
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="column" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
</xs:element>

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

<xs:element name="tab">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="id" />
      <!-- Id of the tab selector in the desktop -->
    </xs:sequence>
  </xs:complexType>
</xs:element>
Live Data Reports

Prerequisites for Live Data

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

- Download the Live Data reports from Cisco.com and import them into Cisco Unified Intelligence Center. Verify that the reports are working in Unified Intelligence Center.

- You must use HTTPS for both Cisco Unified Intelligence Center and Finesse. The default setting for both after a fresh installation is HTTPS.

- Ensure that user integration synchronization is enabled for Cisco Unified Intelligence Center.


- For HTTPS, you must upload security certificates to the Finesse, Cisco Unified Intelligence Center and Live Data servers. Finesse, Cisco Unified Intelligence Center, and Live Data 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.

## Add Live Data Reports to Finesse

To add 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>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>If you have customized the Finesse desktop layout.</td>
</tr>
<tr>
<td>Add Live Data reports to team layout</td>
<td>To the desktop layout for specific teams only.</td>
</tr>
</tbody>
</table>

### Note

The line breaks and spaces that appear in the example text of the procedures are provided only for readability and must not be included in the actual code.

### 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 rows, 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 Default Desktop Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop.
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 and do not have a custom desktop layout, click **Restore Default Layout** on the Manage Desktop Layout gadget and then follow the steps in this procedure.

**Procedure**

**Step 1** Click **Desktop Layout**.

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

- Text Editor
- XML Editor

**Step 3** Add the reports to the desktop layout:

- **Text Editor** - Remove the comment (<!-- and -->) from each report that you want to add to the desktop layout and then replace “my-cuic-server” with the FQDN of the Cisco Unified Intelligence Center Server.
- **XML Editor** - To add a gadget, select `<layout><tabs><gadgets>Add<gadget>` and enter the required parameters such as Id, alternate hosts, managed by, maximum rows, and the hidden details.

**Note** You must select the reports that match the protocol (HTTPS) your agents use to access the Cisco Finesse desktop.

**Step 4** Optionally, change the gadget height.

**Example:**

The height that is 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, replacing 310 with 400:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
gadgetHeight=400&viewId_1=99E6C8E210000141000000D80A0006C4&
filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
filterId_2=agent.id=CL%20teamName
</gadget>
```

To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

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

**Note** In a dynamic type gadget, multiple viewId parameters is not supported. Check the URL in the error message before proceeding to save the default XML layout. The name value "type=dynamic must be part of the gadget URL.

**Note** If you select a TDM agent in the Team Performance Gadget, the recent state history data of the selected agent is not populated.
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.

To add the Live Data report gadgets to a custom desktop layout.

Procedure

**Step 1**  
Click the Desktop Layout tab.

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

- Text Editor
- XML Editor

**Step 3**  
Copy the XML code for the HTTPS report you want to add from the Finesse default layout XML.

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

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&filterId_2=agent.id=CL%20teamName</gadget>
```

**Step 4**  
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:

```
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&filterId_2=agent.id=CL%20teamName</gadget>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
  </tabs>
</layout>
```

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

**Step 6**  
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:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
gadgetHeight=400&viewId_1=99E6C8E210000141000000D80A0006C4&
filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
filterId_2=agent.id=CL%20teamName
</gadget>
```

To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

**Step 7** Click Save.

---

### 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.

To add the Live Data report gadgets to the desktop layout of a specific team:

**Procedure**

**Step 1** Click the Desktop Layout tab.

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

- Text Editor
- XML Editor

**Step 3** Copy the XML code for the HTTPS report you want to add from the Finesse default layout XML.

**Example:**

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

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
filterId_2=agent.id=CL%20teamName
</gadget>
```

**Step 4** Click Team Resources.

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

**Step 6** In the Resources for `<team name>` area, click the Desktop Layout tab.

**Step 7** Check the Override System Default check box.

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

- Text Editor
- XML Editor

**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>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
filterId_1=agent.id=CL%20teamName&
viewId_2=9AB7848B10000141000001C50A0006C4&
filterId_2=agent.id=CL%20teamName
</gadget>
    </tab>
  </tabs>
</layout>
```

Step 10 Replace “my-cuic-server” with the FQDN of your Cisco Unified Intelligence Center 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_1=99E6C8E210000141000000D80A0006C4&
filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
filterId_2=agent.id=CL%20teamName
</gadget>
```

To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). 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.

---

**Modify Live Data Stock Reports for Finesse**

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** Click the Desktop Layout.

**Step 2** Select from the following editors:
- Text Editor
- XML Editor

**Step 3** 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_1=99E6C8E210000141000000D80A0006C4&filterId_1=agent.id=Cl%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&filterId_2=agent.id=Cl%20teamName</gadget>
```

**Step 4** 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 5** Copy the permalink of the customized report from the **HTML Link** field, and paste it in a text editor. Then copy the viewId value from this link into the desired view.

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

```plaintext
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmlx?viewId=5C90012F1000014000000830A4E5B33&linkType=htmlType&viewType=Grid
```

**Step 6** Replace the desired viewId value in the gadget URL with the viewId value from the permalink of the customized report.


**Step 7** Replace my-cuic-server with the FQDN of the Cisco Unified Intelligence Center Server.

**Step 8** Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click Save.

---

**Configure Live Data Reports with Multiple Views**

Cisco Unified Intelligence Center allows you to display multiple Live Data reports or views on a single gadget. Agents can select the desired view to display from a drop-down list on the gadget toolbar, which lists up to five report views in **Report Name - View Name** format.
This procedure describes how to add multiple Live Data views to the Finesse desktop layout using the viewId_n and filterId_n keys. You can specify up to five report views to appear in your gadget. The first view among the five is the default view. There is no defined order for how the remaining views are displayed.

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

---

**Note**

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

---

**Procedure**

**Step 1**

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

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

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

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

**Example:**

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

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

**Step 2**

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

**Example:**

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

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

**Step 3**

To update the URL to refer to a different report view, populate the viewId_1 value (after the equal sign) with the desired viewId obtained in step 1.

**Example:**

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

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

**Step 4**

For each additional view you want to include:

a) At the end of the URL, copy and paste the viewId_1 and agentId_1 strings with a leading ampersand.
Example:

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

b) Update the copied `viewId_1` and `filterId_1` in the URL to the next available integer (in this example, `viewId_2` and `filterId_2`).

Example:

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

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

Example:

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

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

- Agent Reports: `filterId_N=agent.id=CL%20teamName`
- Agent Skill Group Reports: `filterId_N=agent.id=CL%20teamName`
- Skill Group Reports: `filterId_N=skillGroup.id=CL%20teamName`
- Precision Queue Reports: `filterId_N=precisionQueue.id=CL%20teamName`

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

**Step 6**
Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click Save.
Manage Phone Books

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

- Phone Books and Contacts, on page 79
- Add Phone Book, on page 80
- Edit Phone Book, on page 81
- Delete Phone Book, on page 81
- Import Contacts, on page 81
- Export Contacts, on page 82
- Add Contact, on page 83
- Edit Contact, on page 83
- Delete Contact, on page 83

Phone Books and Contacts

Finesse supports the following number of phone books:

- 10 global phone books
- 300 team phone books

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the phone book. It must be unique, and can be a maximum 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>
</tbody>
</table>
### Add Phone Book

#### Field | Explanation
--- | ---
Last Name | The last name of a contact. The last name can be a maximum of 128 characters. This field is optional.
First Name | The first name of a contact. The first name can be a maximum of 128 characters. This field is optional.
Number | The phone number for the contact. The phone number can be 1-32 characters long and cannot be blank.
Note | Optional text that describes the contact. The note can be a maximum of 128 characters.

#### Actions on the Manage Phone Books gadget:
- **New**: Add a new phone book or contact
- **Edit**: Edit an existing phone book or contact
- **Delete**: Delete a phone book or contact
- **Refresh**: Reload the list of phone books or contacts from the server
- **Import**: Import a list of contacts to the phone book
- **Export**: Export a list of contacts from the phone book

#### Add Phone Book

**Procedure**

**Step 1**
In the Manage Phone Books gadget, click **New**.

**Step 2**
In the **Name** field, enter a name for the phone book. 

*Note*  
Phone book names can be a maximum of 64 characters.

**Step 3**
From the **Assign To** drop-down, select **All Users** if the phone book is global or **Teams** if the phone book is available to specified teams.

**Step 4**
Click **Save**.
Edit Phone Book

Procedure

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

If you change the Assign To field from Teams to All Users, click **Yes** to confirm the change.

Delete Phone Book

Procedure

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

Import Contacts

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

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

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

<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>Note: The CSV file that contains the contacts to import must use Latin encoding.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>32</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td>128</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
The following is an example of a phone book CSV file:

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

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

---

**Note**

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

---

**Procedure**

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

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

**Step 3**
Click **Browse** and navigate to the location of the CSV file containing the contacts you want to import.

**Note**

The CSV file must use Latin encoding.

**Step 4**
Click **OK**.

---

**Export Contacts**

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

**Procedure**

**Step 1**
In the Manage Phone Books gadget, select the phone book that contains the contacts you want to export.

**Step 2**
Click **Export**.

**Step 3**
Click **Open** to open the CSV file in Excel, or click the **Save** drop-down list and choose **Save**, **Save as**, or **Save and open**.

**Step 4**
A message appears that gives you the option to view the downloaded file, open the folder into which the download was saved, view the Internet Explorer View Downloads window, or dismiss the message without viewing the file.
**Add Contact**

**Procedure**

**Step 1** In the Manage Phone Books gadget, select the phone book to which you want to add a contact. The List of Contacts for `<phone book name>` area appears.

**Step 2** Click New.

**Step 3** Complete the fields. The First Name, Last Name, and Note fields are optional and have a maximum length of 128 characters. The Number field is required and has a maximum length of 32 characters.

**Step 4** Click Save.

---

**Edit Contact**

**Procedure**

**Step 1** In the Manage Phone Books gadget, select the phone book that contains the contact you want to edit. The List of Contacts for `<phone book name>` area appears.

**Step 2** Select the contact you want to edit.

**Step 3** Click Edit.

**Step 4** Edit the fields that you want to change. The First Name, Last Name, and Note fields are optional and have a maximum of 128 characters. The Number field is required and has a maximum of 32 characters.

**Step 5** Click Save.

---

**Delete Contact**

**Procedure**

**Step 1** In the Manage Phone Books gadget, select the phone book that contains the contact you want to delete. The List of Contacts for `<phone book name>` area appears.

**Step 2** Select the contact that you want to delete.

**Step 3** Click Delete.
Step 4  Click Yes to confirm the deletion of the selected contact.
CHAPTER 7

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.

Reason code tables support search across reason codes and reason code labels. You can configure different reason codes with the same reason code label across various teams.

- Not Ready Reason Codes, on page 85
- Sign Out Reason Codes, on page 88
- Predefined System Reason Codes, on page 90
- Manage Reason Code Conflicts During Upgrade, on page 92
- Wrap-Up Reasons, on page 93

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 Type header to sort and display system or custom reason codes. 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).

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
</table>

| Reason Label | The label for the Not Ready reason code. The label has a maximum length of 40 characters and should be unique for each Not Ready reason code. Alphanumeric and special characters are supported. |
| Type | The type of reason code (System or Custom). The column is default and can be sorted to display both System reason codes and Custom reason codes. |
| Reason Code | A code for the Not Ready reason. The 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). |

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

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

---

**Note**

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

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

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

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

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).

---

**Note**

During a PG or CTI server failover, the pending state of an agent is not retained.
Add Not Ready Reason Code

Procedure

Step 1  In the Manage Reason Codes (Not Ready) gadget, click New.
Step 2  In the Reason Label box, enter a label for the reason code.
  Note  Not Ready reason code labels are limited to 40 characters.
Step 3  In the Reason Code box, an auto populated reason code is displayed. If you choose not to save the prepopulated reason code, you can enter your own reason code.
  Note  The code must be between 1 and 65532 and must be unique.
  Ensure there are no leading or trailing spaces.
Step 4  If the reason code is global, select the Global? check box. If the reason code is specific to a team, clear the Global? check box.
  Note  By default, the Global? check box is selected.
Step 5  Click Save.
  Note  The Finesse server removes leading or trailing spaces before saving the Reason Label in the database.

Edit Not Ready Reason Code

Procedure

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

Delete Not Ready Reason Code

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

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

**Step 2** Click **Delete**.

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

---

**Sign Out Reason Codes**

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

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

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

---

**Note**

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason Label</td>
<td>The label for the Sign Out reason code. The label has a maximum length of 40 characters and should be unique for each Sign Out reason code. Alphanumeric and special characters are supported.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of reason code (System or Custom). The column is default and can be sorted to display both System reason codes and Custom reason codes.</td>
</tr>
<tr>
<td>Reason Code</td>
<td>A code for the Sign Out 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>

**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

**Procedure**

| Step 1 | In the Manage Reason Codes (Sign Out) gadget, click **New**. |
| Step 2 | In the Reason Label box, enter a label for the reason code. Note: Sign Out reason code labels are limited to 40 characters. |
| Step 3 | In the Reason Code box, an auto populated reason code is displayed. If you choose not to save the prepopulated reason, you can enter your own reason code. Note: The code must be between 1 and 65535 and must be unique. Ensure there are no leading or trailing spaces. |
| Step 4 | If the reason code is global, select the **Global?** checkbox. If the reason code is specific to a team, clear the **Global?** checkbox. Note: By default, the **Global?** check box is selected. |
| Step 5 | Click **Save**. |

### Edit Sign Out Reason Code

**Procedure**

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

Delete Sign Out Reason Code

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

**Procedure**

**Step 1**  
In the Manage Reason Codes (Sign Out) gadget, select the Sign Out reason code that you want to delete.

**Step 2**  
Click Delete.

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

Predefined System Reason Codes

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

<table>
<thead>
<tr>
<th>System Reason Code</th>
<th>Reason Label</th>
<th>Reason Label Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>32767</td>
<td>Not Ready - Call Not Answered</td>
<td>Agent state changed because the agent did not answer the call.</td>
</tr>
<tr>
<td>32762</td>
<td>Not Ready - Offhook</td>
<td>The system issues this reason code in the following scenarios:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When the agent goes off-hook to place a call, the Finesse desktop changes the agent status to Not Ready with this reason code.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When the agent is in Ready state and a call is placed from the ACD (Automatic Call Distribution) line, the system issues this reason code.</td>
</tr>
</tbody>
</table>
|                    |                             | **Note**  
Reason Code—50006 is used in place of 32762 in Cisco Finesse Release 12.5(1) when used along with Unified CCE Release 12.5(1) or higher. |
<p>| 50001              | Logged Out - System Disconnect | The CTI OS client disconnected, logging the agent out.                                    |</p>
<table>
<thead>
<tr>
<th>Code</th>
<th>Reason Description</th>
<th>Reason Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>5002</td>
<td><strong>Logged Out - System Failure</strong></td>
<td></td>
</tr>
</tbody>
</table>
  A CTI OS component disconnected, causing the agent to be logged out or set to the Not Ready state. This could be due to closing the agent desktop application, heart beat timeout, or a CTI OS Server failure. |
| 5002  | **Not Ready - Connection Failure**                                                 |  
  The system issues this reason code when the agent is forcibly logged out in certain cases. |
| 5003  | **Logged Out - Device Error**                                                      |  
  Agent was logged out because the Unified CM reported the device out of service. |
| 5004  | **Logged Out - Inactivity Timeout**                                                |  
  Agent was logged out due to agent inactivity as configured in agent desk settings. |
| 5005  | **Not Ready - Non ACD Busy**                                                       |  
  For a Unified CCE agent deployment, where the Agent Phone Line Control is enabled in the peripheral and the Non ACD Line Impact is configured to impact agent state, the agent is set to Not Ready while talking on a call on the Non ACD line with this reason code. |
| 5006  | **Not Ready - Offhook**                                                            |  
  The system issues this reason code in the following scenarios:  
  - When the agent goes off-hook to place a call, the Unified CCE changes the agent status to Not Ready with this reason code.  
  - When the agent is in Ready state and a call is placed from the ACD (Automatic Call Distribution) line, the system issues this reason code.  
  **Note**  This reason code is used from Cisco Finesse Release 12.5(1) along with Unified CCE Release 12.5(1) or higher. |
| 5010  | **Not Ready - Call Overlap**                                                       |  
  Agent was set to Not Ready state because the agent was routed two consecutive calls that did not arrive. |
| 5020  | **Logged Out - Queue Change**                                                      |  
  Agent was logged out when the agent's skill group dynamically changed on the Administration & Data Server. |
| 5030  | **Logged Out - Device Conflict**                                                    |  
  If an agent is logged in to a dynamic device target that is using the same Dialed Number (DN) as the PG static device target, the agent is logged out. |
| 5040  | **Logged Out - Mobile Agent Call Fail**                                            |  
  Mobile agent was logged out because the call failed. |
| 5041  | **Not Ready - Mobile Call Not Answered**                                           |  
  Mobile agent state changed to Not Ready because the call fails when the mobile agent's phone line rings busy. |
| 5042  | **Logged Out - Mobile Agent Disconnect**                                           |  
  Mobile agent was logged out because the phone line disconnected while using nailed connection mode. |
### Manage Reason Code Conflicts During Upgrade

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

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

**Note**

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

**Note**

When performing an upgrade from an earlier version in a Unified CCE deployment, modify the following custom reason codes: 999, 255, 20001, 20002, 20003, and 50041. This is done to avoid conflict with the system reason codes.

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>65535</td>
<td>Not Ready - System Reinitialized</td>
<td>Agent reinitialized (used if peripheral restarts).</td>
</tr>
<tr>
<td>65534</td>
<td>Not Ready - System Reset</td>
<td>PG reset the agent, normally due to a PG failure.</td>
</tr>
<tr>
<td>65533</td>
<td>Not Ready - Extension Modified</td>
<td>An administrator modified the agent's extension while the agent was logged in.</td>
</tr>
<tr>
<td>20001</td>
<td>Not Ready - Starting Force Logout</td>
<td>Places the agent in the Not Ready state first before forcefully logging them off.</td>
</tr>
<tr>
<td>20002</td>
<td>Logged Out - Force Logout</td>
<td>Forces the logout request; for example, when Agent A attempts to log in to Cisco Agent Desktop and Agent B is already logged in under that agent ID, Agent A is asked whether or not to force the login. If Agent A answers yes, Agent B is logged out and Agent A is logged in. Reports then show that Agent B logged out at a certain time with a reason code of 20002 (Agent B was forcibly logged out).</td>
</tr>
<tr>
<td>20003</td>
<td>Not Ready - Agent Logout Request</td>
<td>If not already in the Logout state, request is made to place agent in the Not Ready state. Then logout request is made to log agent out.</td>
</tr>
<tr>
<td>999</td>
<td>Not Ready - Supervisor Initiated</td>
<td>The system issues this reason code when the agent’s state is forcibly changed to Not Ready by the Supervisor.</td>
</tr>
<tr>
<td>999</td>
<td>Logged Out - Supervisor Initiated</td>
<td>The system issues this reason code when the agent’s state is forcibly changed to Logout by the Supervisor.</td>
</tr>
<tr>
<td>255</td>
<td>Logged Out - Connection Failure</td>
<td>The system issues this reason code when the agent is forcibly logged out when there is a connection failure between the Cisco Finesse Desktop and the Cisco Finesse Server.</td>
</tr>
</tbody>
</table>
All conflicting reason codes are highlighted. To edit, select each conflicting reason code and click Edit. The Edit Reason Code area appears. Select the reason code from the available options listed or enter any other code you wish. The code must be unique to the particular category (Not Ready or Sign Out).

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

**Wrap-Up Reasons**

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

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

Use the Manage Wrap-Up Reasons gadget to view, add, edit, or delete Wrap-Up reasons. Click the Reason Label header to sort the Wrap-Up reasons in ascending or descending order. 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 1500 team Wrap-Up reasons. No more than 100 Wrap-Up reasons can be assigned to any one team.

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

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.

---

**Note**

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

If showWrapUpTimer is set to true then timer is displayed.

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

For Example, if you set the timer to 30 seconds, then by default the timer starts from 30 and ends on zero. The default behavior can be changed by setting the wrapUpCountDown property to false.

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

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

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

Actions on the Manage Wrap-Up Reasons gadget:

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

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

**Add Wrap-Up Reason**

**Procedure**

**Step 1**

In the Manage Wrap-Up Reasons gadget, click **New**.

**Step 2**

In the Reason Label field, add a label for the Wrap-Up reason.

**Note**

Wrap-Up reason labels are limited to 39 bytes.
Step 3 If the Wrap-Up reason is global, select the Global? check box. If the Wrap-Up reason is specific to a team, clear the Global? check box.

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

Step 4 Click **Save**.

---

**Edit Wrap-Up Reason**

**Procedure**

**Step 1** In the Manage Wrap-Up Reasons gadget, select the Wrap-Up reason that you want to edit.

**Step 2** Click **Edit**.

The Edit Wrap-Up Reason area appears.

**Step 3** In the Wrap-Up Reason Label field, enter the new label for the Wrap-Up reason. If you want to change who has access to the Wrap-Up reason, select or clear the Global? check box.

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

---

**Delete Wrap-Up Reason**

**Procedure**

**Step 1** In the Manage Wrap-Up Reasons gadget, select the Wrap-Up reason that you want to delete.

**Step 2** Click **Delete**.

A question appears asking you to confirm that you want to delete the selected Wrap-Up reason.

**Step 3** Click **Yes** to confirm the deletion of the selected Wrap-Up reason.

---

**Force Wrap-Up Reason**

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

**Note** The Force Wrap-Up reason is enabled by default. Use the CLI commands to disable and enable this feature. For more information, see *Desktop Properties*.
Manage Reasons

Force Wrap-Up Reason
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 97
• Assign Phone Books and Reasons to Team, on page 98
• Unassign Phone Books and Reasons from Team, on page 99
• Assign Custom Desktop Layout to Team, on page 99
• Assign Workflows to Team, on page 102
• Unassign Workflows from Team, on page 102

Team Resources

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

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

<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 and unassign phone books to the team. Only phone books that are defined in the Manage Phone Books gadget as available to teams are available for assignment.</td>
</tr>
<tr>
<td>Reason Codes (Not Ready)</td>
<td>Use this tab to assign and unassign Not Ready reason codes to the team. Only Not Ready reason codes that are defined in the Manage Reason Codes (Not Ready) gadget as available to teams (not global) are available for assignment.</td>
</tr>
<tr>
<td>Reason Codes (Sign Out)</td>
<td>Use this tab to assign and unassign Sign Out reason codes to the team. Only Sign Out reason codes that are defined in the Manage Reason Codes (Sign Out) gadget as available to teams (not global) are available for assignment.</td>
</tr>
</tbody>
</table>
Assign Phone Books and Reasons to Team

**Actions on the Manage Team Resources Gadget**

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

**Note**

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

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

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

### Assign Phone Books and Reasons to Team

**Procedure**

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

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

**Step 3**
Click **Add**.

**Step 4**
Select one or more resources from the list to assign them to the team.

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

**Step 5**
When you finish assigning resources, click **Save**.
You can make changes on all resource tabs and then save them at the same time. If there is an error on one resource tab but not others, the changes on the tabs with no errors are saved while the changes on the tab with errors are not saved.

---

### Unassign Phone Books and Reasons from Team

**Procedure**

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

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

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

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

---

### Assign Custom Desktop Layout to Team

**Procedure**

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

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

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

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

The XML becomes editable.

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

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

For more information, see *Default Layout XML*.

**Step 5** Edit the XML.

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

The custom desktop layout replaces the default desktop layout for the team after 10 seconds. If a supervisor or agent is signed in when the change is saved, the change does not take effect on their desktop until the supervisor or agent signs out and signs in again.
If you clear the Override System Default checkbox, any changes you made to the XML are lost and the XML in the editing pane reverts to the default desktop layout XML.

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

Customize Desktop Properties at Team Level

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

Procedure

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

**Step 2**
Click Desktop Layout.

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

**Step 4**
Select from the following editors:
- Text Editor
- XML Editor

**Step 5**
Enter the desktop property name in the config key tag.

**Step 6**
Enter the possible value of the desktop property in the value tag.

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

```
<!-- <config key="enableDragDropAndResizeGadget" value="false"/> -->
<!-- <config key="wrapUpCountDown" value="true"/> -->
<!-- <config key="desktopChatAttachmentEnabled" value="true"/> -->
<!-- <config key="forceWrapUp" value="true"/> -->
```

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

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

For more information on Finesse CLIs, see Desktop Properties.

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

<table>
<thead>
<tr>
<th>Config Key</th>
<th>Value</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enableDragDropAndResizeGadget</td>
<td>true/false</td>
<td>false</td>
</tr>
<tr>
<td>enableShortCutKeys</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>Config Key</td>
<td>Value</td>
<td>Default Value</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------</td>
<td>---------------</td>
</tr>
<tr>
<td>forceWrapUp</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>wrapUpCountDown</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>showWrapUpTimer</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>desktopChatAttachmentEnabled</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>desktopChatMaxAttachmentSize</td>
<td>Range: 1—10 (MB)</td>
<td>5</td>
</tr>
<tr>
<td>desktopChatUnsupportedFileTypes</td>
<td>Unsupported file formats include comma-separated valid file extensions. For example: .exe, .sh</td>
<td>.exe, .msi, .sh, .bat</td>
</tr>
<tr>
<td>showAgentHistoryGadgets</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>showActiveCallDetails</td>
<td>true/false</td>
<td>true</td>
</tr>
<tr>
<td>pendingDTMFTresholdCount</td>
<td>Range: 1—20</td>
<td>20</td>
</tr>
<tr>
<td>dtmfRequestTimeoutInMs</td>
<td>Range: 1000—200000 (1 to 200 seconds)</td>
<td>5000 (5 seconds)</td>
</tr>
</tbody>
</table>

**Note**  To enable the following Finesse desktop properties in Cisco Finesse, Release 12.5(1), install Cisco Finesse Release 12.5(1) ES1 COP or higher.

- pendingDTMFTresholdCount
- dtmfRequestTimeoutInMs

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

**Step 7**

Click **Save**.

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

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

Procedure

Step 1  In the Manage Team Resources gadget, select a team.
Step 2  Click the Workflows tab.
Step 3  Click Add.
Step 4  Select one or more workflows from the list to assign them to the team.

Workflows you assign are highlighted in blue in the Add Workflows popup and added to the List of Workflows area.

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

Step 6  When you 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 on others, the changes on the tabs with no errors are saved while the changes on the tab with errors are not saved.

Unassign Workflows from Team

Procedure

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

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

- Workflows and Workflow Actions, on page 103
- Add Browser Pop Workflow Action, on page 108
- Add HTTP Request Workflow Action, on page 108
- Edit Workflow Action, on page 110
- Delete Workflow Action, on page 110
- Add Workflow, on page 110
- Edit Workflow, on page 111
- Delete Workflow, on page 111

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

Additionally, following are the fields that can be used to configure workflows:

- queueNumber
- queueName
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 must be unique and can be a maximum length of 40 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the workflow can be a maximum length of 128 characters.</td>
</tr>
<tr>
<td>Media</td>
<td>The media of the workflow. You can configure the media to Voice and any preferred Digital Channel.</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 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 and 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.

**Note**

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

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

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

- While previewing an Outbound Option call

Digital Channels dialog events include the following:
- When a task is offered
- When a task is accepted
- When a task is active
- When a task is paused
- When a task is interrupted
- When a task is closed

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

The workflow logic and examples are similar for all media.

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

Outbound Preview calls are an exception to this rule. You can have a workflow run while the agent previews the call and 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.
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.

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 comprise of the following:

- A piece of event data to be examined, for example, DNIS or call variables.
- A comparison between the event data and 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 listed order.

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

If 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 Finesse server as the first displayed call. This call may not be 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. Put the supervisors in their own team to keep agent workflows from being run for them.

### Workflow Triggers and Outbound Calls

---

**Note**

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

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

<table>
<thead>
<tr>
<th>Workflow Trigger</th>
<th>Direct Preview Outbound Call</th>
<th>Preview Outbound Call</th>
<th>Progressive/Predictive Outbound Call</th>
</tr>
</thead>
<tbody>
<tr>
<td>While previewing a call</td>
<td>When the agent previews the call (before accepting or rejecting it)</td>
<td>When the agent previews the call (before accepting or rejecting it)</td>
<td>Does not trigger</td>
</tr>
<tr>
<td>When a call arrives</td>
<td>Does not trigger</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 and during failover</td>
<td>When the customer answers the call and during failover</td>
<td>When the customer answers the call</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</td>
<td>When the customer call is initiated, and during failover</td>
</tr>
<tr>
<td>When a call ends</td>
<td>When the customer 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.

---

Note

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

---

Procedure

1. In the Manage Workflow Actions gadget, click New.
2. In the Name box, enter a name for the action.
   - Note: Workflow action names are limited to 64 characters.
3. From the Type drop-down list, choose Browser Pop.
4. From the Handled By drop-down list, choose what will execute the action, either the Finesse Desktop or Other (a third-party gadget).
5. In the Window Name box, enter the ID name of the window that is opened. Any action that uses this window name reuses that specific window.
   - Note: Window names are limited to 40 characters, and can be blank. If you leave the window name blank, a new window opens every time the action runs.
6. Enter the URL of the browser window and click the tag icon at the right of the box and select one or more variables from the drop-down list to add tags.
   - Example:

   http://www.google.com/search?q=\${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.
   - Note: Finesse does not validate the URL you enter.
7. Click Save.

---

Add HTTP Request Workflow Action

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

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

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

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

**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.  
**Note** The drop-down list contains variables from all the configured media channels.

**Example:**  
The following is the URL example for a Finesse API:

```
finesse/api/Dialog/dialogId
```

**Note** When the location is FINESSE, do not specify the protocol, host, and port information. Finesse automatically fetches these details when the REST request is executed.  
If you want to make a request to another API, you must enter the entire URL (for example, http://googleapis.com).

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

**Step 9**  
In the Body box, enter the text for the request. The body must match the content type (for example, if the content 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**.
**Step 3**  Edit the fields that you want to change.
**Step 4**  Click **Save**.

Delete Workflow Action

**Procedure**

**Step 1**  In the Workflow Actions gadget, select the action that you want to delete.
**Step 2**  Click **Delete**.
**Step 3**  Click **Yes** to confirm the deletion of the selected action.

Add Workflow

**Procedure**

**Step 1**  In the Manage Workflows gadget, click **New**.
**Step 2**  From the **Choose Media** drop-down, select the media.

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

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

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

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

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

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

**Note**  The drop-down actions change depending on the selected media.
Step 6  In the How to apply Conditions box, select if all conditions are met, or if any conditions are met, and then click Add Condition to add up to five conditions.

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

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

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

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

Step 9  Click Save.

Step 10 Assign the workflow to one or more teams.

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

---

**Edit Workflow**

**Procedure**

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

Step 2  Click Edit.

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

Step 3  Edit the fields that you want to change.

Step 4  Click Save.

---

**Delete Workflow**

**Procedure**

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

Step 2  Click Delete.

Step 3  Click Yes to confirm the deletion of the selected workflow.
CHAPTER 10

Manage Security

- HTTPS Support, on page 113
- Reset Security or Admin Password, on page 114
- Cross-Origin Resource Sharing (CORS), on page 115
- Gadget Source Whitelisting, on page 115
- Security Enhancements, on page 115

HTTPS Support

Cisco Finesse Release 12.5(1) or higher supports only Secure HTTP (HTTPS) and HTTP is permanently disabled. If you access Finesse using HTTP (unsecure port: 80 or 8082), then the 301 HTTP redirect status response is issued to the secure port 8445.

Note

Cisco Finesse Release 12.5(1) or higher supports HTTP/2 protocol by default.

To access the administration console using HTTPS, enter the following URL in your browser:

https://FQDN:8445/cfadmin

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

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

https://FQDN:8445/desktop

To eliminate browser security warnings each time you access the administration console or agent desktop through HTTPS, you can obtain and upload a CA certificate or you can use the self-signed certificate that is provided with Finesse.

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

HSTS

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

**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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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. |
Cross-Origin Resource Sharing (CORS)

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

Gadget Source Whitelisting

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

Security Enhancements

Cisco Finesse Release 12.5(1) onward, following security changes are implemented:

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

  Use the CLI command `utils finesse set_property webservices enableInsecureOpenfirePort true` to enable these ports.

- Validation of the X.509 certificate is enforced. It is mandatory to have the following valid non-expired X.509 CA or self-signed certificates, which must be imported into the Cisco Finesse trust store.
  
  - Cisco Finesse node certificates are available by default. The administrator must verify the validity of the certificates, as non-expired certificates are invalid.
    
    - Valid non-expired Cisco Finesse primary certificate must be present on the secondary Cisco Finesse.
    
    - Valid non-expired Cisco Finesse secondary certificate must be present on the primary Cisco Finesse.

  - Import the CUCM certificate to both the primary and secondary Finesse nodes.

  - Import the IdS certificate to both the primary and secondary Finesse nodes.

  - Import the Customer Collaboration Platform server certificates to both the primary and secondary Finesse nodes in the Unified CCE.

  - Import the LiveData server certificates to both the primary and secondary Finesse nodes in the Unified CCE.

  - Import the Cloud Connect server certificates to both the primary and secondary Finesse nodes in the Unified CCE.
You can override the trust certificate enforcement by using the CLI command `utils finesse set_property webservices trustAllCertificates true`.

For more information on CLI commands, see *Service Properties*.
Manage Finesse IP Phone Agent

- Finesse IP Phone Agent, on page 117
- One Button Sign In, on page 118
- Finesse IP Phone Service Subscription Options, on page 119
- Set Up Application User, Web Access, and HTTPS Server Parameters, on page 120
- Configure Finesse IP Phone Service in Unified CM, on page 121
- Finesse IP Phone Agent Certificate Management, on page 122
- Add Service Parameters for One Button Sign In, on page 125
- Subscribe Agent Phones to Manual Subscription Service, on page 127
- Set Up Agent Access to the Self Care Portal, on page 127

Finesse IP Phone Agent

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

Supervisor Tasks

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

Administration Tasks

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

Reason Code Limitations

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

Finesse IP Phone Agent Service Access Protocol

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

Failure Behavior

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

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

One Button Sign In

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

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

• You can prepopulate only the agent ID and extension, forcing the agents to manually enter their password at sign-in for increased security.

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

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

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

<table>
<thead>
<tr>
<th>Example Set Up</th>
<th>Prepopulated in Unified CM Administration</th>
<th>Prepopulated in Self Care Portal</th>
<th>Entered at Sign-In (by Agent)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator populates the extension only</td>
<td>extension</td>
<td>-</td>
<td>id</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>password</td>
</tr>
</tbody>
</table>
| Administrator populates the ID and extension | id  
extension | - | password |
Finesse IP Phone Service Subscription Options

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

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

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

<table>
<thead>
<tr>
<th>Finesse IPPA Configuration Procedures</th>
<th>Enterprise Subscription</th>
<th>Manual Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Administrator Manually Subscribes the Phones</td>
<td>Agents Manually Subscribe Their Phones Using the Self Care Portal</td>
</tr>
<tr>
<td><strong>Set Up Application User, Web Access, and HTTPS Server Parameters</strong></td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Configure Finesse IP Phone Service in Unified CM</strong></td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>Add Service Parameters for One Button Sign In</strong></td>
<td>Not applicable</td>
<td>Required only with One Button Sign In</td>
</tr>
</tbody>
</table>
### Set Up Application User, Web Access, and HTTPS Server Parameters

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

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

**Before you begin**
Set up call capabilities for the agent phones in Cisco Unified Communications Manager.

**Procedure**

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

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

To set these parameters in Cisco Unified CM Administration, use either of the following pages:
- Phone Configuration page (Product Specific Configuration portion of page): choose Device > Phone.
- Enterprise Phone Configuration page: choose System > Enterprise Phone Configuration.

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

a) In Cisco Unified Communications Manager Administration, select User Management > Application User.

b) Click Add New.

c) Under User Information, enter a user ID and password for the new user.

The password must be 95 characters or less and must contain ASCII characters only.
d) Under Device Information, in the Available Devices pane, select all phones that Finesse IP Phone Agents will use and move them to the Controlled Devices pane using the arrows.

e) Under Permissions Information, click Add to Access Control Group.

f) From the list of search results, select Standard CTI Enabled and Standard CTI Allow Control Of All Devices and then click Add Selected.

The application user is added to the Standard CTI Enabled and Standard CTI Allow Control Of All Devices groups.

g) Click Save at the bottom of the page.

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

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

a) Sign in to the Cisco Finesse Administration Console.

b) Choose Settings > IP Phone Agent Settings.

c) Under Phone URL Authentication Settings, enter the same username and password that you entered in Unified CM for the application user.

The password must be 95 characters or less and must contain ASCII characters only.

d) Click Save.

e) Restart Cisco Finesse Tomcat on the primary Finesses server.

f) After replication is complete, restart Cisco Finesse Tomcat on the secondary Finesses server.

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

---

**Configure Finesse IP Phone Service in Unified CM**

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

**Procedure**

- **Step 1** Log in to the Cisco Unified Communications Manager Administration using administrator credentials.

- **Step 2** Select Device > Device Settings > Phone Services.

- **Step 3** Click Add New to create a new IP phone service.

- **Step 4** In the Service Name field, enter **Cisco Finesse** (or another service name that is appropriate for your environment).

- **Step 5** In the Service URL field, enter: `http://Finesse FQDN:8082/fippa/#DEVICENAME#`

**Note** The Service URL entry is mandatory for Cisco Unified Communications Manager.
Step 6  In the Secure-Service URL field, enter: https://Finess FQDN:8445/fippa/#DEVICENAME# to configure Finess IP Phone Agent.

Note  • Support to HTTP is disabled from Cisco Finess, Release 12.5(1) onwards. Step 5 and Step 6 are mandatory to save the Finess IP Phone Agent settings.

• Import certificates for Finess IP Phone Agent to communicate with the Finess server using Secure HTTP (HTTPS) mode. For more information, see Finess IP Phone Agent Certificate Management.

Step 7  Ensure that the Service Category is set to XML Service, and the Service Type is set to Standard IP Phone Service.

Step 8  Check the Enable check box.

Step 9  Perform one of the following:

• To automatically subscribe all phones in the cluster to the Finess service, check the Enterprise Subscription check box, and click Save. Agents and supervisors can now access Cisco Finess by selecting it from the Services menu on subscribed IP phones.

  Note  One Button Sign In is not supported with enterprise subscriptions.

• To subscribe only the desired phones to the Finess service manually, leave the Enterprise Subscription check box unchecked and click Save.

Step 10  With a two-node Finess setup (primary and secondary Finess servers), perform the preceding steps again to create a secondary Finess service that points to the secondary Finess server. When you create the secondary service, note the following procedural differences:

• At Step 4, in the Service Name field, enter a name that distinguishes the secondary service from the primary service, such as Cisco Finess Secondary.

• At Step 5 and Step 6, replace Finess FQDN with the FQDN of the secondary server.

---

Finess IP Phone Agent Certificate Management

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

• For a CA-signed certificate, see CA-Signed Certificate, on page 123.

• For a self-signed certificate, see Self-Signed Certificate, on page 123.
CA-Signed Certificate

**Procedure**

**Step 1** Obtain the CA-signed certificate from the signed authority for both Cisco Finesse and CUCM server.

**Step 2** Import the CA-signed certificate of CUCM to theCisco Finesse server trust store as **tomcat-trust**. For more information, see Import CUCM Certificate, on page 124.

**Step 3** Import the CA-signed certificate of Cisco Finesse certificate to the CUCM trust store as **Phone-trust**. For more information, see Import Certificate into CUCM Trust Store, on page 125.

Self-Signed Certificate

**Procedure**

**Step 1** Export the self-signed CUCM certificate from the Cisco Unified Operating System Administration. For more information, see Export CUCM Certificate, on page 123.

**Step 2** Import the downloaded self-signed CUCM certificate to the Cisco Finesse trust store as **tomcat-trust**. For more information, see Import CUCM Certificate, on page 124.

**Step 3** Export the self-signed Cisco Finesse certificate from the Cisco Unified Operating System Administration. For more information, see Export Cisco Finesse Certificate, on page 124.

**Step 4** Import the downloaded self-signed Cisco Finesse certificate to the CUCM trust store as **Phone-trust**. For more information, see Import Certificate into CUCM Trust Store, on page 125.

Export CUCM Certificate

**Procedure**

**Step 1** Sign in to Cisco Unified OS Administration on the CUCM server using the following URL: https://FQDN of CUCM server:8443/cmplatform.

**Step 2** Select Security > Certificate Management.

**Step 3** Enter the search criteria as **tomcat** and then click Find to filter the certificate.

The tomcat certificates list is displayed. If you do not find the tomcat certificate for your server in the Certificate List, then click Generate Self-signed. When the certificate generation is complete, reboot your server. Then restart this procedure. For more information on generating the self-signed certificate, see Cisco Unified Operating System Administration Online Help.

**Step 4** Click the tomcat certificate hyperlink in the **Common Name** column.

The tomcat **Certificate Details** dialog box is displayed.

**Step 5** Click Download .PEM File.
Step 6  Save the .PEM file in your local machine.

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

Import CUCM Certificate

Procedure

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

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

Export Cisco Finesse Certificate

Procedure

Step 1  Sign in to Cisco Unified OS Administration on the Cisco Finesse server using the following URL: https://FQDN of Finesse server:8443/cmplatform.
Step 2  Select Security > Certificate Management.
Step 3  Enter the search criteria as tomcat-trust and then click Find to filter the certificate.
Step 4  Click the tomcat-trust certificate hyperlink in the Common Name column. The tomcat Certificate Details dialog box is displayed.
Step 5  Click Download .PEM File.
Step 6  Save the .PEM file in your local machine.
What to do next
Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

Import Certificate into CUCM Trust Store

Procedure

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

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

Add Service Parameters for One Button Sign In

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

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

Procedure

<p>| Step 1  | From Cisco Unified Communications Manager Administration, select the Finesse phone service (under Device &gt; Device Settings &gt; Phone Services). |
| Step 2  | Click New to the right of the Parameters box. |
| Step 3  | Set up service parameters for the agent id, extension, and password credentials as per the following table. Enter only the parameters that you want prepopulated for the agents. For each parameter, enter the required field values and click Save. To add parameters, click Add New and enter the required values. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Parameter Name**            | Enter one of the following parameter names as follows:  
  • Id  
  • Extension  
  • Password  
  The values entered are the exact query string parameters used for the subscription URL.                                                                 |
| **Parameter Display Name**    | Enter a descriptive parameter name; for example, id, extension, and password.                                                                                                                                |
| **Default Value**             | Leave the default value blank for all parameters.                                                                                                                                                            |
| **Parameter Description**     | Enter a description of the parameter. The user can access this text when they subscribe to the service.                                                                                                      |
| **Parameter is Required**     | If the administrator prepopulates the parameter in Unified CM Administration, check the **Parameter is Required** box.  
  However, if the agent prepopulates the parameter in the Self Care Portal, two options are available:  
  • If the agents prepopulates all defined parameters, check the **Parameter is Required** box for each parameter.  
  • If the agent and administrator share the responsibility of prepopulating the parameters, set only the administrator-defined parameters as required. This configuration ensures that the administrator can save the subscription without prepopulating all parameters. In this case, the administrator first prepopulates the required parameters, and then the agents prepopulate the nonrequired parameters. |
| **Parameter is a Password (mask contents)** | Check this box for the password only.  
  This check box masks the password entries in the Self Care Portal, to display asterisks rather than the user entry.                                                                                      |

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

---

**What to do next**

You can prepopulate the agent credentials when you subscribe the agent phones, or the agents can prepopulate their own credentials using the Unified CM Self Care Portal.
Subscribe Agent Phones to Manual Subscription Service

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

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

Procedure

**Step 1**  
From the menu bar, select **Device > Phone**.

**Step 2**  
Select the phone that you want to subscribe to the Finesses service.

**Step 3**  
From the **Related Links** drop-down list on the upper right side of the window, select **Subscribe/Unsubscribe Services** and click **Go**.

The **Subscribed IP phones services** window displays for this phone.

**Step 4**  
From the **Select a Service** drop-down list, select **Cisco Finesses**.

**Step 5**  
Click **Next**.

**Step 6**  
*(Applicable for One Button Sign In only)* Enter values for any of the defined service parameters (id, password, and extension) that you do not want the agents to enter using the Self Service Portal or at sign-in.

**Step 7**  
Click the **Subscribe** button to subscribe this phone to the Cisco Finesses service.

The Cisco Finesses service displays in the **Subscribed Services** list.

**Step 8**  
Click **Save**.

The subscribed agents or supervisors can now access Cisco Finesses by selecting it from the **Services** menu on their IP phones.

**Step 9**  
With a two-node Finesses setup (primary and secondary Finesses servers), perform this procedure again to also subscribe the phones to the secondary Finesses service that points to the secondary Finesses server.

Set Up Agent Access to the Self Care Portal

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

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

Procedure

**Step 1**  
From the Unified CM Administration page, select **System > Enterprise Parameters**.

**Step 2**  
Under the Self Care Portal Parameters, in the **Self Care Portal Default Server** field, select the IP address of the Unified CM Publisher server from the drop-down list and click **Save**.
**Step 3** Select User Management > End User.

**Step 4** Select the user that you want to set up with access to the User Care Portal.

**Step 5** Under Permissions Information, click Add to Access Control Group.

**Step 6** From the list of Access Control groups displayed, check Standard CCM End Users and click Add Selected.

**Step 7** Click Save.

---

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

---

**Note** In a two-node Finesse setup with two services configured, the agents must enter their credentials on the primary and secondary Finesse services.
CHAPTER 12

Manage Third-Party Gadgets

• 3rdpartygadget Account, on page 129
• Upload Third-Party Gadgets, on page 130
• Cisco Webex Experience Management, on page 131

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:

```bash
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, the maximum key length cannot exceed 2048.

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 Finesse server, as illustrated in the following example. Note that third-party gadget files must be .xml files. It does not support .jsp files.

Note

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

```
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:

```
https://<finesse>/3rdpartygadget/files/
```

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

```
https://<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 Finesse desktop 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:

```
<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. To perform these actions, SELinux has to be in permissive mode. This can be accomplished by executing the following CLI command:

```
utils os secure permissive
```

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

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

**Third-Party Gadget Limitations**

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

---

**Cisco Webex Experience Management**

Cisco Webex Experience Management (Experience Management) is the platform for Customer Experience Management (CEM), integrated with powerful tools that allow you to see your business from your customers' perspective. Experience Management has all the sophisticated features and functionality including customer journey mapping, text analytics, and predictive modeling in a single point-n-click platform.


Cloud Connect is a component that hosts services that allow customers to use cloud capabilities such as Cisco Webex Experience Management. The administrator can configure the Cloud Connect server settings in the Finesse administration console to contact the Cisco cloud services. For more information, see Cloud Connect Server Settings, on page 24.

---

**Configure Experience Management Gadgets for Finesse Desktop**

Experience Management Activation Team provides the details to log in to Experience Management. For more information, see Cisco Webex Experience Management Activation.

Gadgets are displayed by default in the Spaces tab of the Experience Management. To know more about default gadgets and derive meaningful insights from them, see Cisco Webex Experience Management Gadgets.

To export the Cisco Finesse gadget code from Experience Management, see Export Cisco Finesse Gadget Code.

To add Experience Management gadgets in Finesse desktop layout, see Add Experience Management Gadgets.
Experience Management Gadgets—Task Activity Notification

Note
This is supported from Cisco Finesse, Release 12.5(1) ES3 onwards.

The TaskActivityNotification API is a mechanism by which the Finesse desktop can now provide a way for gadgets to sense the digital channel task worked on by an agent, across different media. The notifications inform the desktop and other subscribers about which non-voice media dialog is currently selected or de-selected by the agent.

This can be used for showing or processing the relevant information associated with the task activity automatically, in supporting gadgets, which subscribe for these activity notifications, when the agent switches between different tasks.

Note
The feature requires participating gadgets to publish and subscribe for the activity notifications. The Finesse desktop by itself cannot provide these notifications or provide task activity processing based on these notifications.

The implementation of task activity notification is provided by digital channel gadgets such as Cisco Enterprise Chat and Email (ECE). The ECE gadget provides task notifications, and Cisco Webex Experience Management gadget subscribes and displays customer journey information corresponding to the task which is currently active.


CHAPTER 13

Perform Routine Maintenance

- Cisco Finesse Services, on page 133
- Log Collection, on page 134
- Collect Logs using Cisco Unified Real-Time Monitoring Tool, on page 137
- Cisco Finesse Notification Service Logging, on page 139
- Remote Account Management, on page 140

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

The deployed applications in the Cisco Finesse Tomcat service include:

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

- **Finesse Rest API application**: Provides integration with the Cisco CTI Server for the Finesse desktop and Finesse administration application. The APIs 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**: Provides the administrative operations for Finesse.

- **Finesse Diagnostic Portal application**: Provides performance-related information for Finesse.

- **Finesse IP Phone Agent (IPPA) application**: Allows agents and supervisors to perform Finesse operations on their Cisco IP Phone.

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

---

**View, Start, or Stop Services**

**Procedure**

**Step 1**  
Sign in to 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 Finesse Tomcat, enter the command `utils service start Cisco Finesse Tomcat`.

**Step 4**  
To stop a service, enter the following command: `utils service stop service name`.  
**Example:**  
For example, to stop Cisco Finesse Tomcat, enter the command `utils service stop Cisco Finesse 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:** 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:** 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:** 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.
  
  - **audit-log:** Audit logs contain all admin operations (including Finesse admin UI and REST client operations) and supervisor operations for Team Message. The maximum size of an uncompressed audit log file is 100 MB. The maximum size of total audit log files (including compressed log files) is approximately 1 GB. After a log file reaches 100 MB, that file is compressed and a new log file is generated. The log file wrap-up duration can vary, based on the number of users on the system. The log contains the following parameters:
    
    - Timestamp
    - User Id of the administrator
    - Method of operation (PUT, POST, DELETE). GET operations will not be logged
    - URL
    - Payload

• **clientlogs:** Contains the client-side logs that are submitted from the Cisco 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 that 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. The directory holds a maximum number of 25000 clientlog files. When the directory exceeds the size limit or the file count, the oldest files are deleted.

• **openfireservice:** Contains startup and shutdown-related information logs for the Cisco Finesse Notification Service.

• **openfire:** Contains limited error and information logs for the Cisco Finesse Notification Service.

• **finesse-dp:** Contains startup, error, and information logs generated by the Finesse Diagnostic Portal application.

• **realm:** Contains the logs for authentication requests from clients that are handled by the Finesse backend.

• **db:** Contains the Finesse database logs.

• **/finesse/logs:** Contains the logs for the Cisco Finesse Tomcat service.

• **fippa:** Contains logs for the Finesse IP Phone Agent (IPPA) application.

• **3rdpartygadget:** Contains information, error, startup, and shutdown-related logs for the Cisco Finesse 3rdpartygadget server.
Log Collection

- **jmx**: Contains the JMX counters data that is generated by the JMX logger process. It contains important jmx counters that are exposed by Finesses and openfire.

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

- **WebProxy Service logs**: `file get activelog webproxy recurs compress`

Use this command to obtain logs for the WebProxy Service. The maximum size of an uncompressed webproxy log file is 10 MB. The maximum size of this directory is approximately 500 MB. After a log file reaches 10 MB, that file is compressed and wraps to the new log file which is generated. 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 webproxy log.

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

This command uploads a zip file that contains the following log files:

- **access.log**: Contains the webproxy access logs after you configure the access log-level using the `set webproxy access-log-level` CLI. For more information on CLI commands, see [WebProxy Service](#).

- **error.log**: Contains the webproxy error logs.

- **webproxy_cli.log**: Contains the webproxy CLI logs. For more information on CLI commands, see [WebProxy Service](#).

- **webproxy_launcher.log**: Contains the logs after the WebProxy Service is launched.

**Note**

To access the individual log file, use the command `file get activelog webproxy/<log filename>`.

For example, `file get activelog webproxy/error.log`

- **Servm log**: `file get activelog platform/log/servm*.* compress`

Use this command to obtain logs that are generated by the platform service manager that manages the starting and stopping of the Finesses 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 the 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 the timestamp in long format.

- **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.

Call Variables Logging

From Cisco Finesse Release 12.5(1) onwards, the call variables logging in Cisco Finesse logs are disabled by default. The callVariables contain sensitive user information and this property allows the administrator to decide whether the information must be captured in the logs. You can enable the call variables logging by using the CLI commands.

Collect Logs using Cisco Unified Real-Time Monitoring Tool

Cisco Finesse supports the Cisco Unified Real-Time Monitoring Tool (RTMT) for log collection. Use the following procedure to collect logs using Unified RTMT.

Note: Finesse supports RTMT only for log collection. Other RTMT features are not supported.

Before you begin

Download and install RTMT on a client computer from the following URL:

https://FQDN:8443/plugins/CcmServRtmtPlugin.exe

where FQDN is the Fully Qualified Domain Name of the Finesse server.

Procedure

Step 1: Log in to Unified RTMT using Finesse administrator credentials.
Step 2: In the tree hierarchy, select Trace & Log Central.
Step 3: Double-click Collect Files.
   The Trace Collection wizard appears.
Step 4: Select the services and Finesse nodes for which you want to collect logs, and complete the wizard.

What to do next

For detailed instructions, see the Cisco Unified Real-Time Monitoring Tool Administration Guide, which is listed here:

Syslog Support for Critical Log Messages

Cisco Finesse generates syslogs for critical log messages. Use the following procedure to view the logs using Unified RTMT.

**Before you begin**
Download and install RTMT on a client computer from the following URL: https://FQDN:8443/plugins/CcmServRtmtPlugin.exe, where FQDN is the Fully Qualified Domain Name of the Finesse server.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to Unified RTMT using Finesse administrator credentials.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the tree hierarchy, select <strong>SysLog Viewer</strong> or choose <strong>System &gt; Tools &gt; SysLog Viewer &gt; Open SysLog Viewer</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the <strong>Select a Node</strong> drop-down list, choose the server where the logs that you want to view are stored.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Under the <strong>Logs</strong> tab, select <strong>Application Logs &gt; CiscoSyslog</strong> to view and save the syslog file.</td>
</tr>
</tbody>
</table>

**Tip**
When you double-click the CiscoSyslog message, the **Show Detail** dialog displays the syslog definition and recommended actions in an adjacent pane.


**Note**
System log messages generated by Cisco Finesse are also available under **SysLog Viewer > System Logs > messages**.

The following are the different types of messages and corresponding descriptions that are captured in the **SysLog Viewer > System Logs > messages**.

- **CTI_SOCKET_ERROR**
  System has encountered an error connecting to the CTI server.

- **CTI_CONNECTION_LOST**
  System has lost contact with the CTI server.

- **CTI_OPEN_FAILURE**
  CTI Server rejected open request.

- **CTI_CONNECTION_RETRIES_EXCEEDED**
  System has failed to connect to CTI server in the allowed number of retries.

- **CTI_CONNECTION_ESTABLISHED**
  System has successfully connected to CTI server.

- **SUBSYS_INIT_ERROR**
  Error initializing subsystem.
Cisco Finesse Notification Service Logging

Use the following commands to view the status of, enable, or disable 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.

  ```
  $ utils finesse notification logging status
  ```

  **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.

- **utils finesse notification logging enable**: This command enables Cisco Finesse Notification Service logging.

  ```
  $ utils finesse notification logging enable
  ```
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.

**Note**

- `utils finesse notification logging disable`: This command disables Cisco Finesse Notification Service logging.

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.

**Note**

---

**Remote Account Management**

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

```bash
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`
CTI Failover

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

The prerequisites for successful CTI failover are as follows:

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

In the duplex mode, if Finesses loses connection to the CTI server, it attempts to connect to the server which is running. Finesses alternates between the configured servers until it makes a successful connection.

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

After reconnecting to a CTI server and transitioning to IN_SERVICE state, Finesses responds to client requests and publishes events.

Connection to the CTI server can be lost due to the following reasons:

- Finesses misses three consecutive heartbeats from the connected CTI server (heartbeat interval is five seconds).
- Finesses socket opened to the CTI server fails.

After failover is complete, the last state of call control, call data, or agent state are published as events to all clients. This allows Finesses clients to reflect an accurate view of the call control, call data, and agent state.
If an agent either makes or answers a call, and then ends that call during failover (that is, the entire call takes place during failover), the corresponding events are not published.

---

**Note**

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

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

Despite these limitations, the agent and 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.

---

**Prevent Non-Voice Task RONAs during CTI Reconnect**

When CTI disconnection happens, the agent state is changed to WORK, on the respective non-voice Media Routing Domain (MRD), to prevent tasks getting routed to the disconnected agents. Previous releases of Unified CCE used to change the agent states back to an available state when the CTI connection is re-established, even though the media handling gadgets and the media channels are not initialized by then.

The media handling gadgets, and the media channels are initialized only after the Finesse desktop failover completes.

Due to the significant delay in desktop failing over after the Finesse server reconnects to the CTI server, chances of occurrence of RONA (Redirection on No Answer) are high when dealing with non-voice tasks.

Unified CCE, Release 12.5 (1) or later allows the agent state to remain in WORK mode after CTI reconnection. This allows the agents to change to an available state in non-voice MRD explicitly after the Finesse desktop and media channels are initialized. This avoids the task being routed to the user before the agent is ready to handle non-voice media tasks.

By default, Cisco Finesse Release 12.5(1) retains the earlier behavior, which can be modified using the `enableAutoWorkModeStateChange` property. By default, this property is set to `true`, and the administrator can set to `false` to change to the new behavior.

---

**Note**

This behavior is supported from Unified CCE Release 12.5(1) onwards, and only after the relevant non-voice gadgets or custom desktop or clients support this behavior.

The agents remain in the WORK mode until they are explicitly set to active on the respective MRD using the REST API. This informs the CTI that the media channel is available (and connected) and the tasks can be routed to the respective user on that MRD.
The Media—Change Agent from Work State to Active API allows a user to change the agent state from WORK state to active (READY or NOT_READY), which is automatically computed by Unified CCE. Users can only use this API when an agent state is WORK.

**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 Cisco Finesse administration console.
- Cisco Finesse 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 or call control request), the credentials are cached in Cisco Finesse for 30 minutes from the time of the request. After a user is authenticated, that user continues to be authenticated until 30 minutes pass, even if both AWDBs are down. Cisco Finesse attempts to reauthenticate the user against the AWDB only after the cache expires.

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

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

If Cisco Finesse cannot connect to either of the Administration & Data servers and the cache has expired, the systems returns the following errors:

- Agents and supervisors who attempt to sign in to the Finesse desktop receive an “Invalid user ID or password” error message.
- Administrators cannot update or retrieve settings in the Cisco Finesse administration console.
- Users who are already signed in to Cisco Finesse receive an “Operation timed out” error message.
- Users who make API requests receive an 401 “Unauthorized” HTTP error message.

If Cisco Finesse loses connection to one AWDB and then receives requests, these requests may time out before Cisco 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.

**Finesse Desktop Failover**

Desktop failover can occur for the following reasons:

- When the Finesse desktop loses network connectivity to the Finesse Notification Service.
- When the Finesse Tomcat Service becomes *Unavailable*.
- When the Finesse REST API Service becomes *Unavailable*.
• When the Finesse Notification Service becomes *Unavailable*.

• When the Finesse loses connection to CTI servers

---

**Note**

• After the failover, the pending state of an agent will not be displayed once the agent fails over to the subscriber. The pending state change is lost during the failover, as the agent will be logged out, and logged in again.

• Finesse is IN_SERVICE, co-ordinates the distribution of desktop reloads, such that failover and consequent desktop reloads are evenly distributed to prevent overwhelming of the Finesse server. Configuration data such as reason codes, workflows and so on are not reloaded during failover to improve the performance.

---

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

• Checks whether the subscriber is available and IN_SERVICE.

• Continues to check whether the publisher recovers its state.

If the subscriber is available, then the desktop automatically signs the agent into the subscriber. If the publisher recovers its state, the desktop notifies the agent that it has reconnected.

The failover logic has three triggers to detect desktop failure:

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

• The Finesse Notification Service is disconnected.

• The XMPP presence of “finesse” user changes to *Unavailable*.

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

1. Poll SystemInfo for publisher every 20 seconds.

2. If SystemInfo API reports Finesse is IN_SERVICE, check the Finesse Notification Service.

3. If SystemInfo is IN_SERVICE, check whether the last CTI heartbeat status of the side being connected is a success.

---

**Note**

The last CTI heartbeat status is checked to ensure that the subscriber is healthy before failover, and thus does not immediately transition to OUT_OF_SERVICE after the client has failed over. This may occur in CTI failure, since both Finesse servers connect to the same PG and CTI server, and a CTI failure can cause both Finesse servers to disconnect and connect to the alternate PG. Depending on the network topology the subscriber might be slower to sense a network disconnect.

---

4. If XMPP is disconnected, make the Finesse Notification Service request.

5. If the Finesse Notification Service is successful and Finesse service is IN_SERVICE, refresh the data.
The failover logic prefers to stay with the publisher. If the failover logic detects that the subscriber is available, it checks the publisher one more time. If the publisher has recovered, the desktop reconnects to the publisher. If the publisher is still down, the desktop connects the agent to the subscriber. In this case, the agent does not automatically reconnect to the failed server after it recovers, but instead remains connected to the subscriber. If the Finesse Notification Service is the source of failure, the desktop makes three attempts to reconnect before changing the state of the desktop to disconnected. These attempts occur before the failover logic begins.

Desktop Behavior

Cisco Finesse sends a code of 255 to the CTI server and 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. If the browser crashes, 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.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Desktop Behavior</th>
<th>Server Action</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>The agent closes the browser, the browser crashes, or the agent clicks the Back button on the browser.</td>
<td>Finesse desktop makes a best-effort attempt to notify the server.</td>
<td>Finesse receives a presence notification of Unavailable from the client. Finesse waits 60 seconds, and then sends a forced logout request to the CTI server.</td>
<td>Race Conditions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. The agent closes the browser window. Finesse receives a presence notification of Unavailable for the user. Finesse tries to sign the agent out, however, that agent is already signed out.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. If the browser crashes, it can take the Finesse server up to 120 seconds to detect that the client is gone and send a presence notification to Finesse. A situation can occur where the client signs into the subscriber before</td>
</tr>
</tbody>
</table>
the publisher receives the presence notification caused by the browser crash. In this case, the agent may be signed out or put into Not Ready state on the subscriber.

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.

4. If agent is in Not Ready State before Failover, agent moves to Not Ready - Connection Failure after CTI Disconnect or Reconnect.

   If agent is in Ready State before Failover, agent moves to Not Ready - Connection Failure upon his next state change to Not Ready.

<p>| The client refreshes the browser | — | Finesse receives a presence notification | — |</p>
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The client encounters a network glitch (Finesse is IN_SERVICE)</td>
<td>Connection to the Finesse server temporarily goes down, consequently the client fails over to the subscriber.</td>
<td>The publisher receives a presence notification of Unavailable from the client. Finesse is IN_SERVICE, so it sends a forced logout request to the CTI server for the agent.</td>
</tr>
<tr>
<td>The Refresh Token has expired. For more information on tokens, see <a href="https://developer.cisco.com/docs/finesse/#single-sign-on-apis">https://developer.cisco.com/docs/finesse/#single-sign-on-apis</a>.</td>
<td>Finesse desktop sends a forced logout request to the CTI server.</td>
<td>The session expiry warning appears 10 minutes and 5 minutes before the Refresh Token expires. In the last minute, a countdown timer appears till the Refresh Token expires.</td>
</tr>
<tr>
<td></td>
<td>The Finesse server forwards the forced logout request to the CTI server.</td>
<td></td>
</tr>
</tbody>
</table>

**Race Conditions**

A situation can occur where the forced logout does not happen before the client signs in to the subscriber. If the agent is on a call, the publisher 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 subscriber.

If agent is in Not Ready State before Failover, agent moves to Not Ready - Connection Failure after CTI Disconnect or Reconnect.

If agent is in Ready State before Failover, agent moves to Not Ready - Connection Failure upon his next state change to Not Ready.
Token expires. The agent is forcefully logged out when the timer reaches zero and must log in again.

For Unified CCE, the state of the agent changes to Log Out or Not Ready based on the Load parameter set as below.

**Load parameter = 0**

- When the agent's current state is Not Ready, Ready, or Wrap-Up, the agent's state after force logout is changed to Not Ready – Connection Failure.
- When the agent's current state is Talking, the Agent goes into Not-Ready – Connection Failure state after the call ends.

**Load parameter = 1**

- When the agent's current state is Not Ready, Ready, or Wrap-Up, the agent goes to Logged Out – System Failure.
- When the agent's current state is Talking, the Agent goes to Logged Out – System Failure immediately even
though the call is still active.

Desktop Chat Failover

The following table lists the desktop chat failover scenarios:

<table>
<thead>
<tr>
<th>Failover Type</th>
<th>Desktop Chat Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IM&amp;P server failover</td>
<td>The desktop chat status is retained, and all active chat sessions are lost.</td>
</tr>
<tr>
<td>Finesse server failover</td>
<td>The desktop chat status is retained, and all active chat sessions are lost.</td>
</tr>
<tr>
<td>CTI server failover</td>
<td>The desktop chat status and all chat sessions are retained.</td>
</tr>
</tbody>
</table>

Finesse IP Phone Agent Failover

Finesse IPPA failover can occur for the following reasons:

- The Finesse REST API Service transitions to OUT_OF_SERVICE.
- The Finesse Notification Service transitions to OUT_OF_SERVICE.
- If Finesse IPPA detects a server failure before Finesse fails over to the alternate CTI server, then Finesse IPPA declares the Finesseserver OUT_OF_SERVICE.

The server that an agent is connected transitions to OUT_OF_SERVICE, the Finesse IP Phone Agent (IPPA) displays a notification that the server is unavailable. Finesse IPPA continues to check whether the current Finesseserver recovers its state and notifies the agent if it reconnects.

Finesse IPPA attempts to reconnect to the server every 5 seconds and declares it OUT_OF_SERVICE after three failed attempts. The total time required for the transition to OUT_OF_SERVICE is approximately 15 seconds.

Unlike the Finessedesktop, Finesse IPPA does not check whether the subscriber is available. To connect to subscriber, the agent must exit the publisher, and manually sign into the subscriber.

Finesse IPPA failover logic has the following two triggers to detect failure:

- Finesse IPPA receives a SystemInfo event that the publisher is OUT_OF_SERVICE.
  
  Finesse IPPA polls SystemInfo every 5 seconds to check whether the Finesseserver is IN_SERVICE. After three attempts, if the Finesseserver is not IN_SERVICE, Finesse IPPA displays a server unavailable message to the agent.

- Finesse IPPA receives notification that the Finesse Notification Service is disconnected.

  Finesse IPPA tries every 5 seconds to reconnect with the XMPP server. After three attempts, if the Finesse Notification Service cannot be reestablished, Finesse IPPA displays a server unavailable message to the agent.
While the agent is still signed into the current service, Finesse IPPA continues attempting to reestablish the connections with the Finesse and XMPP servers. If they both resume service, Finesse IPPA displays the Sign In screen and the agent can sign in again and continue as normal.

Alternately, the agent must exit the current Finesses service and try to connect using an alternate Finesse service.

**Guidelines for Optimal Desktop Failover**

The following are the guidelines to optimize failover scenarios, to avoid server overload and unnecessary delays.

- Browser Configuration, on page 150
- Agent Configuration, on page 151
- Finesse Configuration, on page 151
- Agent PG Configuration, on page 152
- CUIC Configuration, on page 152
- Common Configuration Safeguards, on page 152

**Note**

The guidelines for optimal failover ensure that desktop initialization time and general system performance is optimized.

**Browser Configuration**

Finesse browser failover performance depends on the number of requests made to the Finesse server. Fewer the requests, lesser the system load on the Finesse server. The following browser-specific configurations ensure that the browser does not fetch static resources unnecessarily from the server, and it is a key requirement for faster failover.

**Note**

Clear the browser cookies before logging in to the Finesses desktop. This avoids unexpected expiry of the Refresh Token in the Single Sign-On mode for Unified CCE.

- Avoid loading the Finesses desktop with `bypassServerCache=true&nocache` as a query parameter in the desktop URL. The `bypassServerCache` is to bypass Webproxy cache, and `nocache` is to bypass Shindig cache.
- Host systems must have at least 200 MB of free disk space more than the free space required by the operating system (OS).
- Adequate network bandwidth must be available between the Finesses desktop and the Finesses server. Lower latency results in faster failover.

For more information on bandwidth measurements, see [Finesses Bandwidth Calculator for Unified Contact Center Enterprise](#) and [Cisco Unified Contact Center Express Bandwidth Calculator](#) at
Host systems must have adequate memory and CPU without being overloaded at any point in time. A slow host slows the browser enough to cause it to fail and reload resources randomly during failover.

External gadget hosting servers must prefer CA-signed certificates for easy integration with the browser. If they are self-signed, then import those certificates into the agent browser.


Firefox Configurations

Disable the Race Cache With Network (RCWN) in all the agent desktops to avoid any unwanted requests to the Finesseserver. If RCWN is enabled, the Firefox browser by-passes the cached data and fetches the static requests again from the server. Set the network.http.rcwn.enabled configuration as false.

For more information, see https://support.mozilla.org/en-US/questions/1267945.

Google Chrome, Internet Explorer, and Microsoft Edge Configurations

Import the Finesseself-signed certificates on Google Chrome, Internet Explorer, and Microsoft Edge browsers trust store.


Agent Configuration

Agents configured must be evenly distributed between the publisher and subscriber. This prevents all agents from failing over when there is an outage that affects only one of the deployed Finesseserver.

The number of agents failing over impacts system load and has a linear relationship with the maximum time taken for the operation to complete.

Finesses Configuration

The number of signed-in users, the gadget types, and the average number of gadgets configured per user, significantly impacts failover load.

The following are the best practices for ensuring a trouble-free failover.

- Number of Gadgets per Agent—Gadget-initiated requests constitute the bulk of the requests made during Finessedesktop failover or startup. Configuring fewer gadgets in the desktop layout results in faster desktop failover and startup. The administrator must configure the team or desktop layouts such that only the required gadgets for each team are available in the desktop layout.

- Type of Gadget—XML-based gadgets load much faster than gadgets served using a dynamic JSP-based URL. The gadget content is also cached at the WebProxy Service, which allows the Finesseserver to scale further. The JSP-based gadgets take thrice the time to load than the XML-based gadgets.

The Unified CCE deployments must ensure that Cisco Unified Intelligence Center (CUIC) 12.5(1) servers are deployed, and CUIC JSP-based URLs are replaced using the CLI utilities finesse layout updateCuicGadgetUrl to reduce latency and improve performance.
• Finesse Server Capacity—Deployments with 2000 active users and configuring more than eight XML-gadgets per user on average, or more than six JSP-based gadgets per user on average, are recommended to deploy Cisco Finesse OVA with 8 vCPUs.

When OVA with 8 vCPUs is configured for Finesse, the time taken for CTI server/Agent PG failover and desktop failover improves by 20 percent. This configuration is supported on all deployment types including the 24000 Agent deployment type. For more information on OVA with 8 vCPUs, see Virtualization for Cisco Finesse at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-finesse.html.

• Gadget Configuration—Gadgets developers must follow certain best practices to ensure that gadgets load faster.


• Secondary Resources—The preloading of server resources reduces latency and improves performance during desktop failover. By default, the preLoadSecondaryResources property is enabled. Disabling this property impacts failover time. For more information, see Desktop Properties.

Agent PG Configuration

Upgrading to the latest Agent PG version allows faster detection of failure, which results in faster failover. When Cisco Finesse connects to Agent PG 11.6(x) and 12.0(x) versions, it incurs a delay of up to 40 seconds to detect CTI failover compared to Agent PG 12.5(1) or later.

CUIC Configuration

CUIC 12.5 (1) or later supports only XML-based gadgets corresponding to the JSP-based gadget URLs that supported the real-time reports.

Cisco Finesse 12.5 (1) provides CLI utils finesse layout updateCuicGadgetUrl, which automatically changes the JSP references to XML with no functional changes.

Switching to XML-based gadgets reduces latency and improves performance. After the CUIC or Coresident deployment installation, run the command to optimize the faster failover.

Common Configuration Safeguards

• Import the self-signed certificates into the browser.

• Do not disable browser caching for Finesse desktop.

• Do not clear the cache every time the browser is launched.

• Distribute the agents between the publisher and subscriber.
Failover Planning

CTI Failover

CTI failover happens when the Finesse server disconnects from the CTI server/Agent PG due to network failure or server error. In these scenarios, the Finesse server is unavailable to its clients. If the desktop is connected, it displays that the server is unavailable and tries to reconnect to the available Finesse server.

The duration required for Finesse CTI failover depends on the following factors.

• Agent PG 12.5(1) or later versions results in faster failover.

• Available bandwidth from the CTI server to the Finesse server.

• Round Trip Time (RTT) between the CTI server and the Finesse server in case of WAN deployments.

• The number of signed-in users.

• The number of gadgets configured.

• The number of active non-voice tasks.

When deployed with Agent PG 12.5(1) or later, CTI server/Agent PG failover varies approximately from 35 seconds to 75 seconds. When deployed with Agent PG 12.0(1) or 11.6(1), CTI server/Agent PG failover varies approximately from 75 seconds to 120 seconds. The numbers indicated varies depending on the customer configuration and the above-stated factors. It must be used as a guideline to determine the approximate range for failover time.

Note

The time indicated does not include CTI server/Agent PG server recovery time. It only indicates the time taken for Finesse to reconnect and be IN_SERVICE, once an active Agent PG is detected.

Desktop Failover

The Finesse desktop failover happens in all failure scenarios. The Finesse desktop tries to find an active server and fails over to it, once it has located a reachable server which is IN_SERVICE.

The duration required for Finesse desktop failover depends on the following factors.

• Bandwidth available to the client to reach the Finesse server.

• RTT between the client and the Finesse server.

• The number of signed-in users.

• The number of gadgets configured in the desktop per user.

• Type of gadgets (XML) and the resources it loads. For more information on Finesse gadgets, see https://developer.cisco.com/docs/finesse/#finesse-gadgets.

• The number of vCPU configured on the Finesse server.

• Agent PG version.

• The time required for the upstream CTI and the Finesse servers to become reachable and be IN_SERVICE.
The desktop failover performance improvements in Cisco Finesse 12.5(1) are available in all releases irrespective of the Agent PG version.

When deployed with Agent PG 12.5(1) or later, desktop failover with the default desktop layout varies approximately from 50 seconds to 110 seconds. When deployed with Agent PG 12.0(1) or 11.6(1), desktop failover is approximately 40 seconds more when compared to Agent PG 12.5(1) or later.

The numbers indicated vary depending on the customer configuration and the above-stated factors. It must be used as a guideline to determine the approximate range for failover time.

The following table displays the time taken for failover for different configurations (illustration purpose only) using the out-of-the-box gadgets with Agent PG 12.5(1).

<table>
<thead>
<tr>
<th>Affected Users</th>
<th>Number of Gadgets (XML)</th>
<th>LAN or WAN</th>
<th>Time Taken (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>6</td>
<td>LAN</td>
<td>50-55</td>
</tr>
<tr>
<td>2000</td>
<td>6</td>
<td>LAN</td>
<td>70-80</td>
</tr>
<tr>
<td>2000</td>
<td>6</td>
<td>WAN (RTT of 400 milliseconds)</td>
<td>80-110</td>
</tr>
</tbody>
</table>

**Note**

- The time indicated does not include the Finesse or CTI server recovery time. It only indicates the time taken for the desktop to reconnect all agents post detecting a reachable Finesse server, which is IN_SERVICE.

- Deployments with 2000 active users and configuring more than eight XML-gadgets per user on average, or more than six JSP-based gadgets per user on average, are recommended to deploy Cisco Finesse OVA with 8 vCPUs.

- During failover, agents are redirected to the subscriber and are signed in automatically, and desktop is reloaded. Expected bandwidth utilization reaches up to approximately 250 Mbps for 90 seconds (peak), to ensure all 2000 agents failover successfully from one side to another. The bandwidth requirements increase depending on the type and number of gadgets configured for teams.
Backup and Restore

Cisco Finesse uses the backup and restore tools that are provided by the common Cisco Unified Communications platform services for complete data backup-and-restore capabilities. Cisco DRS allows you to perform regularly scheduled automatic or user-invoked data backups and to restore data if the system fails.

To access the Disaster Recovery System (DRS) application, direct your browser to the following URL: https://FQDN:8443/drf, where FQDN is the fully-qualified domain name of your Finesse server.

Note
Cisco Finesse does not support One-Step Restore with the DRS application.

In the case of high availability (HA), Cisco DRS performs a cluster-level backup, which means that it collects backups for all servers to Cisco Finesse and archives the backup data to a remote SFTP server.

DRS backs up and restores its own settings, that is, backup device settings (saved in file drfDevice.xml) and schedule settings (saved in file drfSchedule.xml) as part of the platform component. Once a server is restored with these files, you do not need to reconfigure DRS backup device and schedule settings.

Note
Cisco DRS uses the SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the publisher and subscriber nodes. Cisco DRS uses the IPSec certificates for its Public/Private Key encryption. If you delete the IPSec truststore (hostname.pem) file from the Certificate Management pages, then Cisco DRS will not work as expected. If you delete the IPSec-trust file manually, then you must ensure that you upload the IPSec certificate to the IPSec-trust. For more information about the certificate management, see, Cisco Unified Communications Manager Security Guide at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
Important Considerations

Following are the important considerations when you perform the backup and restore procedures:

• Before you run a backup or a restore, make sure that both nodes in a cluster are running the same version of Cisco Finesse. If different nodes are running different versions, you will have a certificate mismatch and your backup or restore fails.

• Before you restore Cisco Finesse, make sure that the hostname, IP address, DNS configuration, version, and deployment type matches the hostname, IP address, DNS configuration, version, and deployment type of the backup file that you want to restore.

• Before you restore Cisco Finesse, ensure that the version that is installed on the server matches the version of the backup file that you want to restore. Cisco DRS supports restore only for matching versions of Cisco Finesse. For example, Cisco DRS does not allow you to restore from Version 8.5(1).1000-1 to Version 9.0(1).1000-1, or from Version 8.5(2).1000-1 to Version 9.0(1).1000-2.

• Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.

• After you use the recovery disk to bring a server with a corrupted file system into a bootable and semi-functional state, rebuild the server.

Note If you do not rebuild the server, you may notice missing directories, lost permissions, or corrupted soft links.

SFTP Requirements

To back up data to a remote device on the network, you must have an SFTP server that is configured and accessible from the Cisco Finesse node to run the backup. Cisco allows you to use any SFTP server products that have been certified with Cisco through the Interoperability Verification Testing (IVT) process. Cisco Developer Network (CDN) partners, such as GlobalSCAPE, certify their products with a specified version.

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

• Open SSH (see http://sshwindows.sourceforge.net/)
• Cygwin (see http://www.cygwin.com/)
• Titan (see http://www.titanftp.com/)

Cisco does not support use of the SFTP product freeFTPd, because it has a 1-GB file-size limit.
For issues with third-party products that have not been certified through the IVT process, contact the third-party vendor for support.

While a backup or restore is running, you cannot perform any Operating System (OS) Administration tasks because Cisco DRS blocks all OS Administration requests. However, you can use CLI commands to back up or restore the system.

Master and Local Agents

Added content as part of CSCvp71798

The system automatically starts the Master Agent service on each node of the cluster, but it is functional only on the first node. Both servers in the Cisco Finesse cluster must have Local Agent running to perform the backup and restore functions.

By default, a Local Agent automatically gets activated on each node of the cluster.

Master Agent Duties

Added content as part of CSCvp71798

The Master Agent (MA) performs the following duties:

- Stores system-wide component registration information.

- Maintains a complete set of scheduled tasks in an XML file. The MA updates this file when it receives updates of schedules from the user interface. The MA sends executable tasks to the applicable Local Agents, as scheduled. Local Agents execute immediate backup tasks without delay.

- Lets you perform activities such as configuring backup devices, scheduling backups by adding new backup schedules, viewing or updating an existing schedule, displaying status of executed schedules, and performing system restoration.

- Stores backup data on a remote network location.

Local Agent Duties

In the Cisco Finesse cluster, the Local Agent runs backup and restore scripts on each node in the cluster.

Cisco DRS uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the publisher and subscriber nodes. Cisco DRS uses IPSec certificates for its Public/Private Key encryption. This certificate exchange is handled internally; you do not need to make any configuration changes to accommodate this exchange.
Backup Tasks

You can perform the following backup tasks using Cisco DRS:

- Create and manage backup devices
- Create and manage backup schedules
- Perform manual backup and check backup status
- Estimate size of backup tar file
- View history of last 20 backups

Manage Backup Devices

Before using Cisco DRS, you must configure the locations where the backup files will be stored. You can configure up to ten backup devices. Perform the following steps to configure backup devices.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Access the DRS application (<a href="https://Finesse">https://Finesse</a> server IP:8443/drf).</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select <strong>Backup &gt; Backup Device</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Add New</strong> to add a new device or click the device name to edit settings of an existing backup device.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the backup device name and select destination. For more details on the field description, see the detailed online help provided with the DRS application.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

*Note*  You cannot delete a backup device that is configured as the backup device in a backup schedule.

Manage Backup Schedules

You can create up to ten backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, and a storage location.

*Caution*  Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Access the DRS application (<a href="https://Finesse">https://Finesse</a> server IP:8443/drf).</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select <strong>Backup &gt; Scheduler</strong>.</td>
</tr>
</tbody>
</table>
Step 3
Click Add New to add a new schedule or click the schedule name to edit settings of an existing backup schedule.

Step 4
Enter the backup schedule name, select the backup device, and select feature as Finesse.

Step 5
Enter the backup date and frequency details as required. For more details on the field description, see the detailed online help provided with the DRS application.

Step 6
Click Save.

Step 7
Select a schedule from the Schedule List and then click Enable Selected Schedules.

**Note**
- If you plan to schedule a backup on a two-node deployment, ensure that both the servers in the cluster are running the same version of Cisco Finesse and are communicating in the network. Servers that are not communicating at the time of the scheduled backup will not be backed up.
- Do not schedule a backup to run while the Update Database Statistics task is running. By default, this task is set to run every Saturday at 3:00 a.m. and Shrink-repack on Sunday at 3:00 a.m..

---

### Perform Manual Backup

**Procedure**

**Step 1**

**Step 2**
Select Backup > Manual Backup.

**Step 3**
Select a backup device and feature as Finesse.

**Step 4**
Click Start Backup to start the manual backup.

**Note**
Click Estimate Size to get the approximate size of the disk space that the backup file consumes on the SFTP server.

To perform backup tasks on virtual machines, see Unified Communications VMware Requirements, at:https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html.

---

### Check Backup Status

**Procedure**

**Step 1**

**Step 2**
Select Backup > Current Status to check the backup status.
Caution  The backup to the remote server to be completed within 20 hours otherwise the backup session times out and you will have to start the fresh backup.

---

## Restore the Nodes 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 and the secondary Finesse nodes (publisher and subscriber node). Perform the following steps to restore the Finesse nodes to its last backed up state.

⚠️ **Caution**  Cisco Finesse data can only be retrieved from the backup file. The recent Finesse configuration data, which is not backed up, must be manually configured in the Cisco Finesse administration console after the restore.

### 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 2**  Access the DRS application (https://Finesse server IP:8443/drf).

**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 and feature as **Finesse**.

**Step 6**  When prompted to choose the nodes, either choose both nodes or choose each node to individually restore them.

**Step 7**  After the restore process is complete, restart the node.

**Step 8**  Run the following command on the primary Finesseserver:

```
utils dbreplication stop all
```

**Step 9**  Run the following CLI command on the primary Finesseserver to set up replication:

```
utils dbreplication reset all
```

**Note**  The dbreplication reset command can take some time to complete.

Run the CLI command **utils dbreplication runtimestate** on the primary Finesseserver. If the RTMT counter value for replication status is 2 on all nodes, replication is functioning properly.
After the installation is complete, check that the dbreplication is functioning and allowing 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`.

---

Note

After the installation is complete, check that the dbreplication is functioning and allowing 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`. 
Backup and Restore

Restore the Nodes in HA Setup with Rebuild
Supported Cisco Unified Communications OS Services

The following sections list the Cisco Unified Communications OS services that Cisco Finesse supports. For more information about CLI commands, see 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. As 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
• show network ipv6 settings
• show tls server min-version
• show tls client min-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 forcedatasynccSUB
• utils dbreplication reset
• utils dbreplication runtimestate
• utils dbreplication setreptimeout
• 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
• utilssystem boot
• utilssystem restart
• utilssystem upgrade
• utilsvmtools status

Set Commands
• set network ipv6 gateway
• set network ipv6 service disable
• set network ipv6 service enable
• set network ipv6 static_address
• set tls server min-version <version>
• set tls client min-version <version>

Note
Cisco SNMP integration with Finesse is restricted to platform MIBs. Finesse does not have any application-specific MIBs.
Cisco Finesse CLI

- Commands Supported for Cisco Finesse, on page 167
- Cisco Finesse Services, on page 167
- Cisco Finesse Trace Logging, on page 168
- Toaster Notifications, on page 169
- Finesse IPPA Inactivity Timeout, on page 169
- Configuring Queue Statistics, on page 170
- Cross-Origin Resource Sharing (CORS), on page 171
- Gadget Source Whitelisting, on page 174
- Supported Content Security Policy Directives, on page 175
- Finesse System Commands, on page 176
- Desktop Properties, on page 177
- Service Properties, on page 185
- Log Collection Schedule, on page 188
- Upgrade, on page 189
- Shutdown, on page 190
- Replication Status, on page 190
- View Property, on page 191
- Update Property, on page 191
- Signout from Media Channels, on page 191

Commands Supported for Cisco Finesse

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

Cisco Finesse Services

To view, start, or stop services:

- **show network all detail**: View the platform TCP/IP services, UDP services, and Unix domain sockets used by Cisco Finesse:

- **utils service list**: This command retrieves a list of all services and their status.

  Services are shown in one of the following states:
STOPPED means the service is not running. STARTING means the service is starting operation and performing any necessary initialization. STARTED means the service has successfully initialized and is operational.

- **utils service start service name**: This command starts the named service.
- **utils service stop service name**: This command stops the named service.
- **utils service start Cisco Finesse Tomcat**: This command starts Cisco Finesse Tomcat.
- **utils service stop Cisco Finesse Tomcat**: This command stops Cisco Finesse Tomcat.
- **utils service restart Cisco Finesse Tomcat**: This command restarts Cisco Finesse Tomcat.

---

**Note**
If a Cisco Finesse service-related problem exists, restart the Finesse service. Note that most service-related problems cannot be corrected by restarting a service.

---

### Cisco Finesse Trace Logging

Use the following commands to toggle trace logs for Cisco Finesse, enable trace logs for Finesse IPPA, and enable debug logs for realm.

---

**Note**
Enabling trace logging may cause an overload in the system and must be used for debugging purposes only.

- **utils finesse trace enable**:

  This command allows you to:
  - Enable trace logs for Cisco Finesse.
  - Turn on command dispatcher logs.
  - Enable trace logs for Finesse IPPA.
  - Enable debug logs for Realm.

- **utils finesse trace disable**

  This command allows you to:
  - Disable trace logs for Cisco Finesse.
  - Turn off command dispatcher logs.
  - Disable trace logs for Finesse IPPA.
  - Disable debug logs for Realm.
After execution of each command, wait for 60 seconds for the changes to take effect.

Note
- **utils finesse trace status**
  This command allows you to display status as:
  - Enabled - When all four actions are enabled.
  - Disabled - When all four actions are disabled.

If all actions are not enabled or disabled, a warning message is displayed.

### Toaster Notifications

Toaster notifications are enabled by default after a fresh installation of Cisco Finesse. Use the following CLI commands to disable, enable, and check the status of the toaster notifications:

- **utils finesse toaster enable [closeTimeout]**: This command enables the Cisco Finesse toaster notification.

  **Note** While enabling toaster notification, use the `closeTimeout` parameter (timeout in seconds) to set the time interval after which toaster automatically closes. If no parameter is specified, timeout is set to 8 seconds by default. The valid range for timeout activity is between 5-15 seconds. The browser must be refreshed for timeout changes to take effect.

  The `closeTimeout` parameter is applicable only for Chrome and Firefox browsers in Windows OS. In macOS, Chrome and Firefox browsers automatically close the toaster notification.

- **utils finesse toaster disable**: This command disables the Cisco Finesse toaster notification.

- **utils finesse toaster status**: This command displays the status (enable or disable) of the Cisco Finesse toaster notification.

**Note** Cisco Finesse Toaster Notification does not work with Internet Explorer browser.

### Finesse IPPA Inactivity Timeout

Use the following CLI commands to enable or disable the Inactivity Timeout feature in Finesse IPPA. You must either disable the Finesse Inactivity Timeout feature or increase the timeout in the range of 120 seconds to one day (in seconds), so that the Finesse IPPA agent is not logged out if on any other screen:

- **utils finesse ippa_inactivity_timeout enable**: This command enables Finesse IPPA Inactivity Timeout.
The default time set for inactivity timeout is 120 seconds.

- **util finesse ippa_inactivity_timeout disable**: This command disables Finesse IPPA Inactivity Timeout.

  **Note**: When inactivity timeout is disabled, you will not be logged out of Finesse IPPA, if the agent is on any other screen.

- **util finesse ippa_inactivity_timeout enable inactivity_timeout**: This command enables the Finesse IPPA Inactivity Timeout with timeout set to n seconds.

  **Note**: Minimum value of n must be 120 seconds and maximum value can be up to one day (86400 seconds).

- **util finesse ippa_inactivity_timeout status**: This command checks the status of Finesse IPPA Inactivity Timeout.

**Note**: The Finesse IPPA Inactivity Timeout CLIs should be run on primary and secondary Finesse servers. Enabling or disabling this feature requires a restart of Cisco Finesse Tomcat, and restart must be done in the maintenance window. During upgrade, the inactivity timeout configuration is not retained and should be re-configured post upgrade.


---

### Configuring Queue Statistics

The Queue Statistics gadget is enabled by default as part of Cisco Finesse new installation (Unified CCE only). When performing a system upgrade from Cisco Finesse 11.5(1), the desktop custom layout needs to be modified by the administrator for the Queue Statistics gadget to be displayed on the Agent and Supervisor desktop.

Use the following CLI commands to enable and disable the queue statistics polling or check the status of the queue statistics polling:

- **util finesse queue_statistics enable**

- **util finesse queue_statistics disable**

- **util finesse queue_statistics status**

After performing a system upgrade, during switch-version the queue statistics polling will be enabled by default. The procedure to disable the queue statistics polling remains the same.
Cross-Origin Resource Sharing (CORS)

CORS support to third-party web server is disabled by default for Cisco Finesse and OpenFire. Use the following CLIs to enable CORS for Cisco Finesse and OpenFire and configure the allowed origin list:

Note
CORS support to third-party clients is enabled for all origins by default in Cisco Finesse and OpenFire. This corresponds to the enable_all mode below.

Important
After you make changes to the CORS status or to the allowed origin list, restart Cisco Finesse Tomcat and Notification Services for changes to take effect.

• **utils finesse cors enable_all**: This command allows all origins to make cross domain requests. It responds and allows CORS preflight requests from any domain to make Finesse API/OpenFire requests.

  Note
  This is not a secure configuration and is included only to support backward compatibility.

• **utils finesse cors enable**: This command allows CORS for Cisco Finesse APIs and OpenFire requests for whitelisted origins. It responds to browser CORS preflight requests and allows valid whitelisted domains to make Finesse API/OpenFire requests.

  Note
  Use the `utils finesse cors allowed_origin` CLI to customize the whitelisted origins. Any custom headers used in the CORS requests have to be added using `utils finesse cors allowed_headers` CLI.

• **utils finesse cors disable**: This command restricts CORS for Cisco Finesse APIs and OpenFire requests. It disallows or prevents CORS preflight requests from any external domain to make Finesse API and OpenFire requests.

  Note
  If allowed origin list is already present, then the list is preserved and used when CORS is enabled. Note that the CLI changes are reflected only after you clear your cache and close and re-open the browser.

• **utils finesse cors status**: This command displays the CORS status (enable_all, enabled, or disabled) on the console.
For allowing any other header, the following set of CLI commands are added to enable CORS for both Cisco Finesse and OpenFire and configure the allowed origin list:

- **utils finesse cors allowed_origin list**: This command lists all the origins in the allowed origin list.
- **utils finesse cors allowed_origin add**: This command adds origins to the allowed origin list. Origins can be added by using a comma separated string. For example:
  
  ```bash
  utils finesse cors allowed_origin add https://origin1.com:[port]
  utils finesse cors allowed_origin add https://origin1.com:[port],https://origin2.com:[port]
  ```

  **Note**
  The wildcard character * is not a valid origin in the allowed origin list.

- **utils finesse cors allowed_origin delete**: This command deletes origins from the allowed origin list.

  ```bash
  utils finesse cors allowed_origin delete
  1: http://google.com
  2: https://www.cisco.com
  3: https://def.com
  4: https://abc.com:7777
  a: all
  q: quit
  ```

  **Note**
  Delete will list all the origins in the allowed origin list, of which origins can be deleted by selecting the correct choice. For example:

  ```bash
  utils finesse cors allowed_origin delete
  ```

  ```bash
  1: http://google.com
  2: https://www.cisco.com
  3: https://def.com
  4: https://abc.com:7777
  a: all
  q: quit
  ```

  Select the index of origin(s) to be deleted [1-4 or a,q]

By default the following headers are allowed and exposed:


**Note**
These headers cannot be modified. Custom headers can be added or removed using the following CLIs:

- **utils finesse cors allowed_headers list**: This command lists all the allowed headers for CORS. The list is used to validate incoming requests to Finesse.
- **utils finesse cors allowed_headers add**: This command adds one or more allowed headers for CORS. Multiple headers can be added as a comma separated string. For example:
utils finesse cors allowed_headers add header1
utils finesse cors allowed_headers add header1,header2,header3

Note Wildcard character * is not supported.

- **utils finesse cors allowed_headers delete**: This command lists the choices for deleting the allowed headers. The choice should be an index as displayed in the list of allowed headers. The list provides the option to delete a single header or all configured custom headers. For example:

```
utils finesse cors allowed_headers delete
1: header1
2: header2
a: all
q: quit
```
Select the index of allowed header to be deleted [1-2 or a,q]: 1

- **utils finesse cors exposed_headers list**: This command lists all the exposed headers for CORS. The list will be used by the browser to validate the accessible headers in the response.

- **utils finesse cors exposed_headers add**: This command adds one or more exposed headers for CORS. Multiple headers can be added by a comma separated string. For example:

```
utils finesse cors exposed_headers add header1
utils finesse cors exposed_headers add header1,header2,header3
```

Note Wildcard character * is not supported

- **utils finesse cors exposed_headers delete**: This command lists the choices for deleting the exposed headers. The choice should be an index as displayed in the list of allowed headers. The list provides the option to delete a single header or all configured custom headers. For example:

```
utils finesse cors exposed_headers delete
1: header1
2: header2
a: all
q: quit
```
Select the index of exposed header to be deleted [1-2 or a,q]: 1

All CLIs are node specific and must be executed on all nodes in the cluster.
Gadget Source Whitelisting

Shindig proxies requests from the Finesse desktop to external servers and this introduces the possibility of server side request forgery (SSRF). To prevent SSRF, you can choose to allow outgoing connections for specified sources to be used in the gadgets by adding URLs to the whitelist. Note that this functionality is disabled by default for Cisco Finesse.

Use the following CLIs to enable or disable Gadget Source Whitelist functionality and to configure source(s) in the whitelist:

**utils finesse gadget_source_check enable**  This command enables whitelist for Cisco Finesse.

**utils finesse gadget_source_check disable**  This command disables whitelist for Cisco Finesse.

**utils finesse gadget_source_check status**  This command prints the whitelist status (enabled or disabled) on Cisco Finesse console.

**utils finesse gadget_source_check whitelist list**  This command lists all the source(s) in the whitelist.

**utils finesse gadget_source_check whitelist add**  This command adds source(s) to the whitelist. For Example,

```
utils finesse gadget_source_check whitelist add https://www.abc.com:8445
```

Note: Wildcard character * is not supported.

The whitelisting feature will not perform hostname resolutions. The format of the whitelist entry should match the format in which the gadget requests for a resource.

**utils finesse gadget_source_check whitelist delete**  This command deletes source(s) from the whitelist. For Example:

```
utils finesse gadget_source_check whitelist delete
1: http://origin1:8080
2: https://origin2:7777
a: all
q: quit
```

Select the index of origin to be deleted [1-2 or a,q]: 1

Note: All CLIs are node-specific and must be executed on all nodes in the cluster.

After any changes are done to gadget source status or to the whitelist, restart Cisco Finesse Tomcat for changes to take effect.
Supported Content Security Policy Directives

**Note**
To enable this feature in Cisco Finesse, install Finesse 12.5(1) ES3 COP or higher.

Content Security Policy (CSP) is a standardized set of security directives that can inform the browser of the policies to be used to help mitigate various forms of attacks. CSP frame-ancestor policy defines the allowable locations from where the Finesse desktop can be accessed as an embedded HTML content, which can help prevent click-jacking attacks.

Use the following CLI commands to view, add, or delete the frame-access sources in the response header of Cisco Finesse. This ensures that only the configured sources can embed the Cisco Finesse in an iFrame within their HTML pages.

**Note**
Internet Explorer does not support frame-ancestors, and therefore will not block any websites from loading Cisco Finesse within it.

- **utils finesse frame_access_whitelist add [source1,source2]**—This command adds one or more frame sources, thereby allowing the configured sources to embed the Cisco Finesse in their iFrames. Multiple sources can be provided as a comma-separated list. The source should be of the following format:
  - `https://<fqdn>:[port]`
  - `https://IP:[port]`

  Wildcard character * is also supported for the FQDN and port entries, which indicates that all the legal FQDN or ports are valid.

```
admin:utils finesse frame_access_whitelist add
Source(s) successfully added.
```

Ensure Source(s) is added to the frame access list in all Finesse nodes in the cluster.

Restart Cisco Finesse Tomcat and Cisco Finesse Notification Service for the changes to take effect:
```
utils service restart Cisco Finesse Tomcat
utils service restart Cisco Finesse Notification Service
```

- **utils finesse frame_access_whitelist delete**—This command displays an indexed list of all the configured frame sources that have been allowed to access Cisco Finesse. Enter the corresponding index number to delete a single source or all the configured sources.

```
admin:utils finesse frame_access_whitelist delete
1: https://www.abc.com:8445
2: https://*.abc.com
3: https://*.abc.com:*
```
4: https://10.21.255.25
a: all
q: quit

Select the index of source to be deleted [1-4 or a,q]: 1
Sources deleted successfully.

Restart Cisco Finesse Tomcat and Cisco Finesse Notification Service for the changes to take effect:
  utils service restart Cisco Finesse Tomcat
  utils service restart Cisco Finesse Notification Service

• **utils finesse frame_access_whitelist list**—This command lists all the frame sources that are allowed to access Cisco Finesse.

```
admin:utils finesse frame_access_whitelist list
```

The following source(s) are configured in the frame access list:
1: https://www.abc.com:8445
2: https://*.abc.com
3: https://*.abc.com:*
4: https://10.21.255.25

---

**Finesse System Commands**

Configure the following Cisco Finesses system CLIs:

**Notifications**

Use the following CLI commands to enable or disable the Cisco Finesses notifications. By default, this feature is disabled.

- To enable: **utils finesse notification logging enable**
- To disable: **utils finesse notification logging disable**

**Node Statistics**

Use the following CLI command to view the run-time statistics for the current node.

- To view: **utils finesse node_statistics list**

```
admin:utils finesse node_statistics list
```

Warning: Running this command frequently will affect system performance.
Press ENTER to continue. Press any other key to exit:

Wait while the statistics (updated every 5 secs) are being fetched...

The following are the runtime statistics for the current node.
Active Dialogs Count: 0
Active Tasks Count: 0
Average Configured Media per Agent Count: 0
Average Logged in Media per Agent Count: 0
Average Skill Groups per Agent Count: 0
Max Skill Groups per Agent Count: 0
Total Time for Finesse to Start (in seconds): 32
Logged in Agents on current node: 0
Unique Configured Skill Groups per Agent Count: 0

For more information, see RuntimeConfigInfo API Parameters section in the Cisco Finesse Web Services Developer Guide at https://developer.cisco.com/docs/finesse/.

Desktop Properties

Configure the desktop properties using the following CLIs for the features.

Note

Refresh the browser for the changes to take effect.

Active Call Details in the Team Performance Gadget
Use the following CLI commands to enable or disable the active call details.

• To enable: utils finesse set_property desktop showActiveCallDetails true
• To disable: utils finesse set_property desktop showActiveCallDetails false

View History in the Team Performance Gadget
Use the following CLI commands to enable or disable the agent history.

• To enable: utils finesse set_property desktop showAgentHistoryGadgets true
• To disable: utils finesse set_property desktop showAgentHistoryGadgets false

Force Wrap-Up Reason
Use the following CLI commands to enable or disable the force wrap-up reason.

• To enable: utils finesse set_property desktop forceWrapUp true
• To disable: utils finesse set_property desktop forceWrapUp false

Show Wrap-Up Timer
Use the following CLI commands to show or hide the timer in wrap-up state. By default, the value of this property is set to true.

• To hide the timer in wrap-up state: utils finesse set_property desktop showWrapUpTimer false
• To display the timer in wrap-up state: utils finesse set_property desktop showWrapUpTimer true

Wrap-Up Timer Count Down
Use the following CLI commands to set the wrap-up timer to count down or count up the time. By default, the value of this property is set to true.
• To count up the time: `utils finesse set_property desktop wrapUpCountDown false`
• To count down the time: `utils finesse set_property desktop wrapUpCountDown true`

**Notification Connection Type**

Use the following CLI commands to update the desktop notification connection type as WebSockets or BOSH. By default the connection type is WebSockets.

- For WebSockets: `utils finesse set_property desktop notificationConnectionType websocket`
- For BOSH: `utils finesse set_property desktop notificationConnectionType bosh`

**Desktop Chat Attachment**

Use the following CLI commands to enable or disable the attachment support in Desktop Chat. Attachments are enabled by default in Desktop Chat.

- To enable: `utils finesse set_property desktop desktopChatAttachmentEnabled true`
- To disable: `utils finesse set_property desktop desktopChatAttachmentEnabled false`

**Desktop Chat Maximum Attachment Size**

Use the following CLI commands to configure the attachment size in Desktop Chat. If you do not configure the maximum attachment size, then it is set to 5 MB by default.

- `utils finesse set_property desktop desktopChatMaxAttachmentSize Attachment Size`
  
  For example, to set the maximum attachment size to 2 MB, use:
  
  `utils finesse set_property desktop desktopChatMaxAttachmentSize 2097152`

  **Note**  
  The maximum attachment size configurable is up to 10 MB.

**Desktop Chat Unsupported File Types**

The .exe, .msi, .sh, and .bat file types are not supported by default. Use the following CLI commands to override the default list and customize the file types that will not be supported in the Desktop Chat. Multiple file types can be added using a comma separated string.

- `utils finesse set_property desktop desktopChatUnsupportedFileTypes File Types`
  
  For example, to set the .jar and .bin as unsupported file types, use:
  
  `utils finesse set_property desktop desktopChatUnsupportedFileTypes jar,bin`

**Automatic Desktop Login Retries**

Cisco Finesse supports automatic desktop login retries when the desktop login fails due to device-related errors. The following properties allow the administrator to control how this feature behaves. By default, the value of this property is set to true.

- To enable: `utils finesse set_property desktop enableRetryLoginFeature true`
  
  If this feature is enabled, then you can define the retry attempts and intervals.
  
  - To set attempts: `utils finesse set_property desktop loginFailureRetryAttempts <value>`
The maximum retry attempts is 10. Default value is 3.

- To set intervals: `utils finesse set_property desktop loginFailureRetryInterval <value>`

The login retry has a configurable amount of delay between each retry to allow the device to recover. The minimum and maximum interval between retries is 15-180 seconds. Default value is 60 seconds.

**Note**
Reducing the retry interval increases the load on the system when there is a system-wide outage of devices.

- To disable: `utils finesse set_property desktop enableRetryLoginFeature false`

**Sign in as a Mobile Agent**

Use the following CLI commands to enable or disable the Sign in as a Mobile Agent feature on the Finesse sign in page. By default, the value of this property is set to true.

- To enable: `utils finesse set_property desktop enableMobileAgentLogin true`
- To disable: `utils finesse set_property desktop enableMobileAgentLogin false`

**Enable or Disable Keyboard Shortcuts**

Use the following CLI commands to enable or disable the keyboard shortcuts for the Finesse agent and supervisor desktop. By default, the value of this property is set to true.

- To enable: `utils finesse set_property desktop enableShortCutKeys true`
- To disable: `utils finesse set_property desktop enableShortCutKeys false`

**Enable or Disable Drag-and-Drop and Resize for a Gadget or Component**

Use the following CLI commands to enable or disable the drag-and-drop and resize features for a gadget or component in the Finesses desktop. By default, the value of this property is set to false.

- To enable: `utils finesse set_property desktop enableDragDropAndResizeGadget true`
- To disable: `utils finesse set_property desktop enableDragDropAndResizeGadget false`


**Configure Desktop Chat Organization Unit (OU) Search**

Use the following CLI commands to configure the OU based user search for the base LDAP context for desktop chat in HCS for CC. By default, the whole LDAP base context is configured in Cisco Unified Communications Manager IM and Presence Service LDAP search settings. For more details on desktop search see, Desktop Chat Server Settings.

To set field key: `utils finesse set_property desktop chatOUSearchFieldKey <value>`

To set field value: `utils finesse set_property desktop chatOUSearchFieldValue <value>`

The following example displays the search criteria set for chat users who belong to specific OU.
admin:utils finesse set_property desktop desktopChatOUSearchFieldKey "OU"

Property successfully updated.
Ensure property is updated in all Finesse nodes in the cluster.

No service restart required. Ensure browser is refreshed for the changes to take effect.

admin:utils finesse set_property desktop desktopChatOUSearchFieldValue "chat"

Property successfully updated.
Ensure property is updated in all Finesse nodes in the cluster.

No service restart required. Ensure browser is refreshed for the changes to take effect.

Enable or Disable Preloading of the Secondary Resources

Use the following CLI commands to enable or disable the preloading of the secondary server resources from the alternate side during desktop sign in. The resources that are preloaded are: images, CSS, JS, and HTML. The preloading reduces latency and improves performance during desktop failover. By default, the value of this property is set to true.

- To enable: `utils finesse set_property desktop preLoadSecondaryResources true`
- To disable: `utils finesse set_property desktop preLoadSecondaryResources false`

Security Banner Message for Desktop Users

Cisco Finesse supports custom banner messages in the desktop Sign In page. The administrator defines the banner message for Finesse desktop users so that they are aware of the security policy while using Cisco Finesse. The banner message can have a maximum of 220 characters. It supports both alphanumeric and special characters. By default, the banner message is not displayed.

- To add the security banner message to the desktop Sign In page: `utils finesse set_property desktop desktopSecurityBannerMessage <value>`

The following example displays the sample security banner that is defined for desktop Sign In page.

```
admin:utils finesse set_property desktop desktopSecurityBannerMessage "IMPORTANT: Finesse may only be accessed by authorized users!"
```

Property successfully updated.
Ensure property is updated in all Finesse nodes in the cluster.

No service restart required. Ensure browser is refreshed for the changes to take effect.

- To remove the security banner message in the desktop Sign In page: `utils finesse set_property desktop desktopSecurityBannerMessage ""`

WORK Mode Retention for Non-Voice

Use the following CLI commands to enable or disable the user to remain in WORK mode after CTI reconnection. The administrator can enable this CLI, to allow the agents to change to an available state in non-voice MRD explicitly after the Finesse desktop and media channels are initialized (contrary to the previous behavior where, agents moving automatically to available state, and causing RONA, because of the delay in re-initialization of the gadgets which handle non-voice media).

By default, the value of this property is set to `true` (disabled).
To enable agent to retain WORK mode after CTI reconnection (non-voice): `utils finesse set_property desktop enableAutoWorkModeStateChange false`

To make the agent available automatically after CTI reconnection (non-voice): `utils finesse set_property desktop enableAutoWorkModeStateChange true`

**Dual-Tone Multi Frequency (DTMF) Desktop Behaviour**

To enable this CLI in Cisco Finesse, install Finesse 12.5(1)ES2 COP or higher.

The Wrap-Up button and the call control buttons Hold, Transfer, Consult, and End are disabled across all calls when DTMF Keypad is opened, and until the responses to all DTMF requests are completed or have timed out.

**DTMF Pending Requests Threshold Count**

When the network or the server is slow to respond, then the response to DTMF requests are delayed. DTMF keypad prevents new operations when more than a configured number of outstanding responses are pending. The default value is 20.

- To configure the DTMF threshold count for pending requests: `utils finesse set_property desktop pendingDTMFTresholdCount <value>`

  The following example displays the sample DTMF threshold count.

  ```
  admin:utils finesse set_property desktop pendingDTMFTresholdCount 15
  Property successfully updated.
  Ensure property is updated in all Finesse nodes in the cluster.
  No service restart required. Ensure the desktop browser is refreshed for the changes to take effect.
  ```

**DTMF Request Timeout**

Cisco Finesse waits for a configured time for each DTMF request. The default timeout is 5 seconds.

- To configure the DTMF timeout for pending requests: `utils finesse set_property desktop dtmfRequestTimeoutInMs <value>`

  The timeout value must be entered in milliseconds.

  The following example displays the sample DTMF timeout count.

  ```
  admin:utils finesse set_property desktop dtmfRequestTimeoutInMs 4000
  Property successfully updated.
  Ensure property is updated in all Finesse nodes in the cluster.
  No service restart required. Ensure the desktop browser is refreshed for the changes to take effect.
  ```
**WebProxy Service**

WebProxy Service acts as a transparent reverse proxy between external clients and the Finesse service. It provides SSL termination and caching services to the Finesse server to reduce latency and improve performance. Configuration changes done on the Finesse server may not be immediately available to the clients due to the intermediary webproxy cache. The administrator can clear the intermediary webproxy cache using `utils webproxy cache clear`.

WebProxy cache is automatically cleared when you restart the Finesse Tomcat service. Static resources (images and scripts), Shindig gadget XML, and resources are cached until the Finesse Tomcat service is restarted or explicitly cleared by the administrator.

For more information on REST API Response Caching, see *REST API Developer Guide* at [https://developer.cisco.com/docs/finesse/](https://developer.cisco.com/docs/finesse/).

The logging level of the WebProxy Service is managed using the web proxy log-levels CLI.

---

**Note**

WebProxy Service CLIs are node-specific and must be executed on all nodes in the cluster.

Proxy cache bypassing reduces performance and must be used for debugging purposes during the gadget development or troubleshooting.

Server cache for the Finesse API can be bypassed by including `bypassServerCache=true` as a query parameter in the request or clear server cache using `utils webproxy cache clear`.

Server cache for the Finesses desktop can be bypassed by including `bypassServerCache=true&nocache` as a query parameter in the desktop URL.

---

**utils webproxy cache clear**

This command clears the cache from the WebProxy Service.

**Command Syntax**

`utils webproxy cache clear  {all | webproxy | desktop | rest | shindig}`

**Options**

- `all`—Clears all the configured caches.
- `webproxy`—Cleans the default webproxy cache.
- `desktop`—Clears the desktop cache. The desktop cache contains static HTML, CSS, scripts, and icons used in the Finesses desktop.
- `rest`—Clears the REST APIs cache. The REST API responses cached are:
  - `ECCVariableConfig`
  - `MediaDomain`
  - TeamResource APIs include ReasonCodes, WrapUpReasons, MediaPropertiesLayouts, PhoneBooks, and WorkFlows. The responses of the TeamResource API are cached at the team-level.
• **shindig**—Clears the Shindig cache. The Shindig cache contains XML gadget definition (ifr request-response) and gadget resources (concat request-response).

**Command Modes**
Administrator (admin)

**Requirements**
Command privilege level: 1
Allowed during upgrade: Yes
Applies to: Unified CCE, Unified CCX, Packaged CCE and HCS for Contact Center

**Example**
```
admin:utils webproxy cache clear desktop
Successfully cleared desktop cache
```

### set webproxy access-log-level

This command sets the log-level for the access logs generated by the WebProxy Service. The access logs record information about all external requests that reach the proxy. The requests are logged in the access log after the request is processed.

**Command Syntax**
```
set webproxy access-log-level {off | info | debug}
```

**Options**
- **off**—Turns off the logging into the access logs of the WebProxy Service.
- **info**—Sets the log-level for access logs of the WebProxy Service to information. This captures the data of each request such as time, client, host, user, and so on.
- **debug**—Sets the log-level for access logs of the WebProxy Service to debug. This captures the detailed data of each request for debugging.

**Note**
Setting the access logs to debug impacts performance. Hence, avoid using in the production deployment.

**Command Default**
The default value is **off**.

**Command Modes**
Administrator (admin)

**Requirements**
Command privilege level: 1
Allowed during upgrade: Yes
Applies to: Unified CCE, Unified CCX, Packaged CCE and HCS for Contact Center
Example

admin:set webproxy access-log-level off
Webproxy access log-level is turned off
admin:set webproxy access-log-level info
Successfully set webproxy access log-level to info
Service restarted

set webproxy log-severity

This command sets the severity of the error logs that are generated by the WebProxy Service. The error logs record information about encountered issues of different severity levels.

Command Syntax

set webproxy log-severity  {debug | warn | error | crit | alert | emerg}

Options

• debug—Sets the severity level to debug.

Note Setting the error logs to debug impacts performance. Hence, avoid using in the production deployment.

• warn—Sets the severity level to warning.
• error—Sets the severity level to error.
• crit—Sets the severity level to critical.
• alert—Sets the severity level to alert.
• emerg—Sets the severity level to emergency.

Command Default
The default value is warn.

Command Modes
Administrator (admin)

Requirements
Command privilege level: 1
Allowed during upgrade: Yes
Applies to: Unified CCE, Unified CCX, Packaged CCE and HCS for Contact Center

Example

admin:set webproxy log-severity warn
Successfully set webproxy log severity to warn
Service restarted
show webproxy access-log-level

This command displays the configured log-level for the access logs of the WebProxy Service.

Command Syntax

show webproxy access-log-level

Command Modes

Administrator (admin)

Requirements

Command privilege level: 1
Allowed during upgrade: Yes
Applies to: Unified CCE, Unified CCX, Packaged CCE and HCS for Contact Center

Example

admin:show webproxy access-log-level
Current webproxy access log-level is: info

show webproxy log-severity

This command displays the configured severity level for the error logs of the WebProxy Service.

Command Modes

Administrator (admin)

Requirements:

Command privilege level: 1
Allowed during upgrade: Yes
Applies to: Unified CCE, Unified CCX, Packaged CCE and HCS for Contact Center

Example

admin:show webproxy log-severity
Current webproxy log-severity is: warn

Service Properties

Configure the service properties using the following CLIs for the features.

Note

The CLIs require Cisco Finesse Tomcat restart except for desktop related properties.

Security Banner Message for Administrators
Cisco Finesse supports custom banner messages in the administration Sign In page. The administrator defines the banner message for the users so that they are aware of the security policy while using Cisco Finesse. The banner message can have a maximum of 220 characters. It supports both alphanumeric and special characters. By default, the banner message is not displayed.

- To add the security banner message to the administrator Sign In page: `utils finesse set_property admin adminSecurityBannerMessage <value>

The following example displays the sample security banner that is defined for the administrator Sign In page.

```
admin:utils finesse set_property admin adminSecurityBannerMessage "IMPORTANT: Finesse may only be accessed by authorized users!"
```

Property successfully updated.
Ensure property is updated in all Finesse nodes in the cluster.

Restart Cisco Finesse Tomcat Service for the changes to take effect:
```nutils service restart Cisco Finesse Tomcat```

- To remove the security banner message in the administrator Sign In page: `utils finesse set_property admin adminSecurityBannerMessage ""

**Enable or Disable User Authentication Discovery API**

Use the following CLI commands to enable or disable the UserAuthMode API. This API allows a client to discover the authentication mode of a user in Unified CCE deployments when the system is in hybrid mode (SSO or non-SSO). By default, this API is enabled.

**Note**

This API does not require HTTP BASIC authentication. It is provided for 3rd party integration to decide if the user authentication must proceed with SSO or non-SSO authentication modes.

- To enable: `utils finesse set_property webservices enableUserAuthMode true`
- To disable: `utils finesse set_property webservices enableUserAuthMode false`

**Enable or Disable Plain XMPP Socket—Port 5222**

Use the following CLI commands to enable or disable the Cisco Finesse Notification Service plain XMPP port (5222). This port can be enabled only if you have third-party solutions that connect directly to the Cisco Finesse Notification Service over plain Transmission Control Protocol (TCP) connection. This port is not required for the Finesse desktop or BOSH/WebSocket based integrations. By default, the port is disabled.

- To enable: `utils finesse set_property webservices enableInsecureOpenfirePort true`
- To disable: `utils finesse set_property webservices enableInsecureOpenfirePort false`

**Enable or Disable Secure XMPP Socket—Port 5223**

Use the following CLI commands to enable or disable the external access to the Cisco Finesse Notification Service TCP-based XMPP port (5223). The port must be enabled for external client connectivity only if you have third-party solutions that connect directly to the Cisco Finesse Notification Service over this port. By default, the port is enabled (value is set to `true`).
When the port is enabled, it can be accessed by the Cisco Finesse nodes (primary and secondary) and by external clients. When the port is disabled, it cannot be accessed by external clients.

- To enable: `utils finesse set_property webservices enableExternalNotificationPortAccess true`
- To disable: `utils finesse set_property webservices enableExternalNotificationPortAccess false`

**Enable or Disable Enforcement of X.509 Certificate Trust Validation**

Use the following CLI commands to enable or disable the validation of the X.509 CA or the self-signed certificate. From Release 12.5(1) onwards, Cisco Finesse validates SSL certificates of all the servers (CUCM and Customer Collaboration Platform) it communicates. This requires the custom CA providers or the self-signed certificates of the server it communicates to be present in the Cisco Finesse Tomcat trust store. If the certificates are not added into the Cisco Finesse trust store, then certain interactions can fail. It is advised to add the certificates into the Cisco Finesse trust store. If any user chooses to ignore the validation, enforcement can be turned off. This CLI allows users to disable or enable validation. By default, the validation is turned on.

- To enable: `utils finesse set_property webservices trustAllCertificates true`
- To disable: `utils finesse set_property webservices trustAllCertificates false`

**Enable or Disable Call Variables Logging**

Use the following CLI commands to enable or disable the call variables logging. The callVariables contain sensitive user information and this property allows the administrator to decide whether the information must be captured in the logs. By default the property is disabled.

- To enable:
  ```
  utils finesse set_property webservices logCallVariables true
  utils finesse set_property fippa logCallVariables true
  ```
- To disable:
  ```
  utils finesse set_property webservices logCallVariables false
  utils finesse set_property fippa logCallVariables false
  ```

**Permissions to Drop Participants from Conference**

To enable this CLI in Cisco Finesse, install Finesse 12.5(1) ES3 COP or higher.

Use the following commands to allow an agent or a supervisor, who is the participant in a conference call, to drop another agent, supervisor, or caller (participants) from the conference call.

- **Note**
  Only agents and supervisors can drop participants in the conference call.
  ```
  utils finesse set_property webservices enableDropParticipantFor supervisor_only
  ```
conference call. The supervisor cannot drop a CTI Route Point, IVR port, a device to which no agent is signed in, or a caller device. By default, this property is set to supervisor_only.

• **utils finesse set_property webservices enableDropParticipantFor conference_controller_and_supervisor**—This command allows,
  
  • the supervisor to drop any agents, CTI Route Point, IVR port, a device to which no agent is signed in, or a caller device in the conference call.

  • the conference controller (an agent who initiated the conference call) to drop another agent, supervisor, CTI Route Point, IVR port, a device to which no agent is signed in, or a caller device in the conference call.

---

**Note**

In Unified CCE deployment, set the **DropAnyPartyEnabled** registry key to 1 in the Dynamic Registry of the CTI server to drop the extensions (CTI Route Point, IVR port, a device to which no agent is signed in, or a caller device) which are not mapped to an agent or a supervisor.


• **utils finesse set_property webservices enableDropParticipantFor all**—This command allows any agent or supervisor in the conference call to drop another agent, supervisor or the caller.

## Log Collection Schedule

Use the following CLIs to create, list, and delete automatic desktop log collection schedules for agents and supervisors. This can also be used for debugging purposes.

**utils finesse desktop_auto_log_collection create**: This command creates a schedule that collects the agent’s browser logs. You can create up to five log collection schedules for up to 15 agents.

While creating the log schedule, specify the agent IDs, log collection interval, and duration up to when the logs are to be collected.

The log collection interval and the duration have to be between 30 to 900 seconds. The logs that are collected during the schedule are received in a .zip file format. The logs are collected at: /opt/cisco/desktop/logs/clientlogs.

**Example:**

```
admin:utils finesse desktop_auto_log_collection create
Initializing command line interface...
Checking Cisco Finesse Tomcat status...
Enter agent IDs to continue. (Maximum 15 agents) [Example : 1001001,1001002] : 1001002
Agent IDs entered: 1001002
Enter duration in seconds.(value between 30 and 900) : 240
Duration entered: 240
```
Enter interval in seconds. (value between 30 and 240) : 60
Interval entered: 60

Successfully scheduled client log collection for the specified agent(s).

Ensure the same is enabled in all the Finesse nodes in the cluster.

**utils finesse desktop_auto_log_collection list**: This command lists all active log collection schedules.

**Example:**

```
admin:utils finesse desktop_auto_log_collection list
```

Initializing command line interface...
Checking Cisco Finesse Tomcat status...
These are the live log collection schedules:

Schedule ID:1 Created At: Thu Jun 6 23:23:53 PDT 2019
Duration: 240 seconds
Frequency: 60 seconds
Agent Ids: 1001002

**utils finesse desktop_auto_log_collection delete**: This command deletes the active log collection schedules. When this command is executed, all the active log collection schedules are displayed and you are prompted to enter the Schedule ID that you want to delete.

**Example:**

```
admin:utils finesse desktop_auto_log_collection delete
```

Initializing command line interface...
Checking Cisco Finesse Tomcat status...
These are the live log collection schedules:

Schedule ID:1 Created At: Thu Jun 6 23:23:53 PDT 2019
Duration: 240 seconds
Frequency: 60 seconds
Agent Ids: 1001002

Enter schedule ID to delete (enter 'all' to delete all): 1
Schedule ID entered: 1
Successfully deleted the log collection with schedule id : 1

---

**Upgrade**

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

**utils system upgrade initiate**: This command allows you to initiate and install upgrades and Cisco Option Package (COP) files from both local and remote directories.

**utils system upgrade cancel**: This command allows you to cancel an upgrade.

**utils finesse layout updateCucGadgetUrl**: This command allows you to change the .jsp references of Cisco Unified Intelligence Center (CUIC) gadgets to .xml with no functional changes.

Cisco Finesse Release 12.5(1) onwards, CUIC supports only XML gadgets. Switching to XML-based gadgets reduces latency and improves performance. After the installation of CUIC or Co-resident deployment, run this command to optimize the loading of CUIC gadgets.

For CUIC Release 12.5(1) gadgets (Live Data and Historical) to load in Cisco Finesse, the administrator must enable CORS on CUIC server using the **utils cuc cors enable** command.
Shutdown

Use the following command to shut down Finesse:

```
utilssystemshutdown
```

If the virtual hosts running the Finesse servers are also shut down during a maintenance event, to power up Finesse after the maintenance event is complete, you must sign in to the ESXi host or its vCenter with vSphere Client and power up the virtual machines for primary and secondary Finesse servers.

Replication Status

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

```
• utilsdbreplicationruntimestate
```

This command returns the replication status on primary and secondary Finesse servers.

- Check the RTMT counter value for replication. If all nodes in the cluster show a replication status of 2, replication is functioning correctly.
- If the RTMT counter value for replication status is 3 or 4 for all nodes in the cluster, replication is set up but an error occurred and replication is not functioning properly.
- If the majority of the nodes show a value of 0 or 1, run the command `utilsdbreplication reset all` from the primary Finesseserver.
- 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.

The DB replication setup must be completed to reflect the following primary node changes to the secondary node.

- Reason Codes
- Wrap-Up Reasons
- Media Properties Layouts
- Phone Books
- Workflows
- Team Message
**View Property**

Use the following CLIs to view the property values across all property files.

- `utils finesse show_property fippa property_name`: To view the specified Finesse IPPA property's value.
- `utils finesse show_property desktop property_name`: To view the specified desktop property's value.
- `utils finesse show_property webservices property_name`: To view the specified web service property's value.
- `utils finesse show_property admin adminSecurityBannerMessage`: To view the specified banner message for the administrator Sign In page.

**Note**
The View property CLIs do not support multiple values.

**Update Property**

Use the following CLIs to update the property values across all property files.

- `utils finesse set_property desktop property_name property_value`: To update an existing property value used by the Finesse desktop service.
- `utils finesse set_property fippa property_name property_value`: To update an existing property value used by the Finesse IPPA service.
- `utils finesse set_property webservices property_name property_value`: To update an existing property value used by the Finesse web service.
- `utils finesse set_property admin adminSecurityBannerMessage`: To update an existing property value used by the Finesse administrator for the security banner message.

**Signout from Media Channels**

The CLI `utils finesse user_signout_channel` is used by the Administrator to configure the media channels from which the users are signed out.

When signing out from Cisco Finesse, the CLI `utils finesse user_signout_channel type` lists all the choices of media channels from which the user is signed out. For example:

- `utils finesse user_signout_channel type`
  1: signout user from voice channel.
  2: signout user from voice and non-voice media channels configured for Cisco Finesse.
  a: signout from all media channels configured for the user.
This is default behavior. It is suitable if the non-voice media is running as a gadget within Finesse Desktop and hence, it is valid to assume that the desktop user cannot handle tasks when signing out of Finesse.

q: quit.

Select the choice of media [1-2 or a,q]: 2

User signout channel type is now changed to "signout user from voice and non-voice media channels configured for Cisco Finesse."

user_signout_channel type must be updated for all Cisco Finesse nodes in the cluster.

For any changes done to media channels, it will take fifteen minutes for the new media channels signout to take effect.

The CLI utils finesse user_signout_channel status displays the type of media channels from which the user is signed out.
Certificates for Live Data

- Certificates and Secure Communications, on page 193
- Export Self-Signed Live Data Certificates, on page 193
- Import Self-Signed Live Data Certificates, on page 194
- Obtain and Upload Third-party CA Certificate, on page 195

Certificates and Secure Communications

For secure Cisco Finesse, Cisco Unified Intelligence Center, and Live Data server-to-server communication, perform any of the following:

- Use the self-signed certificates provided with Live Data.

  Note
  When using 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.

- Obtain and install a Certification Authority (CA) certificate from a third-party vendor.

- Produce a Certification Authority (CA) certificate internally.

Export Self-Signed Live Data Certificates

Live Data installation includes the generation of 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), first export the certificates from Live Data and Cisco Unified Intelligence Center. You must export from both Side A and Side B of the Live Data and Cisco Unified Intelligence Center servers. Once done, import the certificates into Finesse, importing both Side A and Side B certificates into each side of the Finesse servers.

When using other self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in to use the Live Data gadget.
Procedure

Step 1 Sign in to Cisco Unified Operating System Administration on the Live Data server using the following URL: https://hostname of Live Data server/cmplatform.

Step 2 From the Security menu, choose Certificate Management.

Step 3 Click Find.

Step 4 Perform one of the following:
  • If the tomcat-trust 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-trust 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.

Perform these steps for both Side A and Side B.

Step 6 After you have downloaded the Live Data certificates, sign in to Cisco Unified Operating System Administration on the Cisco Unified Intelligence Center server using the following URL: https://hostname of CUIC server/cmplatform, and repeat steps 2 to 5.

What to do next
Import the Live Data and Cisco Unified Intelligence Center certificates into the Finesse servers.

Import Self-Signed Live Data Certificates

To import the certificates into the Finesse servers, use the following procedure:

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration on the Finesse server using the following URL: https://FQDN of Finesse server:8443/cmplatform

Step 2 From the Security menu, choose Certificate Management.

Step 3 Click Upload Certificate.

Step 4 From the Certificate Name drop-down list, choose tomcat-trust.

Step 5 Click Browse and browse to the location of the Live Data or Cisco Unified Intelligence Center certificate (with the .pem file extension).

Step 6 Select the file, and click Upload File.

Step 7 Repeat steps 3 to 6 for the remaining unloaded certificate.

Step 8 After you upload both certificates, restart Cisco Finesse Tomcat on the Finesse server.
What to do next

Perform these steps for both Side A and Side B.

Obtain and Upload Third-party CA Certificate

You can use a Certification Authority (CA) certificate provided by a third-party vendor to establish an HTTPS connection between the Live Data, Finesse, and Cisco Unified Intelligence Center servers.

To use third-party CA certificates:

- From the Live Data servers, generate and download Certificate Signing Requests (CSR) for root and application certificates.
- Obtain root and application certificates from the third-party vendor.
- Upload the appropriate certificates to the Live Data, Unified Intelligence Center, and Finesse servers.

Obtain and Upload Third-party CA Certificate
For Cisco Finesse to communicate with the Cisco IdS server, you must import the Cisco Identity Service (IdS) certificates into Cisco Finesse.

Cisco IdS server includes the 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), first export the Cisco IdS certificates from Cisco IdS server. You must export from both Side A and Side B of the Cisco IdS servers. Once done, import the certificates into Finesse trust store as tomcat-trust, on both Side A and Side B of the Finesse servers.

When using other self-signed certificates, agents must accept the Cisco IdS certificates in the Finesse desktop.

- Export Cisco Identity Service Certificates, on page 197
- Import Cisco IdS Certificates, on page 198

**Export Cisco Identity Service Certificates**

**Procedure**

**Step 1** Sign in to Cisco Unified Operating System Administration on the Cisco IdS server using the following URL: https://hostname of Cisco IdS server: 8443/cmplatform.

**Step 2** Select Security > Certificate Management.

**Step 3** Enter the search criteria as **tomcat-trust** and then click **Find** to filter the certificate.

The tomcat-trust certificates list is displayed. If you do not find the tomcat certificate for your server in the **Certificate List**, then click **Generate Self-signed**. When the certificate generation is complete, reboot your server. Then restart this procedure. For more information on generating the self-signed certificate, see *Cisco Unified Operating System Administration Online Help*.

**Step 4** Click the tomcat-trust certificate hyperlink in the **Common Name** column. The tomcat **Certificate Details** dialog box is displayed.

**Step 5** Click **Download .PEM File**.

**Step 6** Save the .PEM file in your local machine.
What to do next

Perform the same steps for both the primary and secondary Finesse nodes.
Import the Cisco IdS certificates into the Finesse trust store as tomcat-trust.

Import Cisco IdS Certificates

Procedure

Step 1  Sign in to Cisco Unified Operating System Administration on the Finesse server using the following URL: https://FQDN of Finesse server: 8443/cmplatform.
Step 3  From the Certificate Purpose drop-down list, select tomcat-trust.
Step 4  In the Upload File field, click Choose File and browse to the tomcat.pem file that you saved on your system.
Step 5  Click Upload.
Step 6  Reboot the Cisco Finessenode.

Note  Perform the same steps for both the primary and secondary Finessenodes.