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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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 ix
Change History ix
About This Guide x
Audience x
Related Documents x
Communications, Services, and Additional Information x
Field Notice xi
Documentation Feedback xi
Conventions xi

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 6
Produce Certificate Internally 7
Client-Side Certificate Acceptance 9
Client Requirements 9
Deploy Root Certificate for Internet Explorer 9
Set Up CA Certificate for Internet Explorer Browser 10
Add Live Data Reports to Default Desktop Layout 40
Add Live Data Reports to Custom Desktop Layout 41
Add Live Data Reports to Team Layout 42
Modify Live Data Stock Reports for Finesse 44
Configure Live Data Reports with Multiple Views 45

CHAPTER 5 Manage Phone Books 49
   Phone Books and Contacts 49
   Add Phone Book 51
   Edit Phone Book 51
   Delete Phone Book 52
   Import Contacts 53
   Export Contacts 54
   Add Contact 55
   Edit Contact 56
   Delete Contact 56

CHAPTER 6 Manage Reasons 59
   Not Ready Reason Codes 59
      Add Not Ready Reason Code 61
      Edit Not Ready Reason Code 62
      Delete Not Ready Reason Code 63
   Sign Out Reason Codes 64
      Add Sign Out Reason Code 66
      Edit Sign Out Reason Code 67
      Delete Sign Out Reason Code 67
   Predefined System Reason Codes 68
   Manage Reason Code Conflicts During Upgrade 70
   Wrap-Up Reasons 71
      Add Wrap-Up Reason 73
      Edit Wrap-Up Reason 73
      Delete Wrap-Up Reason 74

CHAPTER 7 Manage Team Resources 75
Team Resources  75
Assign Phone Books and Reasons to Team  77
Unassign Phone Books and Reasons from Team  78
Assign Custom Desktop Layout to Team  78
Assign Workflows to Team  79
Unassign Workflows from Team  80

CHAPTER 8
Manage Workflows  81
Workflows and Workflow Actions  81
   Workflow Triggers and Outbound Calls  85
Add Browser Pop Workflow Action  86
Add HTTP Request Workflow Action  87
Edit Workflow Action  88
Delete Workflow Action  89
Add Workflow  90
Edit Workflow  91
Delete Workflow  92

CHAPTER 9
Manage Security  95
HTTP and HTTPS Support  95
Cisco Finesse HTTPS Redirect  95
   HSTS  96
Reset Security or Admin Password  97

CHAPTER 10
Manage Finesse IP Phone Agent  99
Finesse IP Phone Agent  99
One Button Sign In  100
Finesse IP Phone Service Subscription Options  101
Set Up Application User, Web Access, and HTTPS Server Parameters  102
Configure Finesse IP Phone Service in Unified CM  103
Add Service Parameters for One Button Sign In  105
Subscribe Agent Phones to Manual Subscription Service  107
Set Up Agent Access to the Self Care Portal  108
CHAPTER 11

Manage Third-Party Gadgets 109
3rdpartygadget Account 109
Upload Third-Party Gadgets 110
Third-Party Gadget Limitations 111

CHAPTER 12

Perform Routine Maintenance 113
Cisco Finesse Services 113
View, Start, or Stop Services 114
Log Collection 114
Collect Logs Using Cisco Unified Real-Time Monitoring Tool 116
Syslog Support for Critical Log Messages 117
Cisco Finesse Notification Service Logging 119
Remote Account Management 119

CHAPTER 13

Cisco Finesse Failover Mechanisms 121
CTI Failover 121
AWDB Failover 122
Finesse Client Failover 123
Desktop Behavior 124
Finesse IP Phone Agent Failover 127

CHAPTER 14

Backup and Restore 129
Backup and Restore 129
Important Considerations 130
SFTP Requirements 130
Master and Local Agents 131
Master Agent Duties 131
Local Agent Duties 131
Backup Tasks 132
Manage Backup Devices 132
Manage Backup Schedules 132
Perform Manual Backup 133
Check Backup Status 133
Contents

CHAPTER 15  
Supported Cisco Unified Communications OS Services  137  
Supported Cisco Unified Communications OS Services  137

APPENDIX A  
Cisco Finesse CLI  141  
Commands Supported for Cisco Finesse  141  
Cisco Finesse HTTPS Redirect  141  
Finesse Services  142  
Cisco Finesse Notification Service Logging  143  
Cisco Finesse Trace Logging  144  
Cisco Finesse Toaster Notifications  144  
Cisco Finesse IPPA Inactivity Timeout  145  
Service Properties  146  
Upgrade  146  
Shutdown  146  
Remote Account Management  147  
Replication Status  147  
3rdpartygadget Account  147  
Configuring Queue Statistics  148

APPENDIX B  
Certificates for Live Data  149  
Certificates and Secure Communications  149  
Export Self-Signed Live Data Certificates  149  
Import Self-Signed Live Data Certificates  150  
Obtain and Upload Third-party CA Certificate  151
Preface

This guide describes how to administer Cisco Finesse.

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

Change History

The following table lists changes made to this guide. Most recent changes appear at the top.

<table>
<thead>
<tr>
<th>Change</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added new service property configuration CLI for port 5223.</td>
<td>May 5, 2020</td>
</tr>
<tr>
<td><strong>Initial Release of the Document for Release 11.6(1)</strong></td>
<td>August 10, 2017</td>
</tr>
<tr>
<td>Cisco Finesse localization supports new languages.</td>
<td></td>
</tr>
<tr>
<td>Configure Proxy Server and Browser proxy in Context Service Settings.</td>
<td></td>
</tr>
<tr>
<td>Cisco Finesse application does not support configuration of QoS settings in network traffic.</td>
<td></td>
</tr>
<tr>
<td>Height adjustment is supported for the Team Performance gadget. The desktop layout XML has been updated to include height adjustment for the Team Performance Gadget.</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>
</table>
| **boldface** font | Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names. For example:  
  * Choose **Edit > Find**.  
  * Click **Finish**. |
<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>italic font</td>
<td>Italic font is used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• To introduce a new term. Example: A <em>skill group</em> is a collection of agents who share similar skills.</td>
</tr>
<tr>
<td></td>
<td>• A syntax value that the user must replace. Example: IF <em>(condition, true-value, false-value)</em></td>
</tr>
<tr>
<td></td>
<td>• A book title. Example: See the <em>Cisco Unified Contact Center Enterprise Installation and Upgrade Guide</em>.</td>
</tr>
<tr>
<td>window font</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>&lt; &gt;</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>
Getting Started

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

• User Accounts, on page 1
• Administration Tools, on page 1
• Certificate Management, on page 5
• QoS Settings, on page 14
• Localization, on page 14

User Accounts

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

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

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

Administration Tools

Cisco Finesse Administration Console

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

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

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

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

• **Phone Books:** Add, edit, or delete phone books or phone book contacts.
- **Reasons:** Add, edit, or delete Not Ready reason codes, Sign Out reason codes, or Wrap-Up reasons.
- **Team Resources:** Assign desktop layouts, phone books, reason codes, and wrap-up reasons to specific teams.
- **Workflows:** Create and manage workflows and workflow actions.

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

---

**Note**

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

---

### Sign In to Cisco Finesse Administration Console

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

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

**Procedure**

#### Step 1

Direct your browser to http://*FQDN*/cfadmin, where *FQDN* is the fully qualified domain name of your primary Finesseserver.

**Note**

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

#### Step 2

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

**Note**

If you are using HTTP to access the administration console, this step is not required.

If you are using HTTPS but have installed a CA Certificate, you can skip this step. For more information about installing a CA Certificate, see the *Cisco Finesse Installation and Upgrade Guide*.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you use Internet</td>
<td>a. A page appears that states this site is untrusted.</td>
</tr>
<tr>
<td>Explorer:</td>
<td>b. Click <strong>More information</strong> &gt; <strong>Go on to the webpage</strong>.</td>
</tr>
<tr>
<td>If you use Edge</td>
<td>a. A page appears that states this site is untrusted.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Details</strong> and click <strong>Go on to the webpage</strong>.</td>
</tr>
<tr>
<td>If you use Firefox:</td>
<td>a. A page appears that states this connection is untrusted.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>I Understand the Risks</strong>, and then click <strong>Add Exception</strong>.</td>
</tr>
</tbody>
</table>
**Option** | **Description**
--- | ---
c. In the Add Security Exception dialog box, ensure the **Permanently store this exception** check box is checked. 
d. Click **Confirm Security Exception**.

If you use Chrome:
a. A page appears that states this connection is not private.
b. Click **Advanced**.
c. Click the http://FQDN of Finesse Server/ link.
d. Enter your agent ID or username, password, and extension, and then click **Sign In**.
The following message appears:
Establishing encrypted connection...
A dialog box appears that lists the certificates to accept.
e. Click **OK**.

---

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

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

**Step 5**
Click **Sign In**.
A successful sign-in launches an interface with defined administration gadgets and a Sign Out link.

---

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

**Sign In Using IPv6**

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

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

- For HTTP access, enter:
  http://<FQDN>:8082/cfadmin

The remaining steps of the sign-in procedure remain the same for IPv6.

**Account Locked After Five Failed Sign In Attempts**

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

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

---

**Note**

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

To view whether a user account is locked, enter the following CLI command:

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

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

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

---

**CLI**

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

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

**Related Topics**

- [User Accounts](#), on page 1

---

**Cisco Unified Communications Operating System Administration**

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

- **Show**: View information on cluster nodes, hardware status, network configuration, installed software, system status, and IP preferences.

- **Settings**: Display and change IP settings, network time protocol (NTP) settings, SMTP settings, time, and version.

---

**Important**

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

- **Security**: Manage certificates and set up and manage IPSec policies.

- **Software Upgrades**: Perform and upgrade or revert to a previous version.

- **Services**: Use the Ping and Remote Support features.
Sign In to Cisco Unified Communications Operating System Administration

Procedure

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

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

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

Related Topics
User Accounts, on page 1

Certificate Management

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

Finesse does not support wildcard certificates. After you upload a root certificate signed by a Certificate Authority, the self-signed certificates are overwritten.

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

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

Server-Side Certificate Management

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

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

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

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

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

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

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

Procedure

Step 1
Generate a CSR.

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

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

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

Step 2
Download the CSR.

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

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

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

https://FQDN of secondary Finesse server:8443/cmplatform
Step 4  Use the CSRs to obtain the CA root certificate, intermediate certificate, and signed application certificate from the Certificate Authority.

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

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

Step 6  Upload the root certificate.
   a) From the Certificate Purpose drop-down list, select tomcat-trust.
   b) In the Upload File field, click Browse and browse to the root certificate file.
   c) Click Upload File.

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

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

Step 9  After the upload is complete, sign out from the Platform Admin page of Finesse.

Step 10  Access the CLI on the primary Finesse server.

Step 11  Enter the command utils service restart Cisco Finesse Notification Service to restart the Cisco Finesse Notification service.

Step 12  Enter the command utils service restart Cisco Finesse Tomcat to restart the Cisco Finesse Tomcat service.

Step 13  Upload the application certificate to the secondary Finesse server.
   You do not need to upload the root and intermediate certificates to the secondary Finesse server. After you upload these certificates to the primary server, they are replicated to the secondary server.

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

Produce Certificate Internally

Set up Microsoft Certificate Server for Windows 2008 R2

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

Procedure

Step 1  Click Start, right-click Computer, and select Manage.
Step 2  In the left pane, click Roles.
Step 3  In the right pane, click Add Roles.
Set up Microsoft Certificate Server for Windows Server

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

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

Procedure

Step 1 In Windows, open the Server Manager.
Step 2 In the Quick Start window, click Add Roles and Features.
Step 3 In the Set Installation Type tab, select Role-based or feature-based installation, and then click Next.
Step 4 In the Server Selection tab, select the destination server then click Next.
Step 5 In the Server Roles tab, check the Active Directory Certificate Services box, and then click the Add Features button in the pop-up window.
Step 6 In the Features and AD CS tabs, click Next to accept default values.
Step 7 In the Role Services tab, verify that Certification Authority box is checked, and then click Next.
Step 8 In the Confirmation tab, click Install.
Step 9 After the installation is complete, click the Configure Active Directory Certificate Service on the destination server link.
Step 10 Verify that the credentials are correct (for the domain Administrator user), and then click Next.
Step 11 In the Role Services tab, check the Certification Authority box, and then click Next.
Step 12 In the Setup Type tab, select Enterprise CA, and then click Next.
Step 13 In the CA Type tab, select Root CA, and then click Next.
Step 14 In the Private Key, Cryptography, CA Name, Validity Period, and Certificate Database tabs, click Next to accept default values.
Step 15 Review the information in the Confirmation tab, and then click Configure.
Download CA certificate

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

Procedure

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

Client-Side Certificate Acceptance

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

Client Requirements


Note

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

Deploy Root Certificate for Internet Explorer

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

Note

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

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the Windows domain controller, navigate to Administrative Tools &gt; Group Policy Management.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>Users who have strict Group Policy defined on the Finesse Agent Desktop are required to disable Cross Document Messaging from Group Policy Management to ensure proper functioning of Finesse on Internet Explorer 11.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Right-click Default Domain Policy and select Edit.</td>
</tr>
</tbody>
</table>
Set Up CA Certificate for Internet Explorer Browser

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

In environments where users do not log directly into 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**

1. In Windows Explorer, double-click the `ca_name.cer` file (in which `ca_name` is the name of your certificate) and then click **Open**.
2. Click **Install Certificate > Next > Place all certificates in the following store**.
3. Click **Browse** and select **Trusted Root Certification Authorities**.
4. Click **OK**.
5. Click **Next**.
6. Click **Finish**.
7. *A message appears that states you are about to install a certificate from a certification authority (CA).*
8. Click **Yes**.
9. *A message appears that states the import was successful.*
10. To verify the certificate was installed, open Internet Explorer. From the browser menu, select **Tools > Internet Options**.
11. Click the **Content** tab.
12. Click **Certificates**.
13. Click the **Trusted Root Certification Authorities** tab.
14. Ensure that the new certificate appears in the list.
15. 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.

**Procedure**

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

**Trust Self-Signed Certificate**

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

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

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In your browser, enter the URL for the administration console (<a href="https://FQDN">https://FQDN</a> of the primary Finesse server/cfadmin) or the agent desktop (<a href="https://FQDN">https://FQDN</a> of the primary Finesse server/desktop).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Perform the steps in the following table for the browser you are using.</td>
</tr>
<tr>
<td>Option</td>
<td><strong>If you use Internet Explorer:</strong></td>
</tr>
<tr>
<td>Description</td>
<td>A page appears that states there is a problem with the website's security certificate. Click <strong>Continue to this website (not recommended)</strong>. This action opens the sign in page for the administration console (or agent desktop). A certificate error appears in the address bar of your browser.</td>
</tr>
<tr>
<td>Option</td>
<td>Click <strong>Certificate Error</strong>, and then click <strong>View Certificates</strong> to open the Certificate dialog box.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| c.     | In the Certificate dialog box, click **Install Certificate**. This action opens the Certificate Import Wizard.  
**Note** If you use Internet Explorer 11, you must add Finesse to your trusted sites before the Install Certificate option appears (**Internet Options** > **Security** > **Trusted Sites** > **Sites**).  
After you click **Install Certificate**, under **Store Location**, select **Current User** to install the certificate for the current user only, or select **Local Machine** to install the certificate for all Windows users who use this computer. |
| d.     | Click Next. |
| e.     | Select **Place all certificates in the following store**, and then click **Browse**. |
| f.     | Select **Trusted Root Certification Authorities**, and then click **OK**. |
| g.     | Click Next. |
| h.     | Click **Finish**. |
| i.     | If a Security Warning dialog box appears that asks if you want to install the certificate, click **Yes**.  
A Certificate Import dialog box that states the import was successful appears. |
| j.     | Click **OK**. |
| k.     | Enter your credentials, and then click **Sign In**. |

If you use Firefox:  

| a.     | A page appears that states this connection is untrusted. |
| b.     | Click **I Understand the Risks**, and then click **Add Exception**. |
| c.     | In the Add Security Exception dialog box, ensure the **Permanently store this exception** check box is checked. |
| d.     | Click **Confirm Security Exception**.  
The page that states this connection is untrusted automatically closes and the administration console (or agent desktop) loads. |
| e.     | Enter your credentials, and then click **Sign In**. |
| f.     | For the agent desktop only, an error appears that states Finesse cannot connect to the Cisco Finesse Notification Service and prompts you to add a security exception for the certificates issued by the Finesseserver.  
Click **OK**. |
Add Certificate for HTTPS Gadget

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

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

Note

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

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

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

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

Procedure

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

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 Finesse server.

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

b) Click Security > Certificate Management.

c) Click Upload Certificate.

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

e) Click Browse and navigate to the tomcat.pem file that you downloaded in the previous step.

f) Click Upload File.

Step 3  Restart Cisco Finesse Tomcat on the primary Finesse server.

Step 4  After synchronization is complete, restart Cisco Finesse Tomcat on the secondary Finesse server.
QoS Settings

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

Localization

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

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

Note

You cannot uninstall a language pack after it is installed.

Table 1: Supported Languages for Desktop User Interface

<table>
<thead>
<tr>
<th>Language</th>
<th>Locale File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulgarian</td>
<td>Bg_BG</td>
</tr>
<tr>
<td>Catalan</td>
<td>Ca_ES</td>
</tr>
<tr>
<td>Czech</td>
<td>Cs_CZ</td>
</tr>
<tr>
<td>Croatian</td>
<td>Hr HR</td>
</tr>
<tr>
<td>Danish</td>
<td>da_DK</td>
</tr>
<tr>
<td>Dutch</td>
<td>nl_NL</td>
</tr>
<tr>
<td>English</td>
<td>en_US</td>
</tr>
<tr>
<td>Finnish</td>
<td>fi FI</td>
</tr>
<tr>
<td>French</td>
<td>fr_FR</td>
</tr>
<tr>
<td>German</td>
<td>de.DE</td>
</tr>
<tr>
<td>Hungarian</td>
<td>Hu_HU</td>
</tr>
<tr>
<td>Italian</td>
<td>it_IT</td>
</tr>
<tr>
<td>Norwegian</td>
<td>nb_NO</td>
</tr>
<tr>
<td>Portuguese</td>
<td>pt_BR</td>
</tr>
<tr>
<td>Romanian</td>
<td>Ro_RO</td>
</tr>
<tr>
<td>Language</td>
<td>Locale File</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Spanish</td>
<td>es_ES</td>
</tr>
<tr>
<td>Swedish</td>
<td>sv_SE</td>
</tr>
<tr>
<td>Slovak</td>
<td>Sk_SK</td>
</tr>
<tr>
<td>Slovenian</td>
<td>Sl_SI</td>
</tr>
<tr>
<td>Serbian</td>
<td>Sr_RS</td>
</tr>
<tr>
<td>Japanese</td>
<td>ja_IP</td>
</tr>
<tr>
<td>Chinese (simplified)</td>
<td>zh_CN</td>
</tr>
<tr>
<td>Chinese (traditional)</td>
<td>zh_TW</td>
</tr>
<tr>
<td>Korean</td>
<td>ko_KR</td>
</tr>
<tr>
<td>Polish</td>
<td>pl.PL</td>
</tr>
<tr>
<td>Russian</td>
<td>ru_RU</td>
</tr>
<tr>
<td>Turkish</td>
<td>tr_TR</td>
</tr>
</tbody>
</table>

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

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

The following items are localized on the desktop:

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

Configuration data defined using the Finesse administration console (such as Not Ready and Sign Out reason code labels, Wrap-Up reason labels, and phonebook entries) do not depend on the locale chosen for the desktop. For example, if you defined a Not Ready reason code with a Chinese label, the label appears on the desktop in Chinese, regardless of the language the agent chooses when signing in.
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>
<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 of the limits in this table are exceeded, the variable data is truncated. This is more likely with localized characters that occupy more than one byte in size (for example, characters with an accent require two bytes to store one character and Asian characters require three or four bytes).

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

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

Finesse does not support the following for localization:

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

**Note**

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

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

**Note**

Locale-based searching and sorting may not work as expected.
Manage System Settings

You can configure CTI server, Administration & Data server, cluster settings, Finesse IP Phone Agent (IPPA), and Cisco Context Service settings on the Settings tab of the Cisco Finesse administration console.

For information about Finesse IPPA settings, see Manage Finesse IP Phone Agent, on page 99.

- Contact Center Enterprise CTI Server Settings, on page 17
- Contact Center Enterprise Administration & Data Server Settings, on page 20
- Cluster Settings, on page 23
- Context Service Settings, on page 23

Contact Center Enterprise CTI Server Settings

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

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

Note

After you make any changes to the values on the Contact Center Enterprise CTI Server Settings gadget, you must restart Cisco Finesse Tomcat. If you must make changes to other settings (such as Contact Center Enterprise Administration & Data Server settings), you can make those changes and then restart Cisco 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.
Although the B Side Host/IP Address and B Side Port fields are not shown as required, an A Side and B Side CTI server are mandatory for a production deployment of Unified CCE and Cisco Finesse.

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

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

Configure the A Side and B Side CTI servers on the primary Finess server.

**Procedure**

**Step 1**  
If you are not already signed in, sign in to the administration console on the primary Finess server:  
http://FQDN of Finess server/cfadmin

**Step 2**  
Sign in with the Application User credentials defined during installation.

**Step 3**  
In the Contact Center Enterprise CTI Server Settings area, enter the CTI server settings as described in the following table. Refer to your configuration worksheet if necessary.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Side Host/IP Address</td>
<td>Enter the hostname or IP address of the A Side CTI server. This value is typically the IP address of the Peripheral Gateway (PG). The CTI server runs on the PG.</td>
</tr>
<tr>
<td>A Side Port</td>
<td>Enter the port number of the A Side CTI server. The value of this field must match the port configured during the setup of the A Side CTI server.</td>
</tr>
<tr>
<td>Peripheral ID</td>
<td>Enter the ID of the Agent PG Routing Client (PIM). The Agent PG Peripheral ID should be configured to the same value for the A Side and B Side CTI servers.</td>
</tr>
<tr>
<td>B Side Host/IP Address</td>
<td>Enter the hostname or IP address of the B Side CTI server.</td>
</tr>
<tr>
<td>B Side Port</td>
<td>Enter the port of the B Side CTI server. The value of this field must match the port configured during the setup of the B Side CTI server.</td>
</tr>
<tr>
<td>Enable SSL encryption</td>
<td>Check this box to enable secure encryption.</td>
</tr>
</tbody>
</table>
Step 4

Click Save.

Contact Center Enterprise Administration & Data Server Settings

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

Note

To connect to the Unified CCE administration database, Finesse supports connections using either SQL authentication 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, you must 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 Contact Center Enterprise Administration & Data Server Settings gadget.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Host/IP Address</td>
<td>Either the hostname or IP address of the Unified CCE Administration &amp; Data Server.</td>
</tr>
<tr>
<td>Backup Host/IP Address</td>
<td>(Optional) Either the hostname or IP address of the backup Unified CCE Administration &amp; Data Server.</td>
</tr>
<tr>
<td><em>Database Port</em></td>
<td></td>
</tr>
<tr>
<td><em>AV Database Name</em></td>
<td></td>
</tr>
</tbody>
</table>

*Indicates required fields
The port of the Unified CCE Administration & Data Server. The default value is 1433.

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

The name of the AW Database (AWDB) (for example, ucceinstance_awdb). AWDatabaseName

(Optional) The domain of the AWDB.

The username required to sign in to the AWDB.

**Note** If you specify a domain, this user refers to the Administrator Domain user that the AWDB uses to synchronize with the logger. In which case, the AWDB server must use Windows authentication and the configured username must be a domain user.

If you do not specify a domain, this user must be an SQL user.

The password required to sign in to the AWDB.

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

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

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

- Primary Host/IP Address
- Backup Host/IP Address
- Database Port
- AW Database Name

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

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

**Note** Finesse will not come into service in case of AWDB errors when connecting Cisco Finesse 11.5(1) and higher versions to Unified CCE 11.5(1) and higher versions.
Configure Contact Center Enterprise Administration & Data Server Settings

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

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

**Procedure**

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Host/IP Address</td>
<td>Enter the hostname or IP address of the Unified CCE Administration &amp; Data Server.</td>
</tr>
<tr>
<td>Backup Host/IP Address</td>
<td>Enter the hostname or IP address of the backup Unified CCE Administration &amp; Data Server.</td>
</tr>
</tbody>
</table>
| Database Port          | Enter the port of the Unified CCE Administration & Data Server.  
                         | **Note** Because Finesse expects the primary and backup Administration & Data Server ports to be the same, the Finesse administration console exposes only one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers. |
| AW Database Name       | Enter the name of the AW Database (AWDB) (for example, ucceinstance_awdb). |
| Domain                 | Enter the domain of the AWDB.                                               |
| Username               | Enter the username required to sign in to the AWDB.                         |
| Password               | Enter the password required to sign in to the AWDB.                         |

**Step 3**
Click Save.
Cluster Settings

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>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**

1. **Step 1** If you are not already signed in the primary node, sign in to the administration console of the primary node with the Application User credentials.
2. **Step 2** In the Cluster Settings area, in the Hostname field, enter the hostname of the secondary Finesse server.
3. **Step 3** Click Save.

Context Service Settings

Cisco Context Service is a cloud-based omnichannel solution for Cisco Unified Contact Center Enterprise. It enables you to capture your customer’s interaction history by providing flexible storage of customer-interaction data across any channel.

Context Service works out of the box with Cisco Customer Collaboration products. Context Service also provides an SDK interface for integration with your own applications or third-party applications to capture end-to-end customer-interaction data.

For more information about Context Service and to check service availability, see https://help.webex.com/community/context-service.
Context Service Network Connectivity Requirements

Context Service is a cloud-based service and requires that call center components using Context Service to be able to connect to the public Internet.

Context Service uses port 443 (HTTPS).

The following URLs must be whitelisted in your firewall so that your contact center components can connect to, and receive data from Context Service.

- *.webex.com
- *.wbx2.com
- *.ciscoccservice.com

Note
Use wildcard URLs in your allowed list because Context Service is accessed through multiple subdomains. Context Service subdomain names can dynamically change.

If you register Context Service by enabling the proxy setting option, configure the browser proxy with the URL specified in the Context Service Management Gadget.

Configure Context Service Settings

Use the Context Service Management gadget to register Cisco Finesse with the Context Service.

Procedure

Step 1
If you are not already signed in, log in to the Cisco Finesse administration console.

Step 2
To register Cisco Finesse with the Context Service, in the Context Service Management gadget, click **Register**.

Note
Before initiating Context Service registration you must make sure pop-ups are enabled.

If the Finesse FQDN is not added as an exception in the block popup windows settings of the browser, the registration and deregistration popup windows do not close automatically. You have to manually close the pop-up windows.

If you are not able to see the **Register** button and a message appears asking you to refresh the page, clear your browser cache and try again.

If you wish to configure a Proxy Server for Context Service, check the Enable Proxy Setting option, enter the following Client Setting parameters and click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server URL</td>
<td>Proxy Server address</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Timeout</td>
<td>The number of milliseconds (ms) the system waits before rejecting the Context Service cloud connectivity. Default: 1000 milliseconds Range: 200 to 15,000 milliseconds.</td>
</tr>
</tbody>
</table>
| Lab Mode  | Radio button indicates if the Context Service is in production mode or lab mode.  
• Enable—Context Service switches to lab mode.  
• Disable (default)—Context Service is in production mode. |

Click **Register** to configure Cisco Finesse with Context Service.

**Note** If changes are made to the Context Service Parameters, do not reregister unless the Context Service connectivity takes more than 30 seconds.

**Step 3** You are prompted to sign in and enter your Cisco Cloud Collaboration Management admin credentials to complete the registration.

**Step 4** If after a successful registration you want to deregister Cisco Finesse from the Context Service, click **Deregister**.

**Note** During the registration process, at any time if you wish to cancel the registration, click **Cancel**.

If registration fails or context service cannot be reached, you can reregister by clicking on the **Register** button.

**Note** If using Firefox, enable the `dom.allow_scripts_to_close_windows` config to ensure that any additional tabs opened for context service registration close as expected. To do this:

a. Enter `about:config` in the Firefox browser.

b. Click **I accept the risk**.

c. Search for `dom.allow_scripts_to_close_windows` config.

d. Double click to change the value field to True.

e. Restart your browser.
Configure Context Service Settings

Manage System Settings
CHAPTER 3

Manage Call Variables Layouts

- Call Variables Layouts, on page 27
- Call Variables, on page 28
- Configure Call Variables Layouts, on page 28
- Add ECC Variables to Call Variables Layout, on page 30
- Assign Call Variables Layouts, on page 30
- Manipulate Call Variables Layouts with a Workflow, on page 31

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 layout and 199 custom layouts). As part of this functionality:

- Each layout has a name (required) and description (optional).
- After an upgrade from a release earlier than Cisco Finesse Release 11.0, Finesse migrates the previously configured default layout and assigns it the default name (Default Layout) and description (Layout used when no other layout matches the user layout Custom/ECC Variable).
- You can change the name and description of the default Call Variables Layout.
- You cannot delete the default Call Variables Layout.
- Finesses 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.
- Finesses 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
- wrapUpReason

**Note**

The callKeyPrefix indicates the day when the call was routed.

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

Configure Call Variables Layouts

**Procedure**

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

**Step 2** Under Create New Layout (or under Edit <layoutname> 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** 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 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 6  To view the latest configured Call Variables Layout, click Refresh from the Manage Call Variables Layouts gadget.

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.

The Custom/ECC Variable Entry dialog box appears.

![Custom/ECC Variable Entry](image)

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 both 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](#).
CHAPTER 4

Manage Desktop Layout

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

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

Important

- Finesse Desktop Layout XML, on page 33
- Default Layout XML, on page 34
- Update Default Desktop Layout, on page 35
- alternateHosts Configuration, on page 36
- XML Schema Definition, on page 37
- Live Data Reports, on page 39

Finesse Desktop Layout XML

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

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

- **Finesse Default Layout XML**: Expands to show the layout XML for the default Finesse desktop.

- **Restore Default Layout**: Restores the Finesse desktop to the default layout.

- **Save**: Saves your configuration changes.

- **Revert**: Retrieves and applies the most recently saved desktop layout.

### Default Layout XML

The Finesse default desktop layout XML for Unified CCE and Packaged CCE contains optional gadgets and notes. 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 in 11.6(1) release version:

- Agents can view Recent Call History and Recent State History gadgets in My History tab.

- Supervisors can view Recent Call History and Recent State History gadgets in Manage Team tab.

If Cisco Unified Intelligence Center (11.6(1)) and Live Data (11.6(1)) version is not installed and configured in a Unified CCE 11.6(1) deployment, Recent Call History and Recent State History gadgets XML must be commented out in the Default XML Layout.

- Added an extra attribute to specify alternate hosts from which gadgets can be initially loaded.

- Use the maxRows attribute to increase the height of the Team Performance Gadget.

- Supervisor can view an agent's Queue Interval Details.

- Supervisors can view Queue Statistics gadget in Queue Data tab.
Update Default Desktop Layout

When you modify the layout of the Finesse desktop, the changes you make take effect on the desktop after 10 seconds. However, agents who are signed in when the changes are made must sign out and sign back in to see those changes reflected on the desktop.

Note

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

Procedure

Step 1

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

Example:

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

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

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

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

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

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

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

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

Step 2

Click Save.

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

Step 3

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

Note

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

Related Topics

Upload Third-Party Gadgets, on page 110
Add Live Data Reports to Finesse, on page 39

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>
</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">http://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.

It is possible that under certain circumstances, the Cisco Finesse desktop fails 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 are ignored by the Cisco Finesse desktop.

Note

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.
XML Schema Definition

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

```xml
<?xml version="1.0" encoding="ISO-8859-1" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://www.cisco.com/vtg/finesse"
  xmlns="http://www.cisco.com/vtg/finesse"
  elementFormDefault="qualified">

<!-- definition of role type -->
<xs:simpleType name="role">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Agent"/>
    <xs:enumeration value="Supervisor"/>
    <xs:enumeration value="Admin"/>
  </xs:restriction>
</xs:simpleType>

<!-- definition of simple elements -->
<xs:element name="id">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:pattern value="[a-zA-Z]-[a-zA-Z0-9]*/"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<xs:element name="label">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:minLength value="1" />'
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<xs:element name="gadget">
  <xs:simpleType>
    <xs:restriction base="xs:anyURI">
      <xs:minLength value="1" />
    </xs:restriction>
  </xs:simpleType>
</xs:element>

<xs:element name="role" type="role"/>

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

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

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

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

<xs:element name="tabs">
  <!-- Grouping of tabs -->
  <xs:complexType>
    <xs:sequence maxOccurs="unbounded">
      <!-- No limit to number of tabs for now -->
      <xs:element ref="tab"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="layout">
  <!-- Type of the role -->
  <xs:complexType>
    <xs:sequence ref="role"/>
  </xs:complexType>
</xs:element>

<xs:element name="finesseLayout"/>
Live Data Reports

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

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 either HTTP or HTTPS for both Cisco Unified Intelligence Center and Finesse. You cannot use HTTP for one and HTTPS for the other. The default setting for both after a fresh installation is HTTPS. If you want to use HTTP, you must enable it on both Cisco Unified Intelligence Center and Finesse.


- If your deployment uses 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

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

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

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

This procedure explains how to add the Live Data report gadgets to the default desktop layout. Use this procedure after a fresh installation of Finess. If you upgraded Finess but do not have a custom desktop layout, click **Restore Default Layout** on the Manage Desktop Layout gadget and then follow the steps in this procedure. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

### Procedure

**Step 1** Sign into the Finessadministration console (https://**FQDN of Finess server:**Port Number (8445)/cfadmin), in which FQDN refers to the fully qualified domain name.

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

**Step 3** Remove the comment characters (<!-- and -->) from each report that you want to add to the desktop layout. Make sure you choose the reports that match the method your agents use to access the Finessedesk (HTTP or HTTPS).

**Step 4** Replace my-cuic-server with the fully qualified domain name of your CiscoUnified Intelligence Center Server.

**Step 5** 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, replacing 310 with 400:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=400&viewId_1=99E6C8E210000141000000D8A0006C4&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 6** 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.
After you add a gadget, sign in to the Finesses 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.

On Finesses desktop layout, if you select a TDM agent in Team Performance Gadget, the recent state history data of the selected agent is not populated.

---

**Add Live Data Reports to Custom Desktop Layout**

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

This procedure explains how to add the Live Data report gadgets to a custom desktop layout. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

**Procedure**

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

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

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

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

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

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B100001410000000C50A0006C4&filterId_2=agent.id=CL%20teamName</gadget>
```

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

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

```xml
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
</layout>
```

---

**Note**
Add Live Data Reports to Custom Desktop Layout

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

This procedure explains how to add the Live Data report gadgets to a custom desktop layout. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

**Procedure**

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

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

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

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

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

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B100001410000000C50A0006C4&filterId_2=agent.id=CL%20teamName</gadget>
```

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

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

```xml
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
</layout>
```
Step 6  Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 7  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=9AB7848B100001410000001C50A0006C4&
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 8  Click Save.

Note  After you add a gadget, sign in to the Finesses 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 Team Layout

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

This procedure explains how to add the Live Data report gadgets to the desktop layout of a specific team. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.
Procedure

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

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

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
gadgetHeight=310&viewId_1=99E6C8E210000141000001D80A0006C4&
filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
filterId_2=agent.id=CL%20teamName
</gadget>
```

Step 5  Click the Team Resources tab.
Step 6  Select the team from the list of teams for which you want to add the report.
Step 7  In the Resources for `<team name>` area, click the Desktop Layout tab.
Step 8  Check the Override System Default check box.
Step 9  Paste the XML within the tab tags where you want it to appear.

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

```xml
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
gadgetHeight=310&viewId_1=99E6C8E210000141000001D80A0006C4&
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 fully qualified domain name of your Cisco Unified Intelligence Center Server.
Step 11 Optionally, change the gadget height.

Example:
Modify Live Data Stock Reports for Finesse

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=99E6C8E21000014100000D80A0006C4&
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.

**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.

---

**Procedure**

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

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

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

**Step 4**  
Copy the 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=99E6C8E21000014100000D80A0006C4&
filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
```

---

**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.
FilterId_2=agent.id=CL\20teamName
</gadget>

**Step 5**
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 6**
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.

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

**Step 7**
Replace the desired viewId value in the gadget URL with the viewId value from thepermalink of the customized report.

**Step 8**
Replace my-cuic-server with the FQDN of the Cisco Unified Intelligence Center Server.

**Step 9**
Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click **Save**.

**Note**
After you add the gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of 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 the need to scroll.

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

---

**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=5C90012F1000014000000830A4E5B33&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:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=9AB7848B1000014100001C50A0006C4&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.

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=5C90012F1000014000000830A4E5B33&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:**
   ```
   <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=5C90012F1000014000000830A4E5B33&filterId_1=agent.id=CL%20teamName&viewId_1=5C90012F1000014000000830A4E5B33&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:**
   ```
   <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=5C90012F1000014000000830A4E5B33&filterId_1=agent.id=CL%20teamName&viewId_2=5C90012F1000014000000830A4E5B33&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, \texttt{99E6C8E210000141000000D80A0006C4}).

\textbf{Example:}

\begin{verbatim}
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId\_1=5C90012F1000014000000830A4E5B33&filterId\_1=agent.id=CL\%20teamName&viewId\_2=99E6C8E210000141000000D80A0006C4&filterId\_2=agent.id=CL\%20teamName</gadget>
\end{verbatim}

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

- Agent Reports: filterId\_\texttt{N}=agent.id=CL\%20teamName
- Agent Skill Group Reports: filterId\_\texttt{N}=agent.id=CL\%20teamName
- Skill Group Reports: filterId\_\texttt{N}=skillGroup.id=CL\%20teamName
- Precision Queue Reports: filterId\_\texttt{N}=precisionQueue.id=CL\%20teamName

\textbf{Step 5} 
Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

\textbf{Step 6} 
Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click Save.

\textbf{Note} 
After you add the gadget, sign in to the Finesses 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 the need to scroll.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.
CHAPTER 5

Manage Phone Books

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

- Phone Books and Contacts, on page 49
- Add Phone Book, on page 51
- Edit Phone Book, on page 51
- Delete Phone Book, on page 52
- Import Contacts, on page 53
- Export Contacts, on page 54
- Add Contact, on page 55
- Edit Contact, on page 56
- Delete Contact, on page 56

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 1500.

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

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

Actions on the Manage Phone Books gadget:

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

Procedure

Step 1 In the Manage Phone Books gadget, click New.
The Manage Phone Books area appears.

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

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

Step 4 Click Save.

Edit Phone Book

Procedure

Step 1 In the Manage Phone Books gadget, select the phone book you want to edit.

Step 2 Click Edit.
The Edit Phone Books area appears.
Step 3  In the Name field, enter the new name for the phone book. If you want to change who can access the phone book, in the Assign To field drop-down list, choose **All Users** or **Teams**.

Step 4  Click **Save**.

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

---

### Delete Phone Book

**Procedure**

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

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

A question appears asking you to confirm that you want to delete the selected phone book.
Step 3

Click Yes to confirm the deletion of the selected phone book.

Import Contacts

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

The import list must be in the specified comma separated values (CSV) format, and can contain a maximum of 1500 contacts. Import lists that contain more than 1500 contacts are rejected with an error message.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Max Length</th>
<th>Can Be Blank?</th>
<th>Permitted Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>128</td>
<td>Yes</td>
<td>Alphanumeric characters</td>
</tr>
<tr>
<td>Last Name</td>
<td>128</td>
<td>Yes</td>
<td>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.
Exported CSV files always show each field enclosed in double quotes, as in the preceding example, to ensure that any commas or double quotes that are part of the actual fielded data are not mistaken for field delimiters. If your data does not include these characters, you can omit the double quotes in files you prepare for importing.

### Procedure

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

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

The Import Contacts area appears.

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

**Note**
The CSV file must use Latin encoding.

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

### Export Contacts

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

**Procedure**

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

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

A message is displayed asking if you want to open or save the file.
The default name for an export file is PhoneBookContacts.csv.

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

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

**Related Topics**
- [Import Contacts](#), on page 53

## Add Contact

**Procedure**

**Step 1**
In the Manage Phone Books gadget, select the phone book to which you want to add a contact.

The List of Contacts for `<phone book name>` area appears.

**Step 2**
Click **New**.

The New Contact area appears.
**Edit Contact**

**Procedure**

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

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

**Step 3**
Click **Edit**.

The Edit Contact area appears.

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

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

---

**Delete Contact**

**Procedure**

**Step 1**
In the Manage Phone Books gadget, select the phone book that contains the contact you want to delete. The List of Contacts for `<phone book name>` area appears.
Step 2  Select the contact that you want to delete.

Step 3  Click **Delete**.

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

Step 4  Click **Yes** to confirm the deletion of the selected contact.
Delete Contact
CHAPTER 6

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.

You can configure different reason codes with the same reason code label across various teams.

- Not Ready Reason Codes, on page 59
- Sign Out Reason Codes, on page 64
- Predefined System Reason Codes, on page 68
- Manage Reason Code Conflicts During Upgrade, on page 70
- Wrap-Up Reasons, on page 71

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 Not Ready team reason codes. The team reason codes can be mapped to any team, and the same reason code can be mapped to multiple teams.
The following table describes the fields on the Manage Reason Codes (Not Ready) gadget.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason Label</td>
<td>The label for the Not Ready reason code. The label has a maximum length of 40 characters and should be unique for each Not Ready reason code. Both alphanumeric and special characters are supported.</td>
</tr>
<tr>
<td>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 Not Ready reason. The code can be any value between 1 and 65535 and must be unique.</td>
</tr>
<tr>
<td>Global?</td>
<td>Yes/No. Indicates if the reason code is available globally to all agents (Yes) or to specific teams of agents (No).</td>
</tr>
</tbody>
</table>

**Actions on the Manage Reason Codes (Not Ready) gadget:**
- **New:** Add a new Not Ready reason code
- **Edit:** Edit an existing Not Ready reason code
- **Delete:** Delete a Not Ready reason code
- **Refresh:** Reload the list of Not Ready reason codes from the server

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

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

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

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

Pending state changes appear on the desktop while the agent's state is Talking (for example, on hold, in a consult call, conference, or silent monitor call).

**Note**
During a PG or CTI server failover, the pending state of an agent will not be retained.

**Add Not Ready Reason Code**

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

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

![New Reason Code](image)

**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 pre populated 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

Perform the following procedure to edit the label or code for an existing Not Ready reason code.

**Procedure**

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

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

The Edit Reason Code area appears.
Step 3  If you want to change the label for the Not Ready reason code, in the Reason Label field, enter a new label for the reason code. If you want to change the code, in the Reason Code field, enter the new code. If you want to change who has access to the code, select or clear the Global? check box.

Step 4  Click Save.

---

**Delete Not Ready Reason Code**

**Note**

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

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

**Procedure**

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

Step 2  Click Delete.

A question appears asking you to confirm that you want to delete the selected reason code.
Step 3  Click Yes to confirm the deletion of the selected reason code.

Sign Out Reason Codes

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason Label</td>
<td>The label for the Sign Out reason code.</td>
</tr>
<tr>
<td></td>
<td>The label has a maximum length of 40 characters and should be unique for each Sign Out reason code. Both alphanumeric and special characters are supported.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of reason code (System or Custom).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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
When you add, edit, or delete a Sign Out reason code, the changes you make take effect on the Finesse desktop after three seconds. However, agents who are signed in when the changes are made must sign out and sign back in to see those changes reflected on their desktops.

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

Add Sign Out Reason Code

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

Procedure

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

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 pre populated 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? check box. If the reason code is specific to a team, clear the Global? check box.
Note By default, the Global? check box is selected.

Step 5
Click Save.
Edit Sign Out Reason Code

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

Procedure

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

Step 2
Click Edit.

The Edit Reason Code area appears.

Step 3
If you want to change the label of the Sign Out reason code, in the Reason Label field, enter a new label for the reason code. If you want to change the code, in the Reason Code field, enter the new code. If you want to change who has access to the code, select or clear the Global? check box.

Step 4
Click Save.

Delete Sign Out Reason Code

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

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

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

Step 2 Click Delete.

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

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>Ready - Offhook</td>
<td>The system issues this reason code in the following scenarios:</td>
</tr>
<tr>
<td></td>
<td>Not Ready - Offhook</td>
<td>• When the agent goes off the hook to place a call. If the agent remembers to do</td>
</tr>
<tr>
<td></td>
<td></td>
<td>this task the corresponding agent-triggered reason code is displayed. If the agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>does not remember to do this task, the system issues this reason code.</td>
</tr>
<tr>
<td>Code</td>
<td>Reason Description</td>
<td>Note</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>50001</td>
<td>Logged Out - System Disconnect</td>
<td>The CTI OS client disconnected, logging the agent out.</td>
</tr>
<tr>
<td>50002</td>
<td>Logged Out - System Failure</td>
<td>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 time out, or a CTI OS Server failure.</td>
</tr>
<tr>
<td>50002</td>
<td>Not Ready - Connection Failure</td>
<td>The system issues this reason code when the agent is forcibly logged out in certain cases.</td>
</tr>
<tr>
<td>50003</td>
<td>Logged Out - Device Error</td>
<td>Agent was logged out because the Unified CM reported the device out of service.</td>
</tr>
<tr>
<td>50004</td>
<td>Logged Out - Inactivity Timeout</td>
<td>Agent was logged out due to agent inactivity as configured in agent desk settings.</td>
</tr>
<tr>
<td>50005</td>
<td>Not Ready - Non ACD Busy</td>
<td>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.</td>
</tr>
<tr>
<td>50010</td>
<td>Not Ready - Call Overlap</td>
<td>Agent was set to Not Ready state because the agent was routed two consecutive calls that did not arrive.</td>
</tr>
<tr>
<td>50020</td>
<td>Logged Out - Queue Change</td>
<td>Agent was logged out when the agent's skill group dynamically changed on the Administration &amp; Data Server.</td>
</tr>
<tr>
<td>50030</td>
<td>Logged Out - Device Conflict</td>
<td>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.</td>
</tr>
<tr>
<td>50040</td>
<td>Logged Out - Mobile Agent Call Fail</td>
<td>Mobile agent was logged out because the call failed.</td>
</tr>
<tr>
<td>50041</td>
<td>Not Ready - Mobile Call Not Answered</td>
<td>Mobile agent state changed to Not Ready because the call fails when the mobile agent's phone line rings busy.</td>
</tr>
<tr>
<td>50042</td>
<td>Logged Out - Mobile Agent Disconnect</td>
<td>Mobile agent was logged out because the phone line disconnected while using nailed connection mode.</td>
</tr>
<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>
</tbody>
</table>
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) or higher versions. If there is a reason code conflict then the following message appears when you sign in to 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 Code Description</th>
<th>Reason Code Description</th>
</tr>
</thead>
<tbody>
<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 only for incoming calls and Outbound Option Dialer Calls (Finesse does not support Outbound Option Direct Preview mode). Finesse does not support wrap-up for outgoing calls placed by agents.

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

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

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

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

**Note**

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

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

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

**Actions on the Manage Wrap-Up Reasons gadget:**

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

---

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

---

**Add Wrap-Up Reason**

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

**Procedure**

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

**Step 2**
In the Reason Label field, add a label for the Wrap-Up reason.

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

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

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

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

---

**Edit Wrap-Up Reason**

Perform the following procedure to edit an existing Wrap-Up reason.

**Procedure**

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

**Step 2**
Click **Edit**.
The Edit Wrap-Up Reason area appears.
Step 3  In the Wrap-Up Reason Label field, enter the new label for the Wrap-Up reason. If you want to change who has access to the Wrap-Up reason, select or clear the Global? check box.

Step 4  Click Save.

---

**Delete Wrap-Up Reason**

Perform the following procedure to delete a Wrap-Up reason.

**Procedure**

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

Step 2  Click Delete.

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

Step 3  Click Yes to confirm the deletion of the selected Wrap-Up reason.
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 75
- Assign Phone Books and Reasons to Team, on page 77
- Unassign Phone Books and Reasons from Team, on page 78
- Assign Custom Desktop Layout to Team, on page 78
- Assign Workflows to Team, on page 79
- Unassign Workflows from Team, on page 80

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.
### Tab Name | Description
--- | ---
Desktop Layout | 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.
Phone Books | 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.
Reason Codes (Not Ready) | 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.
Reason Codes (Sign Out) | 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.
Wrap-Up Reasons | Use this tab to assign and unassign Wrap-Up reasons to the team. Only Wrap-Up reasons that are defined in the Manage Wrap-Up Reasons gadget as available to teams (not global) are available for assignment.
Workflows | Use this tab to assign and unassign workflows to the team. Only workflows that are defined in the Manage Workflows gadget are available for assignment.

#### 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. Tabs for each available resource appear.

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

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

Step 4  Select one or more resources from the list to assign them to the team. Resources you assign are highlighted in blue in the Add <resources> popup and added to the List of <resources> area.

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

---

**Unassign Phone Books and Reasons from Team**

**Procedure**

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

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

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

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

---

**Assign Custom Desktop Layout to Team**

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

**Procedure**

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

**Step 2** Click the Desktop Layout tab.
The Desktop Layout XML area appears. The area contains the default desktop layout XML.

**Step 3** Select the Override System Default check box.
The XML becomes editable.

**Step 4** Edit the XML as desired.

**Step 5** Click **Save**.
The custom desktop layout replaces the default desktop layout for the team after 10 seconds. If a supervisor or agent is signed in when the change is saved, the change does not go into effect on their desktop until the supervisor or agent signs out and signs in again.
If you clear the Override System Default check box, any changes you made to the XML are lost and the XML in the editing pane reverts to the default desktop layout XML.

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

Related Topics
Manage Desktop Layout, on page 33

Assign Workflows to Team

Procedure

Step 1 In the Manage Team Resources gadget, select a team. Tabs for each available resource appear.
Step 2 Click the Workflows tab. The List of Workflows area appears.
Step 3 Click Add. The Add Workflow popup appears.
Step 4 Select one or more workflows from the list to assign them to the team. Workflows you assign are highlighted in blue in the Add Workflows popup and added to the List of Workflows area.
Step 5 Workflows are executed in the order in which they are listed. Use the up and down arrows to move a selected workflow to the desired position in the list.
Step 6 When you has finished assigning workflows, click Save.

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

Procedure

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

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

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

**Step 4**  Click **Save**.
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 81
- Add Browser Pop Workflow Action, on page 86
- Add HTTP Request Workflow Action, on page 87
- Edit Workflow Action, on page 88
- Delete Workflow Action, on page 89
- Add Workflow, on page 90
- Edit Workflow, on page 91
- Delete Workflow, on page 92

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, the following fields can be used to configure workflows:

- queueNumber
- queueName
• callKeyCallId
• callKeyPrefix
• wrapUpReason

Click the column headers to sort workflows and workflow actions in ascending or descending order.

The following table describes the fields on the Manage Workflows gadget.

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

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

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

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

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

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

- When a call arrives
- When a call is answered

**Note**

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

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

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

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

**Note**

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

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

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

Workflowsthattriggerwhenacallarrives, whenacallisanswered, orwhenmakingacallruneverywhenthe
browserisrefreshed. When anagent refreshesthebrowser, 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
refreshesthebrowser. Applications thatreceive the HTTPrequests mustaccountfor this scenario. Otherwise,
undesired results may occur.

An example of a workflow is a Call Arrival event that triggers an action that collects information from the
dialog event (for example, the ANI or customer information) and displays a web page containing customer
information.

You can filter trigger events by the value of the data that comes in the event. You can configure a workflow
toexecuteifanyconditionsaremetorfifallconditionsaremet.

Individual conditions consist of the following:

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

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

WorkflowsrunonlyforagentsandsupervisorswhoareFinesseusers. The WorkflowEngineis aJavaScript
library that runs client-side on a per-user basis within the Finesse 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.

Ifmultipleworkflowsareconfigured forateam, the WorkflowEngine 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 Finesse server controls which calls are displayed to the Finesse 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 is not necessarily the same call that was the first displayed call before the browser refresh. Dialogs received for any other call are ignored because they are not considered first displayed calls. If dialogs for more than one call are received before the Workflow Engine is loaded after the browser refresh, no dialogs are evaluated because none are considered first displayed calls.

Workflows run for both Finesse agents and supervisors. The team to which the supervisor belongs (as distinguished from the team that the supervisor manages) determines which workflows run for the supervisor. You may want to put the supervisors in their own team to keep agent workflows from being run for them.

### Workflow Triggers and Outbound Calls

---

**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

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

The New Action area appears.

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

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

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

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

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

**Note**  Window names are limited to 40 characters, and can be blank. If you leave the window name blank, a new window opens every time the action runs.
Step 6 Enter the URL of the browser window to open, and then click the tag icon at the right of the box and select one or more variables from the drop-down list to add tags.

**Example:**

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

For every variable you select, you can enter test data in the Sample Data box. A sample URL is automatically built in the Browser URL box below the Sample Data area. To test the URL, click Open to open the URL in your browser.

**Note** Finesse does not validate the URL you enter.

Step 7 Click Save.

---

## Add HTTP Request Workflow Action

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

**Procedure**

---

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

The New Action area appears.

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

A workflow action name can contain a maximum of 64 characters.

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

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

**Step 5** From the Method drop-down list, select the method to use.

You can select either PUT or POST.

**Step 6** From the Location drop-down list, select the location.

If you are making the HTTP request to a Finesse API, select **Finesse**. If you are making a request to any other API, select **Other**.

**Step 7** In the Content Type box, enter the content type.

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

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

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

/finesse/api/User/dialogId

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

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

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

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

Step 10  Click Save.

---

Edit Workflow Action

Procedure

Step 1  In the Manage Workflow Actions gadget, select the action that you want to edit.
Step 2  Click Edit.

The Edit Action area appears.
Step 3 Edit the fields that you want to change.
Step 4 Click Save.

Delete Workflow Action

Procedure

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

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

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

Procedure

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

**New Workflow**

- **Name**: Workflow1
- **Description**: Pop customer info
- **When to perform Actions**: When a Call arrives
- **How to apply Conditions**: If all Conditions are met
  - callVariable5 Begins with 651

**Ordered List of Actions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pop Customer Info</td>
<td>BROWSER_POP</td>
</tr>
</tbody>
</table>

Step 2
In the Name box, enter the name of the workflow.

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

Step 3
In the Description box, enter a description of the workflow.

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

Step 4
In the When to perform Actions drop-down list, select the event that triggers the workflow.
Step 5 In the How to apply Conditions box, select if all conditions are met, or if any conditions are met, and then click **Add Condition** to add up to five conditions.

**Example:**

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

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

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

Step 8 Click **Save**.

Step 9 Assign the workflow to one or more teams.

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

---

**Related Topics**

[Assign Workflows to Team](#), on page 79

---

**Edit Workflow**

**Procedure**

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

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

The Edit Workflow area appears.
Step 3  Edit the fields that you want to change.
Step 4  Click Save.

Delete Workflow

Procedure

Step 1  In the Manage Workflows gadget, select the workflow that you want to delete.
        The Delete Workflow area appears.
Step 2  Click Delete.
        A question appears asking you to confirm that you want to delete the selected workflow.
Step 3

Click **Yes** to confirm the deletion of the selected workflow.
Delete Workflow
Manage Security

- HTTP and HTTPS Support, on page 95
- Cisco Finesse HTTPS Redirect, on page 95
- Reset Security or Admin Password, on page 97

HTTP and HTTPS Support

The Cisco Finesse administration console and agent desktop support both HTTP and secure HTTP (HTTPS). To access the administration console using HTTPS, enter the following URL in your browser:

https://FQDN:8445/cfadmin

where FQDN is the fully-qualified domain name of your primary Finesse server and 8445 is the port number.

To access the administration console using HTTP, enter the following URL:

http://FQDN/cfadmin

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

- http://FQDN/desktop
- https://FQDN:8445/desktop

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

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

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

Cisco Finesse HTTPS Redirect

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

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

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

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

- **To retrieve the status of Cisco Finesse HTTPS Redirect:** `utils finesse application_https_redirect status`

  This command displays whether Cisco Finesse HTTPS Redirect is currently enabled or disabled on the system.

  **Note**
  On the secondary server, the HTTPS redirect status appears as enabled for the Finesse Agent Desktop only. For Finesse Admin, the HTTPS redirect status always appears as disabled on the secondary server because Finesse Admin is not available on the secondary server.

- **To enable Cisco Finesse HTTPS Redirect:** `utils finesse application_https_redirect enable`

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

  If the Cisco Finesse Tomcat Service is not stopped, the command to enable Cisco Finesse HTTPS Redirect fails. This command also fails if Cisco Finesse HTTPS Redirect is already enabled.

  After you enable Cisco Finesse HTTPS Redirect, start the Cisco Finesse Tomcat Service using the command `utils service start Cisco Finesse Tomcat`.

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

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

  If the Cisco Finesse Tomcat Service is not stopped, the command to disable Cisco Finesse HTTPS Redirect fails. This command also fails if Cisco Finesse HTTPS Redirect is already disabled.

  After you disable Cisco Finesse HTTPS Redirect, start the Cisco Finesse Tomcat Service using the command `utils service start Cisco Finesse Tomcat`.

---

Finesse supports HTTP Strict Transport Security (HSTS) for increased security. HSTS is automatically enabled when you enable HTTPS Redirect, in which case the Finesse server sends HTTPS responses indicating to browsers that Finesse can only be accessed using HTTPS. If users then try to access Finesse 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.

---

**HSTS**

Finesse supports HTTP Strict Transport Security (HSTS) for increased security. HSTS is automatically enabled when you enable HTTPS Redirect, in which case the Finesse server sends HTTPS responses indicating to browsers that Finesse can only be accessed using HTTPS. If users then try to access Finesse 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

**Step 1**
Sign into 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.
Manage Finesse IP Phone Agent

- Finesse IP Phone Agent, on page 99
- One Button Sign In, on page 100
- Finesse IP Phone Service Subscription Options, on page 101
- Set Up Application User, Web Access, and HTTPS Server Parameters, on page 102
- Configure Finesse IP Phone Service in Unified CM, on page 103
- Add Service Parameters for One Button Sign In, on page 105
- Subscribe Agent Phones to Manual Subscription Service, on page 107
- Set Up Agent Access to the Self Care Portal, on page 108

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 Finesse 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 codes 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.
HTTP Only

Finesse IPPA phone clients communicate with the Finesse server using HTTP only, whether or not HTTPS access is enabled on Finesse.

Failure Behavior

Unlike the Finesse desktop, the Finesse IP Phone Agent does not automatically failover to the alternate Finesse server. 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 Finesse service that connects to an alternate Finesse server.

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 Finesse servers.

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 Finesse on the IP Phone without credentials just by selecting Cisco Finesse 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 (by Administrator)</th>
<th>Prepopulated in Self Care Portal (by Agent)</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 password</td>
</tr>
<tr>
<td>Administrator populates the ID and extension</td>
<td>id, extension</td>
<td>-</td>
<td>password</td>
</tr>
<tr>
<td>Agents enter password only using Self Care Portal</td>
<td>id, extension</td>
<td>password</td>
<td>-</td>
</tr>
</tbody>
</table>
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 Finesse service, 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 themselves.

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>
<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>
<td></td>
</tr>
<tr>
<td>Set Up Application User, Web Access, and HTTPS Server Parameters, on page 102</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Configure Finesse IP Phone Service in Unified CM, on page 103</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Add Service Parameters for One Button Sign In, on page 105</td>
<td>Not applicable</td>
<td>Required only with One Button Sign In</td>
<td>Required only with One Button Sign In</td>
</tr>
<tr>
<td>Subscribe Agent Phones to Manual Subscription Service, on page 107</td>
<td>Not applicable</td>
<td>Required</td>
<td>Optional. Allows the administrator to enter agent credentials for 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. And for proper Finesse IPPA operation, you must also set the Web Access and HTTPS Server parameters in Unified CM.

These 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 HTTP and HTTPS Enabled.

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 (FIPPA) from 11.0 (1) onwards, the User Device Profile (UDP) must be associated with the FIPPA Application User along with the physical phones for agents using Extension Mobility. The Finesses Service URL must use the complete FQDN of the UCCX server.

Related Topics
Replication Status, on page 147

Configure Finesse IP Phone Service in Unified CM

The following procedure describes the steps required for both manual and enterprise subscription.

Procedure

Step 1 Log in to the Cisco Unified Communications Manager Administration using administrator credentials.

Step 2 From the Communications Manager menu, select Device > Device Settings > Phone Services.

Step 3 On the IP Phone Services page, 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#

where Finesse FQDN is the fully qualified domain name (FQDN) of your primary Finesses server.

Step 6 Ensure that the Service Category is set to XML Service, and the Service Type is set to Standard IP Phone Service.
**Step 7** Check the **Enable** check box.

**Step 8** Do one of the following:

- To automatically subscribe all phones in the cluster to the Finesse service, check the **Enterprise Subscription** check box, and click **Save**. Agents and supervisors can now access Cisco Finesse by selecting it from the **Services** menu on subscribed IP phones.

  **Note** One Button Sign In is not supported with enterprise subscriptions.

  **Figure 1: Finesse Service Configuration with Enterprise Subscription**

- To subscribe only the desired phones to the Finesse service manually, leave the **Enterprise Subscription** check box unchecked and click **Save**.
Step 9

With a two-node Finesse setup (primary and secondary Finesse servers), perform the preceding steps again to create a secondary Finesse service that points to the secondary Finesse 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 Finesse Secondary.
- At Step 5, in the Service URL field, replace Finesse FQDN with the FQDN of the secondary server.

Note: Since Finesse IPPA works only over HTTP, avoid using Secured Phone URL Parameters in Unified CM.

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.
**Procedure**

**Step 1**
From Cisco Unified Communications Manager Administration, select the Finesse phone service (under **Device > Device Settings > Phone Services**).

**Step 2**
Click **New** to the right of the Parameters box.

The Configure Cisco IP Phone Service Parameter page displays.

**Step 3**
Set up service parameters for the agent id, extension, and password credentials in accordance with 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 additional parameters, click **Add New** and enter the required values.

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter Name</strong></td>
<td>Enter one of the following parameter names as follows:</td>
</tr>
<tr>
<td></td>
<td>• Id</td>
</tr>
<tr>
<td></td>
<td>• extension</td>
</tr>
<tr>
<td></td>
<td>• password</td>
</tr>
<tr>
<td></td>
<td>The values entered are the exact query string parameters used for the subscription URL.</td>
</tr>
<tr>
<td><strong>Parameter Display Name</strong></td>
<td>Enter a descriptive parameter name; for example, id, extension, and password.</td>
</tr>
<tr>
<td><strong>Default Value</strong></td>
<td>Leave the default value blank for all parameters.</td>
</tr>
<tr>
<td><strong>Parameter Description</strong></td>
<td>Enter a description of the parameter. The user can access this text when they subscribe to the service.</td>
</tr>
<tr>
<td><strong>Parameter is Required</strong></td>
<td>If the administrator will prepopulate the parameter in Unified CM Administration, check the <strong>Parameter is Required</strong> check box.</td>
</tr>
<tr>
<td></td>
<td>However, if the agent will prepopulate the parameter in the Self Care Portal, two options are available:</td>
</tr>
<tr>
<td></td>
<td>• If the agents will prepopulate all defined parameters, check the <strong>Parameter is Required</strong> check box for each parameter.</td>
</tr>
<tr>
<td></td>
<td>• If the agent and administrator will 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.</td>
</tr>
<tr>
<td><strong>Parameter is a Password (mask contents)</strong></td>
<td>Check this check 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.</td>
</tr>
</tbody>
</table>
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 Finesse service as a manual subscription, you can subscribe the agent phones to the Finesse service in Unified CM and optionally define agent credentials for One Button Sign In.

If you prefer to allow the agents subscribe to the Finesse 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 Finesse 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 phone services window displays for this phone.

Step 4  From the Select a Service drop-down list, select Cisco Finesse.

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 Finesse service. The Cisco Finesse service displays in the **Subscribed Services** list.

Step 8  Click **Save**.
The subscribed agents or supervisors can now access Cisco Finesse by selecting it from the **Services** menu on their IP phones.

Step 9  With a two-node Finesse setup (primary and secondary Finesse servers), perform this procedure again to also subscribe the phones to the secondary Finesse service that points to the secondary Finesse 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 Finesse 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Unified CM Administration page, select <strong>System &gt; Enterprise Parameters</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Under the Self Care Portal Parameters, in the <strong>Self Care Portal Default Server</strong> field, select the IP address of the Unified CM Publisher server from the drop-down list and click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>User Management &gt; End User</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select the user that you want to set up with access to the User Care Portal.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Under Permissions Information, click <strong>Add to Access Control Group</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>From the list of Access Control groups displayed, check <strong>Standard CCM End Users</strong> and click <strong>Add Selected</strong>.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

With access enabled to the Self Care Portal, agents can sign in to 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 both the primary and secondary Finesse services.
CHAPTER 11

Manage Third-Party Gadgets

- 3rdpartygadget Account, on page 109
- Upload Third-Party Gadgets, on page 110
- Third-Party Gadget Limitations, on page 111

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:

util 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 Finesseserver, as illustrated in the following example.

Note

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

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

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

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

Note

For Unified CCX deployments you must specify port 8082.

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

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

When you add a gadget to the desktop layout, that gadget can be referenced using a relative path. For more information on adding third party gadgets to the 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:

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

```
utils os secure permissive
```

Note

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

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

Third-Party Gadget Limitations

Third-party gadgets must be .xml files. You cannot use .jsp files.
Third-Party Gadget Limitations
CHAPTER 12

Perform Routine Maintenance

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

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

- Cisco Finesse Services, on page 113
- Log Collection, on page 114
- Collect Logs Using Cisco Unified Real-Time Monitoring Tool, on page 116
- Cisco Finesse Notification Service Logging, on page 119
- Remote Account Management, on page 119

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

- **Finesse Rest API application**: This application provides integration with the Cisco CTI Server for the Finesse desktop and Finesse administration application. Which APIs are available to a user depends on the role associated with that user's credentials. This application also provides a programming interface that can be used by third-party applications that are written to use the Finesse REST API.

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

- **Finesse Diagnostic Portal application**: This application provides performance-related information for Finesse.

- **Finesse IP Phone Agent (IPPA) application**: This 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.

**Note**

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 into the CLI using the credentials for the Administrator User account.

**Step 2** To view a list of all services and their states, enter the following command: `utils service list`.

Services are shown in one of the following states: STOPPED, STARTING, or STARTED.

STOPPED means the service is not running. STARTING means the service is starting operation and performing any initialization. STARTED means the service has successfully initialized and is operational.

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

**Example:**
For example, to start Cisco 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). 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 submitted from the Finesse agent desktop to the Finesse server. Each log file is no larger than 1.5 MB and contains a timestamp and the agent ID of the agent who submitted the file. A new log file is created each time an agent submits client-side logs (the data is not appended to an existing log file). The maximum size of this directory is 100 MB. 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 start-up, error, and informational 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 logs pertaining to the Finesse database.

- **/finesse/logs**: contains the logs for the Cisco Finesse Tomcat service.

- **fippa**: contains logs for the Finesse IP Phone Agent (IPPA) application.
- **finesse-auth**: contains the logs for Finessse authentication with the Cisco Context Service.

- **jmx**: contains the JMX counters data generated by the JMX logger process. It contains important jmx counters exposed by Finessse and openfire.

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

- **Context Service registration log**: `file get activelog ccbu/logs/fusion-mgmt-connector`

Use this command to obtain the fusion-mgmt-connector logs generated by Finessse during the registration and deregistration with Cisco Context Service.

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

- **Servm log**: `file get activelog platform/log/servm*.* compress`

Use this command to obtain logs generated by the platform service manager that manages the starting and stopping of the Finessse 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 timestamp>active_nnn.tgz`, where nnn is timestamp in long format.

- **Platform Tomcat logs**: `file get activelog tomcat/logs recurs compress`

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

---

**Note**

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

---

**Collect Logs Using Cisco Unified Real-Time Monitoring Tool**

Cisco Finessse supports the Cisco Unified Real-Time Monitoring Tool (RTMT) for log collection. Use the following procedure to collect logs using Unified RTMT.

---

**Note**

Finessse 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 Finesseserver.

Procedure

Step 1 Log in to Unified RTMT using Finesses administrator credentials.
Step 2 In the tree hierarchy, select Trace & Log Central or choose System > Tools > Trace > Trace & Log Central.
Step 3 Double-click Collect Files.
The Trace Collection wizard appears.
Step 4 Select the services and Finesses nodes for which you want to collect logs, and complete the wizard.

Syslog Support for Critical Log Messages

Cisco Finesses generates sylogs 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 Finesseserver.

Procedure

Step 1 Log in to Unified RTMT using Finesses administrator credentials.
Step 2 In the tree hierarchy, select SysLog Viewer or choose System > Tools > SysLog Viewer > Open SysLog Viewer.
Step 3 From the Select a Node drop-down list, choose the server where the logs that you want to view are stored.
Step 4 Under the Logs tab, select Application Logs > CiscoSyslog to view and save the syslog file.

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 Finesses 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.

- **UNABLE_TO_CONNECT_TO_XMPP_SERVER**
  Unable to connect xmpp server.

- **DB_SS_CONNECTION_CHECK**
  There was an error connecting to the database.

- **cfservice_CORE_ERROR_DB_CONNECTION**
  Unable to connect to the Database.

- **AWDB_NOT_ACCESSIBLE**
  Unable to connect to AWDB server.

- **VOS_DB_ADAPTER_ERROR**
  There was an error on the VOS DB Adapter operation.

- **FINESSE_APP_STARTUP_ERROR**
  Error during Finesse Application Startup.

- **OF_STATE_CHANGED**
  OF subsystem state successfully changed.

- **CONNECTED_TO_XMPP_SERVER**
  Successfully connected to xmpp server.

- **SSO_API_ERROR**
  Error processing REST API Request for SSO.

- **API_ERROR_DETAIL**
Error processing REST API request.

### Cisco Finesse Notification Service Logging

To view the status of, enable, or disable Cisco Finesse Notification Service logging:

- **To retrieve the status of Cisco Finesse Notification Service logging:** `utils finesse notification logging status`

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

  __Note__

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

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

  __Note__

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

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

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

  __Note__

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

**Related Topics**

- [Log Collection](#) on page 114

### Remote Account Management

Run the following command to enable, disable, create, and check the status of a remote access account: `utils remote_account`
A remote account generates a passphrase that allows Cisco support personnel to get access to the system for the specified life of the account.

- **utils remote_account create account life**
  
  *account* is the account name. *life* indicates the life of the account in days.

- **utils remote_account disable**
- **utils remote_account enable**
- **utils remote_account status**
CHAPTER 13

Cisco Finesse Failover Mechanisms

This chapter describes failover and redundancy mechanisms for Cisco Finesse.

- CTI Failover, on page 121
- AWDB Failover, on page 122
- Finesse Client Failover, on page 123
- Desktop Behavior, on page 124
- Finesse IP Phone Agent Failover, on page 127

CTI Failover

The prerequisites for CTI failover are as follows:

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

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

When Finesse is used in a duplex Unified CCE deployment, and it loses connection to the A Side CTI server, it tries to connect once to the B side CTI server. If this attempt fails, Finesse then tries to reconnect to the A Side CTI server. Finesse keeps repeating this process until it makes a successful connection to the CTI server.

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

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

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

Any call control, call data, or agent state actions that occur during CTI failover are published as events to the agent desktop after failover is complete. This allows Finesse clients to reflect an accurate view of the call control, call data, and agent state.

If an agent makes or answers a call and ends that call during failover (that is, the entire call takes place during failover), the corresponding events are not published after failover is complete.
An agent or supervisor who signs in after being on an active conference with other devices (which are not associated with another agent or supervisor) may experience unpredictable behavior with the Finess 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 Finess desktop. Examples of unpredictable behavior include, but are not limited to, the following:

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

Despite these caveats, the agent or supervisor can continue to perform normal operations on the phone. Desktop behavior returns to normal after the agent or supervisor drops off the conference call.

**Related Topics**

[Contact Center Enterprise CTI Server Settings](page 17)

---

**AWDB Failover**

The prerequisites for AWDB failover are as follows:

- The secondary Administrative Workstation Database (AWDB) is configured.
- The secondary AWDB host is configured through the Finesse administration console.
- Finesses can connect to the secondary AWDB host.
- The Distributor service is running on the secondary AWDB host.

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

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

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

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

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

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

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

Related Topics

Contact Center Enterprise Administration & Data Server Settings, on page 20

Finesses Client Failover

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

• The Finesses desktop continues to check whether the current Finesses server recovers its state.
• The Finesses desktop checks if the other Finesses server is available and in service.

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

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

• The Finesses desktop receives a SystemInfo event that the current server is OUT_OF_SERVICE.
• The BOSH connection is disconnected.
• The “finesse” XMPP user presence changes to unavailable.

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

1. Poll SystemInfo every 10 seconds.
2. If SystemInfo is IN_SERVICE, check the BOSH connection.
3. If BOSH is disconnected, make a BOSH connection request
4. If BOSH is connected and the server is IN_SERVICE, refresh the data.

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

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

Client failover can occur for the following reasons:

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

### Desktop Behavior

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

**Note**

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

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

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Desktop Behavior</th>
<th>Server Action</th>
<th>Results</th>
</tr>
</thead>
</table>
| The agent closes the browser, the browser crashes, or the agent clicks the Back button on the browser. | When you close the browser or navigate away from the Finesse desktop, the Finesse desktop makes a best-effort attempt to notify the server. | 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. | **Race Conditions**

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.

2. If the browser crashes, it can take the Finesse server up to 120 seconds to detect that the client is gone and send a presence notification to Finesse. A situation can occur where the client signs in to the secondary Finesse server before the primary Finesse server receives the presence notification caused by the browser crash. In this case, the agent may be signed out or put into Not Ready state on the secondary Finesse server.

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.

| The client refreshes the browser | — | Finesse receives a presence notification of *Unavailable* from the client. Finesse waits 60 seconds before sending a forced logout request to the CTI server to allow the browser to reconnect after the refresh. |
|——|——|——|
| The client encounters a network glitch (Finesse is in service) | Because the connection to the Finesse server temporarily goes down, the client fails over to the secondary Finesse server. | The primary Finesse server receives a presence notification of *Unavailable* from the client. Because Finesse is in service, it sends a forced logout request to the CTI server for the agent. |
|——|——|——|
| The Refresh Token has expired | Finesse desktop sends a forced logout request to the CTI server. | The Finesse server forwards the forced logout request to the CTI server. |

**Race Conditions**

A situation can occur where the forced logout does not happen before the client signs in to the secondary Finesse server. If the agent is on a call, the primary Finesse server sends the forced logout request after the call ends. The agent will be signed out or put into Not Ready state when the call ends, even though the client is already signed in to the secondary Finesse server.

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.

For both Unified CCE and Unified CCX:

- The session expiry warning dialog box appears in the last 10 and 5 minutes before the Refresh Token expires. In the last minute, a timer appears with the remaining time counted down till the Refresh Token expires. The agent is forcefully logged out when the timer reaches zero and will require to login 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.

---

**Note**

To avoid unexpected expiry of the Refresh Token in the Single Sign-On mode for both Unified CCE and Unified CCX, before logging in to the Finesse desktop, clear the browser cookies of your browser.

To clear the browser cookies in the Internet Explorer

1. Navigate to the **Delete Browsing History** window.
2. Uncheck the **Preserve Favorites website** data check box.
3. Check the **Temporary Internet files and website files** and **Cookies and website data** check boxes.
4. Click **Delete**.

To clear the browser cookies in Chrome

1. Navigate to the **Clear browsing data** window.
2. In the **Advanced** tab, check the **Cookies and other site and plugin data** and **Cached images and files** check boxes.
3. Click **Clear browsing data**.

To clear the browser cookies in Firefox

1. Navigate to the **Clear Recent History** window.
2. From the **Time range to clear** drop-down, choose **Everything**.
3. Check the **Cookies** and **Cache** check boxes.
4. Click **Clear Now**.
Finesse IP Phone Agent Failover

With a two-node Finess setup (primary and secondary Finess servers), if the server that an agent is connected to goes out of service, the Finess IP Phone Agent (IPPA) displays a notification that the server is unavailable. Finess IPPA continues to check whether the current Finess server recovers its state, and notifies the agent if it reconnects.

Finess IPPA attempts to reconnect to the server every 5 seconds and declares it out of service after three failed attempts. The total time to go out of service is approximately 15 seconds.

Unlike the Finess desktop, Finess IPPA does not check whether the alternate Finess server is available. To connect to an alternate Finess server, the agent must exit the current Finess service, and manually sign in to the alternate Finess service.

The Finess IPPA failover logic has two triggers to detect failure:

- Finess IPPA receives a SystemInfo event that the current server is OUT_OF_SERVICE.

  Finess IPPA polls SystemInfo every 5 seconds to check whether the Finess server is in service. After three attempts, if the Finess server is not in service, Finess IPPA displays a server unavailable message to the agent.

- Finess IPPA receives an XMPP connection notification that the XMPP connection is disconnected.

  Finess IPPA tries every 5 seconds to reconnect with the XMPP server. After three attempts, if the XMPP connection cannot be reestablished, Finess IPPA displays a server unavailable message to the agent.

While the agent is still signed in to the current service, Finess IPPA continues attempting to reestablish the connections with the Finess and XMPP servers. If they both resume service, Finess IPPA displays the sign-in screen and the agent can sign in again and continue as normal.

Otherwise, the agent must exit the current Finess service and try to connect using an alternate Finess service.

Finess IPPA failover can occur for the following reasons:

- The Finess Webapp Service goes down.

- The Cisco Finess Notification Service goes down.

- If Finess takes longer to failover to the alternate CTI server than it takes for Finess IPPA to detect a server failure, then Finess IPPA declares the Finess server out of service.
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.

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.

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/](http://sshwindows.sourceforge.net/))
- Cygwin (see [http://www.cygwin.com/](http://www.cygwin.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

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

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 1</th>
<th>Access the DRS application (<a href="https://Finesse">https://Finesse</a> server IP:8443/drf).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Backup &gt; Backup Device.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Add New 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 Save.</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 1</th>
<th>Access the DRS application (<a href="https://Finesse">https://Finesse</a> server IP:8443/drf).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Backup &gt; Scheduler.</td>
</tr>
</tbody>
</table>
Perform Manual Backup

Procedure

Step 1 Access the DRS application (https://Finesse server IP:8443/drf).
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 Access the DRS application (https://Finesse server IP:8443/drf).
Step 2 Select Backup > Current Status to check the backup status.
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 Finesse server:

```
utils dbreplication stop all
```

**Step 9** Run the following CLI command on the primary Finesse server 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 Finesse node. 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`. 
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. Because Finesse is not a licensed server, you can disregard these warnings.

File Commands

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

Show Commands

- show account
- show date
- show disk usage
- show hardware
- show logins
- show myself
- show network
- show network ipprefs
- show open
- show packages
- show perf
- show status
- show tech all
- show tech dberrcode
- show tech gateway
- show tech locales
- show tech params
- show tech prefs
- show tech repltimeout
- show tech runtime
- show tech systables
- show tech systems
- show tech version
- show timezone
- show trace
- show version
- show network ipv6 settings
- show tls server min-version
- show tls client min-version

**Utils Commands**

- utils core active list
- utils core inactive list
• utilscsa enable
• utilscsadisable
• utilscsastatus
• utilsdbereplication clusterreset
• utilsdbereplication dropadmindb
• utilsdbereplication forcedatasynccsub
• utilsdbereplication reset
• utilsdbereplication runtimestate
• utilsdbereplication setrepltimeout
• utilsdbereplication stop
• utilsdiasgnose test
• utilsfirewall ipv4
• utilsiostat
• utilsnetwork arp
• utilsnetwork capture eth0
• utilsnetwork connectivity
• utilsnetwork host
• utilsnetwork ping
• utilsnetwork traceroute
• utilsntp
• utilsntp config
• utilsntp restart
• utilsntp server add
• utilsntp server delete
• utilsntp server list
• utilsntp status
• utilsntp start
• utilsrmetric
• utilsservice
• utilssystem
Supported Cisco Unified Communications OS Services

- utilssystemboot
- utilssystemrestart
- utilssystemupgrade
- utilsvmtoolsstatus

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

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

Although Finesse provides access to all Cisco Unified Communications Manager CLIs, many commands are not applicable to Finesse and most have not been validated for Finesse.

You can access the CLI directly, using the monitor and keyboard at the server console, or by SSH. Sign in with the Administrator User credentials created during installation.

- Commands Supported for Cisco Finesse, on page 141

Commands Supported for Cisco Finesse

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

Cisco Finesse HTTPS Redirect

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

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

- Note

This command does not impact the Finesse REST APIs.

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

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

- To retrieve the status of Cisco Finesse HTTPS Redirect: `utils finesse application_https_redirect status`

  This command displays whether Cisco Finesse HTTPS Redirect is currently enabled or disabled on the system.
On the secondary server, the HTTPS redirect status appears as enabled for the Finesse Agent Desktop only. For Finesse Admin, the HTTPS redirect status always appears as disabled on the secondary server because Finesse Admin is not available on the secondary server.

**Note**

- To enable Cisco Finesse HTTPS Redirect: `utils finesse application_https_redirect enable`
  
  You must stop the Cisco Finesse Tomcat Service before you can enable Cisco Finesse HTTPS Redirect. You can use the following command to stop this service: `utils service stop Cisco Finesse Tomcat`.
  
  If the Cisco Finesse Tomcat Service is not stopped, the command to enable Cisco Finesse HTTPS Redirect fails. This command also fails if Cisco Finesse HTTPS Redirect is already enabled.
  
  After you enable Cisco Finesse HTTPS Redirect, start the Cisco Finesse Tomcat Service using the command `utils service start Cisco Finesse Tomcat`.
  
- To disable Cisco Finesse HTTPS Redirect: `utils finesse application_https_redirect disable`
  
  You must stop the Cisco Finesse Tomcat Service before you can disable Cisco Finesse HTTPS Redirect. You can use the following command to stop this service: `utils service stop Cisco Finesse Tomcat`.
  
  If the Cisco Finesse Tomcat Service is not stopped, the command to disable Cisco Finesse HTTPS Redirect fails. This command also fails if Cisco Finesse HTTPS Redirect is already disabled.
  
  After you disable Cisco Finesse HTTPS Redirect, start the Cisco Finesse Tomcat Service using the command `utils service start Cisco Finesse Tomcat`.

**Finesse Services**

To view, start, or stop services:

- To view the platform TCP/IP services, UDP services, and Unix domain sockets used by Cisco Finesse: `show network all detail`
  
- To retrieve the status of services: `utils service list`
  
  This command retrieves a list of all services and their status.
  
  Services are shown in one of the following states: STOPPED, STARTING, or STARTED.
  
  STOPPED means the service is not running. STARTING means the service is starting operation and performing any necessary initialization. STARTED means the service has successfully initialized and is operational.
  
- To start a service: `utils service start service name`
  
  This command starts the named service.
  
- To stop a service: `utils service stop service name`
  
  This command stops the named service.
  
- To start Cisco Finesse Tomcat: `utils service start Cisco Finesse Tomcat`
  
- To stop Cisco Finesse Tomcat: `utils service stop Cisco Finesse Tomcat`
• To restart Cisco Finesse Tomcat: `utils service restart 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 Notification Service Logging**

To view the status of, enable, or disable Cisco Finesse Notification Service logging:

• To retrieve the status of Cisco Finesse Notification Service logging: `utils finesse notification logging status`

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

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

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

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

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

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

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

---

**Related Topics**

- [Log Collection](#) on page 114
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.

**Note**
After execution of each command, wait for 60 seconds for the changes to take effect.

- **utils finesse trace status**
  This command allows you to displays 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.

Cisco Finesse 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]**: Enable Cisco Finesse toaster notification.
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 only available in Windows OS for Chrome browser. In Mac OS, the Chrome browser automatically closes the toaster notification.

- **utils finesse toaster disable**: Disable Cisco Finesse toaster notification.
- **utils finesse toaster status**: Display the status (enable or disable) of the Cisco Finesse toaster notification.

Cisco Finesse toaster notifications do not work with Internet Explorer browser.

### Cisco Finesse IPPA Inactivity Timeout

Use the following CLI commands to enable or disable the Inactivity Timeout feature in Cisco Finesse IPPA. You must either disable the Cisco 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 does not get logged out of Cisco Finesse IPPA if the agent is on any other screen:

- **utils finesse ippa_inactivity_timeout enable**: To enable Cisco Finesse IPPA Inactivity Timeout feature.

  - **Note**: The default time set for Cisco Finesse IPPA Inactivity Timeout is 120 seconds.

- **utils finesse ippa_inactivity_timeout disable**: To disable Cisco Finesse IPPA Inactivity Timeout feature.

  - **Note**: When Cisco Finesse IPPA Inactivity Timeout is disabled, you will not be logged out of Cisco Finesse IPPA, if the agent is on any other screen.

- **utils finesse ippa_inactivity_timeout enable inactivity_timeout**: To enable Cisco 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).

- **utils finesse ippa_inactivity_timeout status**: To check the status of Cisco Finesse IPPA Inactivity Timeout.
The Finesse IPPA Inactivity Timeout CLIs should be run on both the primary and secondary Finesse servers. Enabling or disabling the Cisco Finesse Inactivity Timeout 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.

To know how this feature works on specific IP phone models, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html

Service Properties

Configure the service properties using the following CLI.

Enable or Disable Secure XMPP Socket—Port 5223

To run this CLI in Cisco Finesse, install Release 11.6(1) ES10 COP or higher.
To run this CLI in Cisco Finesse, install Finesse 12.0(1) ES4 COP or higher.

Use the following CLI commands to enable or disable the external access to the Cisco Finesse Notification Service XMPP port (5223). The port must be enabled for external access 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`
- To display the current status: `utils finesse show_property webservices enableExternalNotificationPortAccess`

Upgrade

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

To initiate an upgrade: `utils system upgrade initiate`
This command allows you to install upgrades and Cisco Option Package (COP) files from both local and remote directories.

To cancel an upgrade: `utils system upgrade cancel`

Shutdown

To shut down Finesse: `utils system shutdown`

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 both the primary and secondary Finesse servers.
Remote Account Management

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

`utils remote_account`

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

- `utils remote_account create account life`
  - `account` is the account name. `life` indicates the life of the account in days.
- `utils remote_account disable`
- `utils remote_account enable`
- `utils remote_account status`

Replication Status

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

- `utils dbreplication runtimestate`
  - This command returns the replication status on both the primary and secondary Finesse servers.
  - Check the RTMT counter value for replication. If all nodes in the cluster show a replication status of 2, replication is functioning correctly.
  - If the RTMT counter value for replication status is 3 or 4 for all nodes in the cluster, replication is set up but an error occurred and replication is not functioning properly.
  - If the majority of the nodes show a value of 0 or 1, run the command `utils dbreplication reset all` from the primary Finesse server.
  - If any node shows any replication value other than 1 or 2, replication is not set up correctly.
  - To fix replication, contact Cisco Technical Support.

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:

`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 3rd party gadget account must be between 5 and 32 characters long and cannot contain spaces or double quotes ("").

---

**Note**

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

---

**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:

- `utils finesse queue_statistics enable`
- `utils finesse queue_statistics disable`
- `utils 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.

---

**Note**

When enabled, Queue Statistics supports a maximum of 1500 users (Agents and Supervisors).
Certificates for Live Data

The procedures in this appendix are applicable only for Unified CCE deployments. For information about Live Data certificates with Packaged CCE deployments, see the Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide.

- Certificates and Secure Communications, on page 149
- Export Self-Signed Live Data Certificates, on page 149
- Import Self-Signed Live Data Certificates, on page 150
- Obtain and Upload Third-party CA Certificate, on page 151

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.

  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), you must first export the certificates from Live Data and Cisco Unified Intelligence Center, as described in this procedure. You must export from both Side A and Side B of the Live
Data and Cisco Unified Intelligence Center servers. You must then import the certificates into Finesse, importing both Side A and Side B certificates into each side of the Finesse servers.

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

**Procedure**

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

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

**Step 3** Click Find.

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

- If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)
- If you are using self-signed certificate, do the following:
  
  a. Click Generate New.
  
  b. When the certificate generation is complete, restart the Cisco Tomcat service and the Cisco Live Data NGNIX service.
  
  c. Restart this procedure.

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

Be sure to perform these steps for both Side A and Side B.

**Step 6** After you have downloaded the certificates from Cisco Unified Intelligence Center, sign in to Cisco Unified Operating System Administration on the Live Data server (http://hostname of LiveData server/cmplatform), and repeat steps 2 to 5. This is applicable only for Standalone LiveData.

---

**What to do next**

You must now 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: http://FQDN of Finesse server:8443/cmplatform

**Step 2** From the Security menu, select Certificate Management.
Step 3  Click Upload Certificate.
Step 4  From the Certificate Name drop-down list, select tomcat-trust.
Step 5  Click Browse and browse to the location of the Cisco Unified Intelligence Center certificate (with the .pem file extension).
Step 6  Select the file, and click Upload File.
Step 7  After you have uploaded the Cisco Unified Intelligence Center certificate repeat steps 3 to 6 for Live Data certificates. This is applicable only for standalone Live Data.
Step 8  After you upload both the certificates, restart Cisco Finesse Tomcat on the Finesses server.

What to do next
Be sure to 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 a Certificate Signing Requests (CSR).
- 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