Cisco Finesse Administration Guide Release 11.6(1)

First Published: 2017-08-24

Last Modified: 2020-05-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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.

CONTENTS

PREFACE

CHAPTER 1

CHAPTER 11

CHAPTER 12

CHAPTER 13

CHAPTER 14

Preface

This guide describes how to administer Cisco Finesse.

Change History

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

Change	**Date**
Added new service property configuration CLI for port 5223.	May 5, 2020
Initial Release of the Document for Release 11.6(1)	August 10, 2017
Cisco Finesse localization supports new languages.	
Configure Proxy Server and Browser proxy in Context Service Settings.	
Cisco Finesse application does not support configuration of QoS settings in network traffic.	
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.	

About This Guide

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

Audience

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

For information about administering Finesse within a Unified Contact Center Express environment, see *Cisco Unified Contact Center Express Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

Related Documents

Document or resource	Link
Cisco Finesse Documentation Guide	https://www.cisco.com/en/US/partner/products/ps11324/products_documentation_roadmaps_list.html
Configure SNMP Trap in Cisco Finesse	https://www.cisco.com/c/en/us/support/docs/contact-center/finesse/214387-configure-snmp-trap-in-cisco-finesse.html
Cisco.com site for Finesse documentation	https://www.cisco.com/en/US/partner/products/ps11324/tsd_products_support_series_home.html

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:

Convention	Description
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**.

Convention	Description
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems, Inc. </title></html>`
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

CHAPTER 1

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

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 Managementand 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 Finesse server.

Sign In to Cisco Finesse Administration Console

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

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

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

Step 2 The first time you access the administration console using HTTPS, you are prompted to trust the self-signed certificate provided with Finesse. The following table describes the steps for each supported browser.

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

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

Option	Description
If you use Internet Explorer:	**a.** A page appears that states this site is untrusted. **b.** Click **More information** > **Go on to the webpage**.
If you use Edge	**a.** A page appears that states this site is untrusted. **b.** Click **Details** and click **Go on to the webpage**.
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**.

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:

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 **tomcat**.
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).

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 **tomcat**.
c) Click **Download CSR**.

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

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

https://*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**.

The Add Roles Wizard opens.

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

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

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

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

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

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

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

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

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

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

Client-Side Certificate Acceptance

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

For more information on client requirements, see *Compatibility Information* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

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

Deploy Root Certificate for Internet Explorer

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

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

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

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

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

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

Step 5 Import the *ca_name*.cer file.

Step 6 Go to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Certificate Services Client - Auto-Enrollment**.

Step 7 From the Configuration Model list, select **Enabled**.

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

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

Set Up CA Certificate for Internet Explorer Browser

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

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

Procedure

Step 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**.

Step 2 Click **Install Certificate** > **Next** > **Place all certificates in the following store**.

Step 3 Click **Browse** and select **Trusted Root Certification Authorities**.

Step 4 Click **OK**.

Step 5 Click **Next**.

Step 6 Click **Finish**.

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

Step 7 Click **Yes**.

A message appears that states the import was successful.

Step 8 To verify the certificate was installed, open Internet Explorer. From the browser menu, select **Tools** > **Internet Options**.

Step 9 Click the **Content** tab.

Step 10 Click **Certificates**.

Step 11 Click the **Trusted Root Certification Authorities** tab.

Step 12 Ensure that the new certificate appears in the list.

Step 13 Restart the browser for certificate installation to take effect.

Note If using Internet Explorer 11, you may receive a prompt to accept the certificate even if signed by private CA.

Set Up CA Certificate for Firefox Browser

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

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

Procedure

Step 1 From the Firefox browser menu, select **Options**.

Step 2 Click **Advanced**.

Step 3 Click the **Certificates** tab.

Step 4 Click **View Certificates**.

Step 5 Click **Authorities**.

Step 6 Click **Import** and browse to the *ca_name*.cer file (in which *ca_name* is the name of your certificate).

Step 7 Check the **Validate Identical Certificates** check box.

Step 8 Restart the browser for certificate installation to take effect.

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

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

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

Option	Description
If you use Internet Explorer:	**a.** A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)**. This action opens the sign in page for the administration console (or agent desktop). A certificate error appears in the address bar of your browser.

Option	Description
	b. Click **Certificate Error**, and then click **View Certificates** to open the Certificate dialog box. **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 Finesse server. 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

Language	Locale File
Bulgarian	Bg_BG
Catalan	Ca_ES
Czech	Cs_CZ
Croatian	Hr_HR
Danish	da_DK
Dutch	nl_NL
English	en_US
Finnish	fi_FI
French	fr_FR
German	de_DE
Hungarian	Hu_HU
Italian	it_IT
Norwegian	nb_NO
Portuguese	pt_BR
Romanian	Ro_RO

Language	Locale File
Spanish	es_ES
Swedish	sv_SE
Slovak	Sk_SK
Slovenian	Sl_SI
Serbian	Sr_RS
Japanese	ja_JP
Chinese (simplified)	zh_CN
Chinese (traditional)	zh_TW
Korean	ko_KR
Polish	pl_PL
Russian	ru_RU
Turkish	tr_TR

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

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

The following items are localized on the desktop:

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

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

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

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

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

Variable	Limit
Wrap-Up Reasons	Limited to 40 bytes of UTF-8 data.
Call Variables 1-10	Limited to 40 bytes of UTF-8 data. **Note** If Finesse sends a set call data request that exceeds 40 bytes of data, the request fails.
ECC Variables	UTF-8 data is limited to the maximum size in bytes for ECC variables specified in Unified CCE.

If any 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.

CHAPTER 2

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.

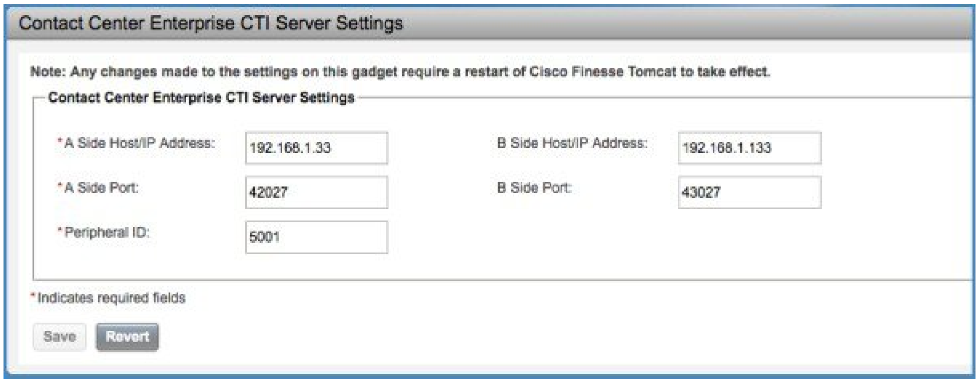
Contact Center Enterprise CTI Server Settings

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.



Contact Center Enterprise CTI Server Settings

Note: Any changes made to the settings on this gadget require a restart of Cisco Finesse Tomcat to take effect.

Contact Center Enterprise CTI Server Settings

*A Side Host/IP Address: 192.168.1.33

B Side Host/IP Address: 192.168.1.133

*A Side Port: 42027

B Side Port: 43027

*Peripheral ID: 5001

*Indicates required fields

Note 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.

Field	Explanation
A Side Host/IP Address	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.
A Side Port	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.
Peripheral ID	The ID of the Agent PG Routing Client (PIM). The Agent PG Peripheral ID should be configured to the same value for the A Side and B Side CTI server. This field is required and accepts values between 1 and 32767. The default value is 5000.
B Side Host/IP Address	Either the hostname or IP address of the B Side CTI server.

Field	Explanation
B Side Port	The port of the B Side CTI server. The value of this field must match the port configured during the setup of the B Side CTI server. This field accepts values between 1 and 65535.

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

Related Topics

View, Start, or Stop Services, on page 114

Configure Contact Center Enterprise CTI Server Settings

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

Procedure

Step 1 If you are not already signed in, sign in to the administration console on the primary Finesse server:

http://FQDN of Finesse server/cfadmin

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

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

Field	Description
A Side Host/IP Address	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.
A Side Port	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.
Peripheral ID	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.
B Side Host/IP Address	Enter the hostname or IP address of the B Side CTI server.
B Side Port	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.
Enable SSL encryption	Check this box to enable secure encryption.

Step 4 Click **Save**.

Contact Center Enterprise Administration & Data Server Settings

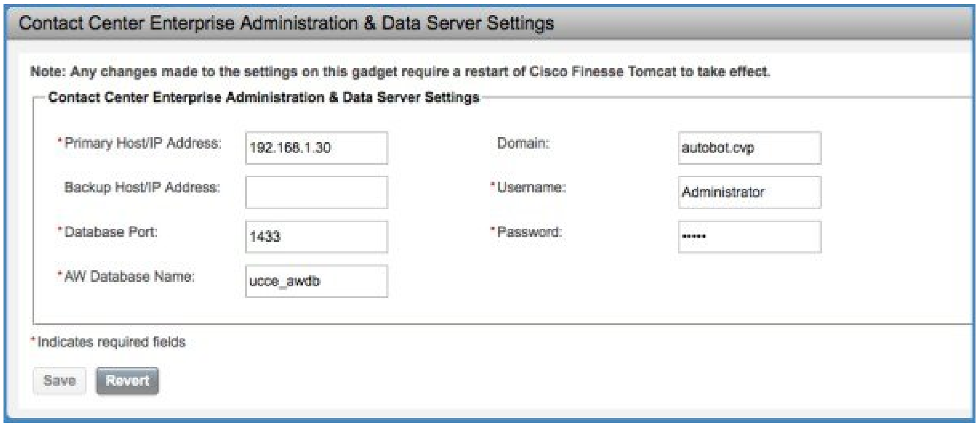
Use the Contact Center Enterprise Administration & Data Server Settings gadget to configure the database settings. These settings are required to enable authentication for Finesse agents and supervisors.

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.



Contact Center Enterprise Administration & Data Server Settings

Note: Any changes made to the settings on this gadget require a restart of Cisco Finesse Tomcat to take effect.

Contact Center Enterprise Administration & Data Server Settings

*Primary Host/IP Address:	192.168.1.30	Domain:	autobot.cvp
Backup Host/IP Address:		*Username:	Administrator
*Database Port:	1433	*Password:	•••••
*AW Database Name:	ucce_awdb		

*Indicates required fields

The following table describes the fields on the Contact Center Enterprise Administration & Data Server Settings gadget.

Field	Explanation
Primary Host/IP Address	Either the hostname or IP address of the Unified CCE Administration & Data Server.
Backup Host/IP Address	(Optional) Either the hostname or IP address of the backup Unified CCE Administration & Data Server.

Database Port	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.
AW Database Name	The name of the AW Database (AWDB) (for example, *ucceinstance*_awdb).
Domain	(Optional) The domain of the AWDB.
Username	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.
Password	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.

Related Topics

View, Start, or Stop Services, on page 114

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.

Field	Description
Primary Host/IP Address	Enter the hostname or IP address of the Unified CCE Administration & Data Server.
Backup Host/IP Address	Enter the hostname or IP address of the backup Unified CCE Administration & Data Server.
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.

Field	Explanation
Hostname	The hostname of the secondary Finesse server.

Actions on the Cluster Settings gadget:

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

Configure Cluster Settings

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

Procedure

Step 1 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.

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

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. Refer to the following links to configure the proxy settings for the related browsers.

Chrome	https://support.google.com/chrome/answer/96815?hl=en
Firefox	https://support.mozilla.org/en-US/kb/advanced-panel-settings-in-firefox
Internet Explorer	http://windows.microsoft.com/en-in/windows/change-internet-explorer-proxy-server-settings#1TC=windows-7

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**.

Field	Description
Proxy Server URL	Proxy Server address
Timeout	The number of milliseconds (ms) the system waits before rejecting the Context Service cloud connectivity. Default: 1000 milliseconds Range: 200 to 15,000 milliseconds.
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.

CHAPTER 3

Manage Call Variables Layouts

Call Variables Layouts

You can use the Call Variables Layouts gadget to define how call variables appear on the Finesse agent desktop. You can configure up to 200 unique Call Variables Layouts (one default 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.
- Finesse appends *(Default)* to the name of the default Call Variables Layout.
- To display a custom Call Variables Layout, in the Unified CCE routing script set the user.Layout ECC variable to the name of a configured Call Variables Layout. In this case, if no custom layouts match the user.Layout value (or no custom layouts are configured), Finesse displays the default layout.
- Finesse retains the custom layout as specified by the user.Layout ECC variable on CTI server failover. During PG failover, Finesse changes the active call layout to the default layout while retaining the call variables and time indicators.

Call Variables

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

- BACampaign
- BAAccountNumber
- BAResponse
- BAStatus
- 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

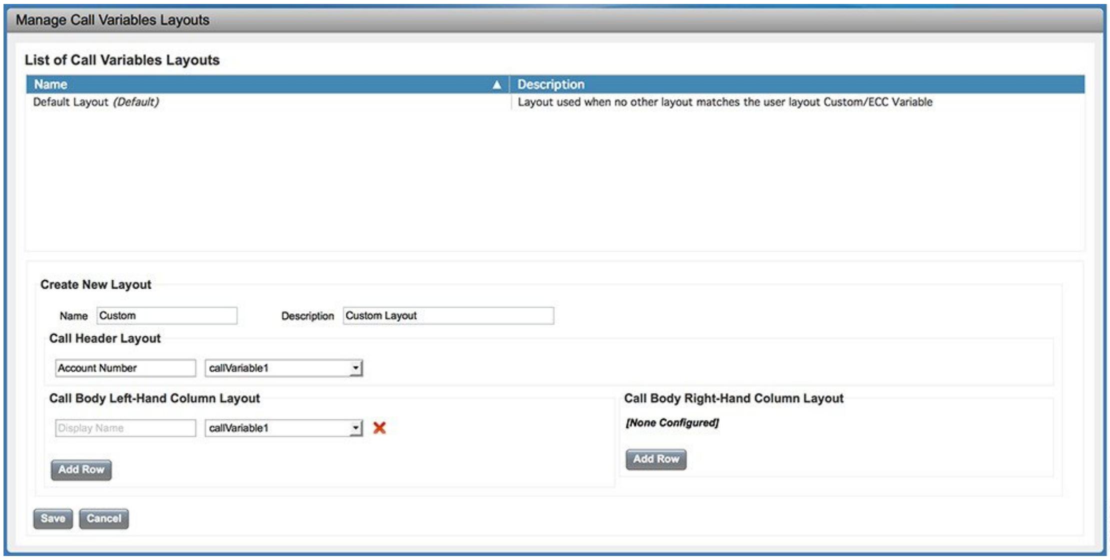
Procedure

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 <layout name> when editing an existing layout):

- Enter a name for the Call Variables Layout (maximum 40 characters).
- Enter a description of the Call Variables Layout (maximum 128 characters).



Manage Call Variables Layouts

List of Call Variables Layouts

Name ▲	Description
Default Layout *(Default)*	Layout used when no other layout matches the user layout Custom/ECC Variable

Create New Layout

Name: Custom   Description: Custom Layout

Call Header Layout

Account Number | callVariable1

Call Body Left-Hand Column Layout

Display Name | callVariable1 ✕

Call Body Right-Hand Column Layout

[None Configured]

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.

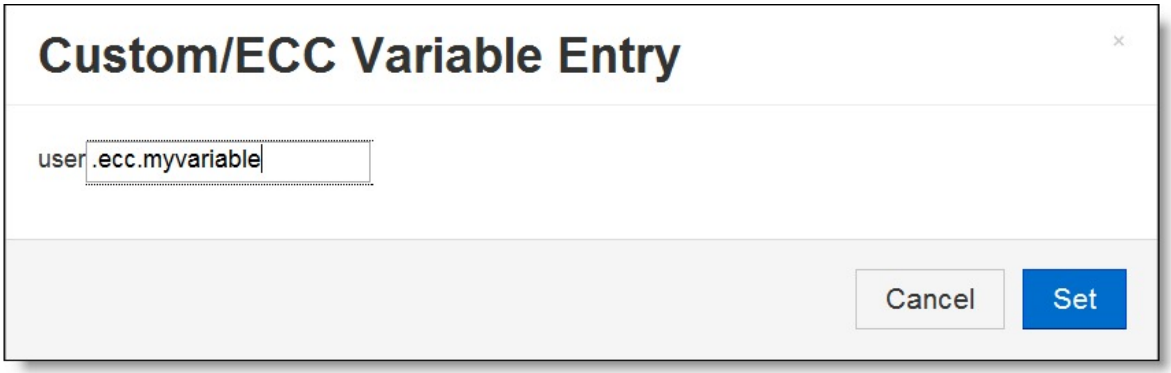
Step 6 To view the latest configured Call Variables Layout, click **Refresh** from the Manage Call Variables Layouts gadget.

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.



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.

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

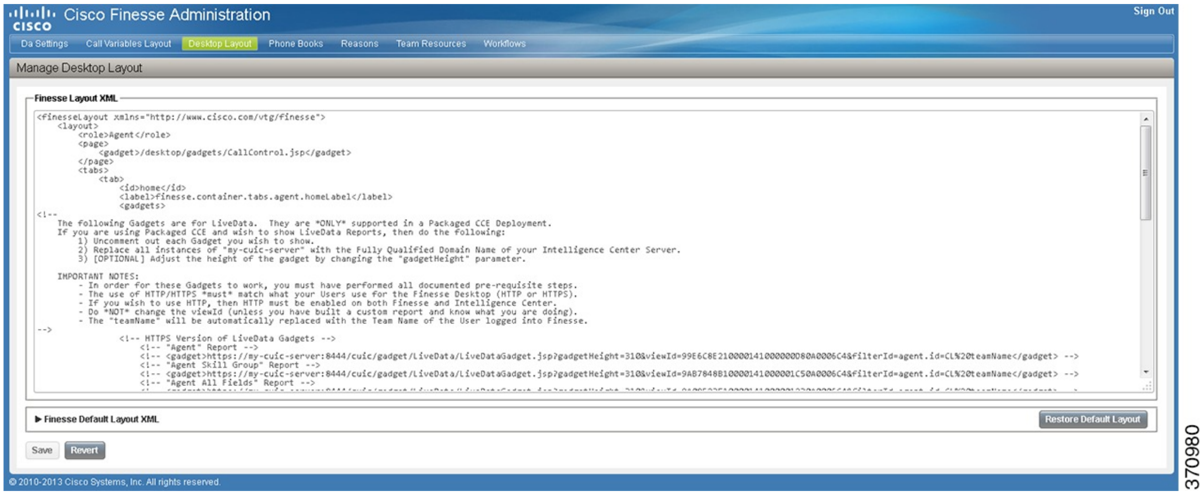
Factors that determine how much power is required for the client include, but are not limited to, the following:

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

Finesse Desktop Layout XML

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

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



```
<finesseLayout xmlns="http://www.cisco.com/vtg/finesse">
    <layout>
        <role>Agent</role>
        <page>
            <gadget>/desktop/gadgets/CallControl.jsp</gadget>
        </page>
        <tabs>
            <tab>
                <id>home</id>
                <label>finesse.container.tabs.agent.homeLabel</label>
                <gadgets>
<!--
    The following Gadgets are for LiveData.  They are *ONLY* supported in a Packaged CCE Deployment.
    If you are using Packaged CCE and wish to show LiveData Reports, then do the following:
        1) Uncomment out each Gadget you wish to show.
        2) Replace all instances of "my-cuic-server" with the Fully Qualified Domain Name of your Intelligence Center Server.
        3) [OPTIONAL] Adjust the height of the gadget by changing the "gadgetHeight" parameter.

    IMPORTANT NOTES:
        - In order for these Gadgets to work, you must have performed all documented pre-requisite steps.
        - The use of HTTP/HTTPS *must* match what your Users use for the Finesse Desktop (HTTP or HTTPS).
        - If you wish to use HTTP, then HTTP must be enabled on both Finesse and Intelligence Center.
        - Do *NOT* change the viewId (unless you have built a custom report and know what you are doing).
        - The "teamName" will be automatically replaced with the Team Name of the User logged into Finesse.
-->
                <!-- HTTPS Version of LiveData Gadgets -->
                    <!-- "Agent" Report -->
                    <!-- <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=99E6C8E210000141000000D80A0006C4&filterId=agent.id=CL%20teamName</gadget> -->
                    <!-- "Agent Skill Group" Report -->
                    <!-- <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=9AB7848B10000141000001C50A0006C4&filterId=agent.id=CL%20teamName</gadget> -->
                    <!-- "Agent All Fields" Report -->
```

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.

Note 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.

```
<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.

```
<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.

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

Step 2 Click **Save**.

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

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

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

Related Topics

Upload Third-Party Gadgets, on page 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.

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

The **alternateHosts** attribute is only applicable for gadgets with an absolute URL. That is URLs containing the FQDN of a host, an optional port, and the complete URL path to the gadget. For example: <gadget alternateHosts="host1,host2">*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 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"/>
  <!-- URI of the gadget xml -->
      </xs:sequence>
  </xs:complexType>
</xs:element>

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

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

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

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

<xs:element name="finesseLayout">
```

```
<!-- Layout of the desktop -->
 <xs:complexType>
     <xs:sequence maxOccurs="3">
     <!-- only support 3 roles for now -->
     <xs:element ref="layout" />
     </xs:sequence>
 </xs:complexType>
 </xs:element></xs:schema>
```

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.

  For information about enabling HTTP for Cisco Unified Intelligence Center, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.
- Ensure that user integration synchronization is enabled for Cisco Unified Intelligence Center. For more information, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.
- 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.

Procedure	When to use
Add Live Data reports to default desktop layout	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.

Procedure	When to use
Add Live Data reports to custom desktop layout	Use this procedure if you have customized the Finesse desktop layout.
Add Live Data reports to team layout	Use this procedure if you want to add Live Data reports to the desktop layout for specific teams only.

Add Live Data Reports to Default Desktop Layout

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

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

Step 4 Replace my-cuic-server with the fully qualified domain name of your Cisco Unified 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=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
        </gadget>
```

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

Step 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.

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.

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

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

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

Step 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:

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

Step 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=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 8 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.

Add Live Data Reports to Team Layout

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

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

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

Step 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:

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

Step 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:

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

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

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

Step 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.

Modify Live Data Stock Reports for Finesse

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

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

Procedure

Step 1 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:

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

```
filterId_2=agent.id=CL%20teamName
</gadget>
```

Step 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 the permalink 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.htmx?
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid
```

Step 2 From the Finesse default layout XML, copy the gadget URL for one of the Live Data reports and paste it into a text editor.

Example:

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

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

Step 3 To update the URL to refer to a different report view, populate the viewId_1 value (after the equal sign) with the desired viewId obtained in step 1.

Example:

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

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

Step 4 For each additional view you want to include:

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

Example:

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

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

Example:

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

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

Example:

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

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

- Agent Reports: filterId_*N*=agent.id=CL%20teamName
- Agent Skill Group Reports: filterId_*N*=agent.id=CL%20teamName
- Skill Group Reports: filterId_*N*=skillGroup.id=CL%20teamName
- Precision Queue Reports: filterId_*N*=precisionQueue.id=CL%20teamName

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

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

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.

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.

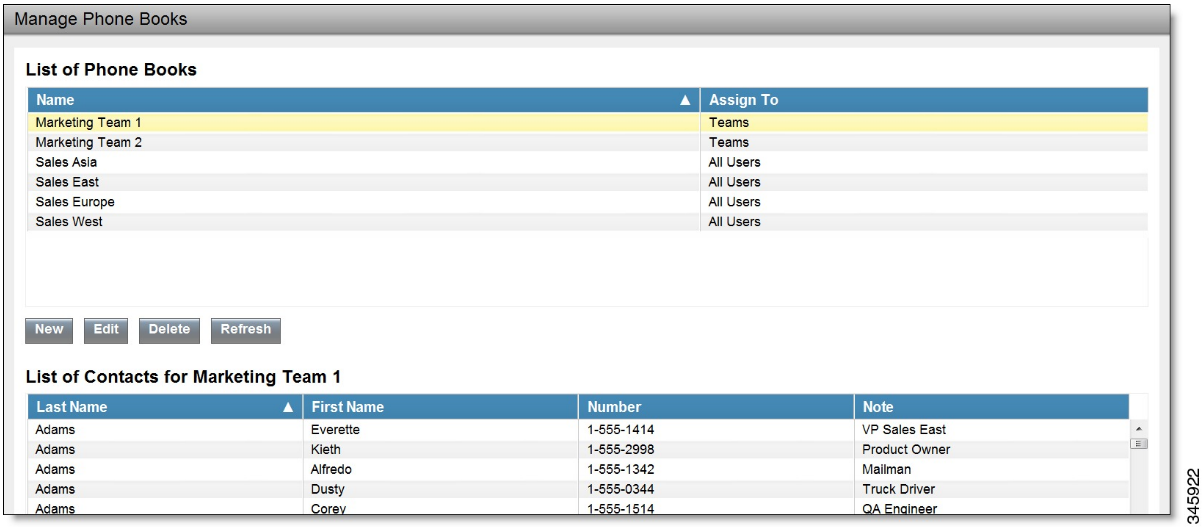
Phone Books and Contacts

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.



List of Phone Books

Name ▲	Assign To
Marketing Team 1	Teams
Marketing Team 2	Teams
Sales Asia	All Users
Sales East	All Users
Sales Europe	All Users
Sales West	All Users

List of Contacts for Marketing Team 1

Last Name ▲	First Name	Number	Note
Adams	Everette	1-555-1414	VP Sales East
Adams	Kieth	1-555-2998	Product Owner
Adams	Alfredo	1-555-1342	Mailman
Adams	Dusty	1-555-0344	Truck Driver
Adams	Corey	1-555-1514	QA Engineer

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

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

Actions on the Manage Phone Books gadget:

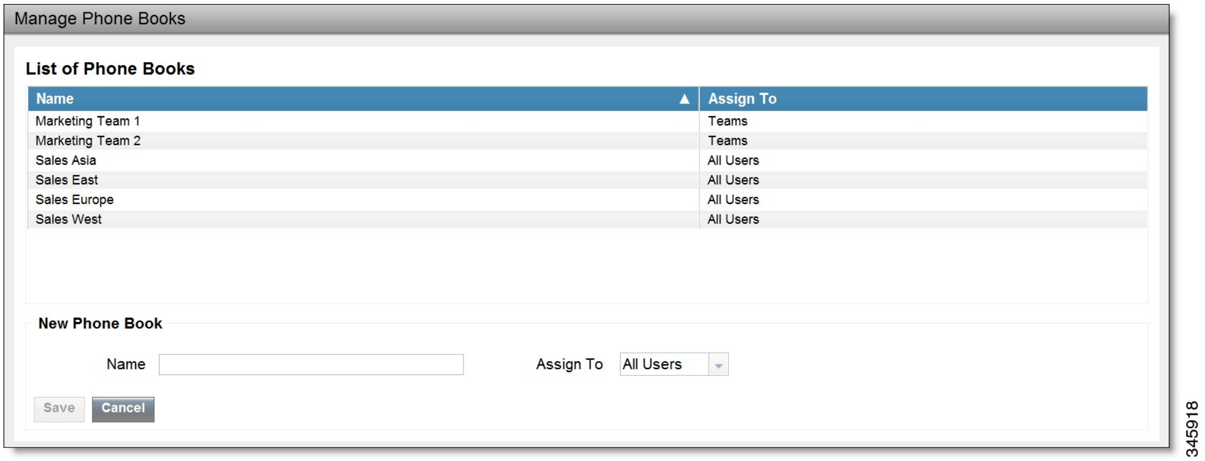
- **New:** Add a new phone book or contact
- **Edit:** Edit an existing phone book or contact
- **Delete:** Delete a phone book or contact
- **Refresh:** Reload the list of phone books or contacts from the server
- **Import:** Import a list of contacts to the phone book
- **Export:** Export a list of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

Add Phone Book

Procedure

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

The Manage Phone Books area appears.



Manage Phone Books

List of Phone Books

Name ▲	Assign To
Marketing Team 1	Teams
Marketing Team 2	Teams
Sales Asia	All Users
Sales East	All Users
Sales Europe	All Users
Sales West	All Users

New Phone Book

Name

Assign To: All Users

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**.

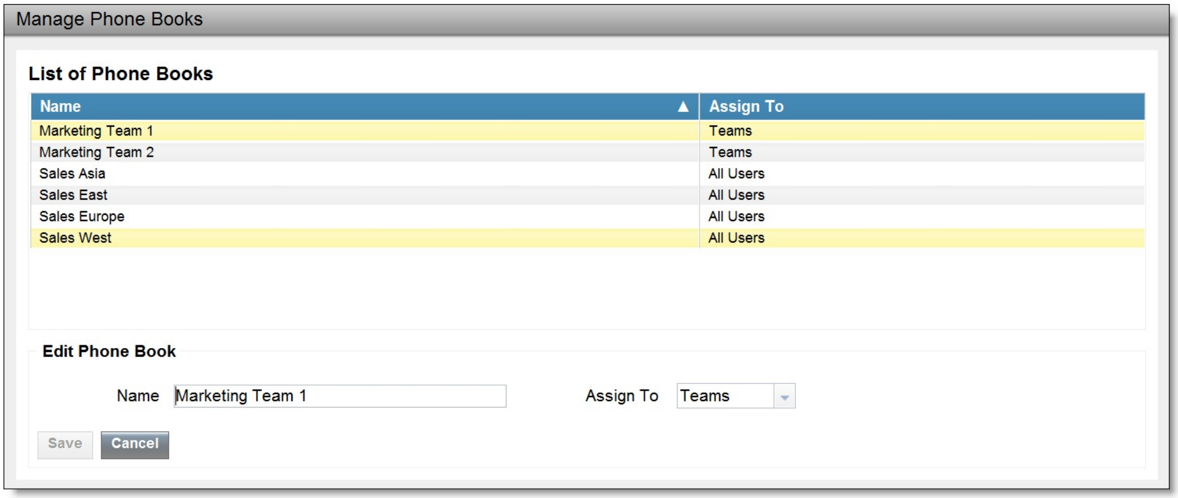
Edit Phone Book

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.



Manage Phone Books

List of Phone Books

Name ▲	Assign To
Marketing Team 1	Teams
Marketing Team 2	Teams
Sales Asia	All Users
Sales East	All Users
Sales Europe	All Users
Sales West	All Users

Edit Phone Book

Name: Marketing Team 1

Assign To: Teams

345921

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.

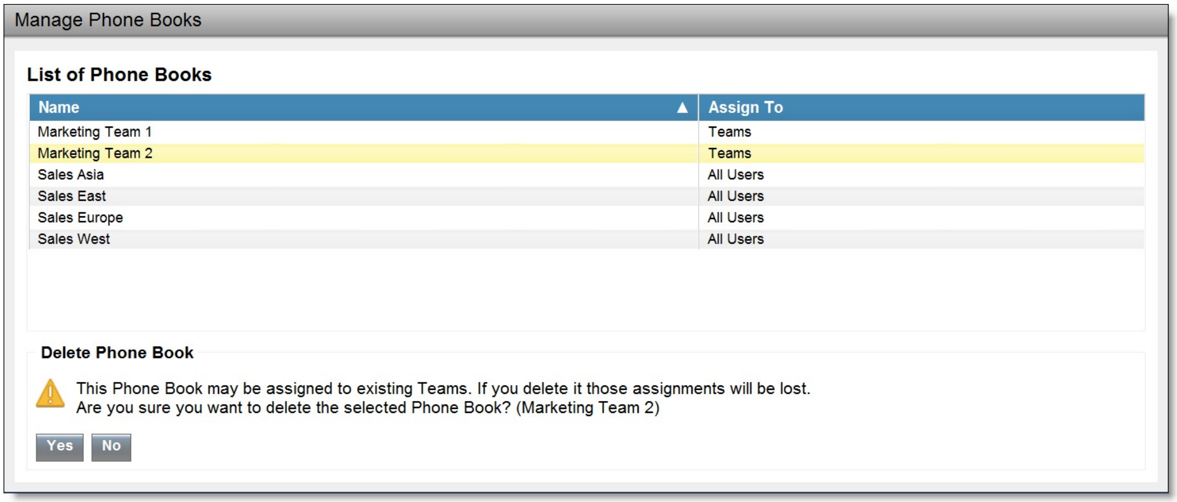
Delete Phone Book

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.



Manage Phone Books

List of Phone Books

Name ▲	Assign To
Marketing Team 1	Teams
Marketing Team 2	Teams
Sales Asia	All Users
Sales East	All Users
Sales Europe	All Users
Sales West	All Users

Delete Phone Book

This Phone Book may be assigned to existing Teams. If you delete it those assignments will be lost.
Are you sure you want to delete the selected Phone Book? (Marketing Team 2)

345920

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.

Field	Max Length	Can Be Blank?	Permitted Characters
First Name	128	Yes	Alphanumeric characters **Note** The CSV file that contains the contacts to import must use Latin encoding.
Last Name	128	Yes	
Phone Number	32	No	
Notes	128	Yes	

The following is an example of a phone book CSV file:

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

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

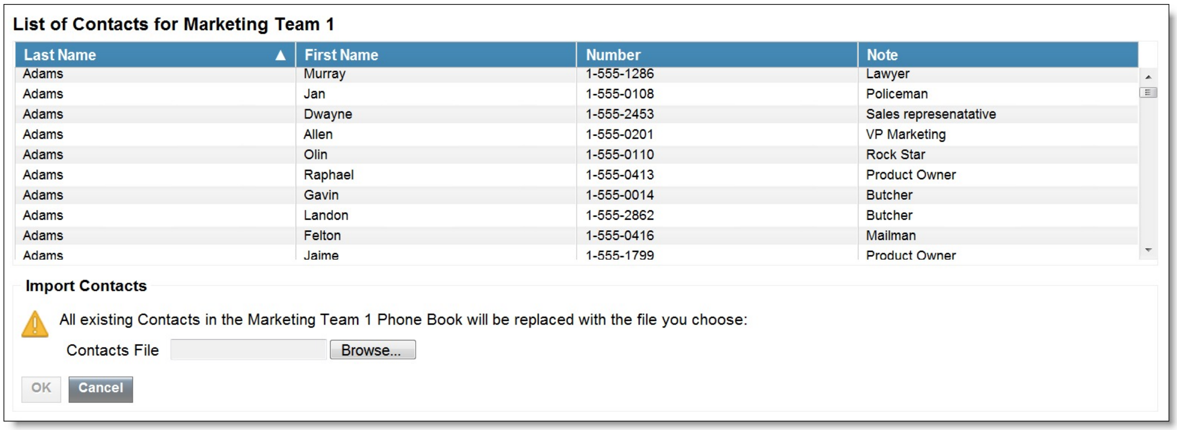
Note Exported CSV files always show each field enclosed in double quotes, as in the preceding example, to ensure that any commas or double quotes that are part of the actual filed data are not mistaken for field delimiters. If your data does not include these characters, you can omit the double quotes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

Procedure

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

Step 2 Click **Import**.

The Import Contacts area appears.



List of Contacts for Marketing Team 1

Last Name ▲	First Name	Number	Note
Adams	Murray	1-555-1286	Lawyer
Adams	Jan	1-555-0108	Policeman
Adams	Dwayne	1-555-2453	Sales represenatative
Adams	Allen	1-555-0201	VP Marketing
Adams	Olin	1-555-0110	Rock Star
Adams	Raphael	1-555-0413	Product Owner
Adams	Gavin	1-555-0014	Butcher
Adams	Landon	1-555-2862	Butcher
Adams	Felton	1-555-0416	Mailman
Adams	Jaime	1-555-1799	Product Owner

Import Contacts

All existing Contacts in the Marketing Team 1 Phone Book will be replaced with the file you choose:

Contacts File

345917

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

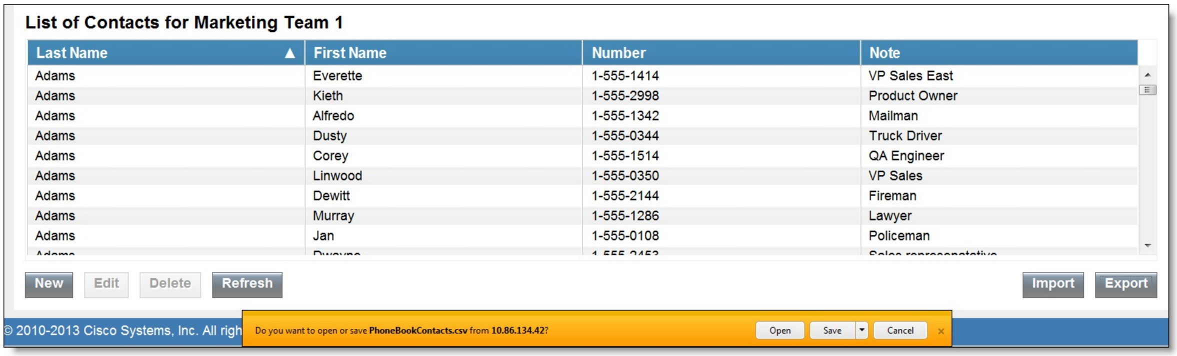
The Export function allows you to extract a list of contacts from an existing phone book. The exported list is saved in CSV format.

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.



List of Contacts for Marketing Team 1

Last Name ▲	First Name	Number	Note
Adams	Everette	1-555-1414	VP Sales East
Adams	Kieth	1-555-2998	Product Owner
Adams	Alfredo	1-555-1342	Mailman
Adams	Dusty	1-555-0344	Truck Driver
Adams	Corey	1-555-1514	QA Engineer
Adams	Linwood	1-555-0350	VP Sales
Adams	Dewitt	1-555-2144	Fireman
Adams	Murray	1-555-1286	Lawyer
Adams	Jan	1-555-0108	Policeman
Adams	Dwayne	1-555-2453	Sales representative

© 2010-2013 Cisco Systems, Inc. All righ

Do you want to open or save **PhoneBookContacts.csv** from **10.86.134.42**?

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

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

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

Related Topics

Import Contacts, on page 53

Add Contact

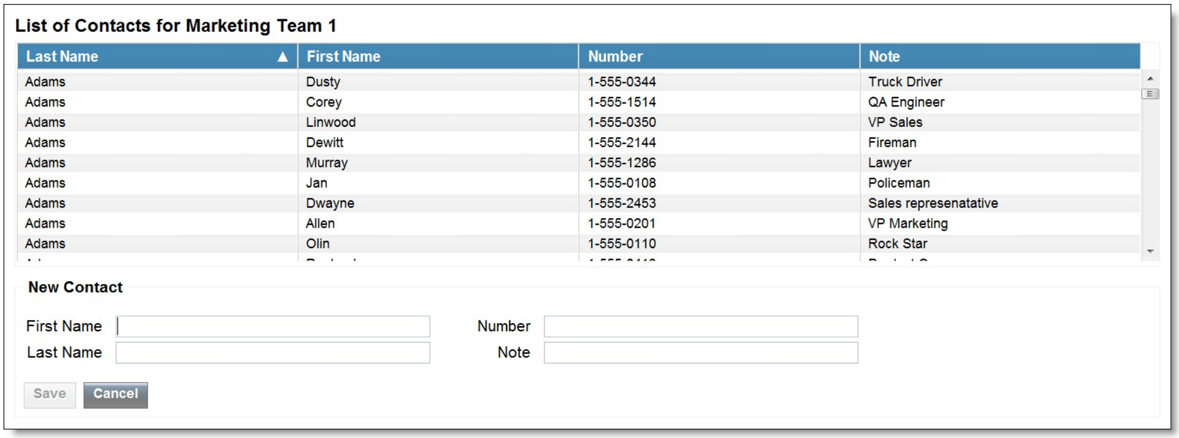
Procedure

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.



List of Contacts for Marketing Team 1

Last Name ▲	First Name	Number	Note
Adams	Dusty	1-555-0344	Truck Driver
Adams	Corey	1-555-1514	QA Engineer
Adams	Linwood	1-555-0350	VP Sales
Adams	Dewitt	1-555-2144	Fireman
Adams	Murray	1-555-1286	Lawyer
Adams	Jan	1-555-0108	Policeman
Adams	Dwayne	1-555-2453	Sales represenatative
Adams	Allen	1-555-0201	VP Marketing
Adams	Olin	1-555-0110	Rock Star

New Contact

First Name		Number	
Last Name		Note	

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

Step 4 Click **Save**.

Edit Contact

Procedure

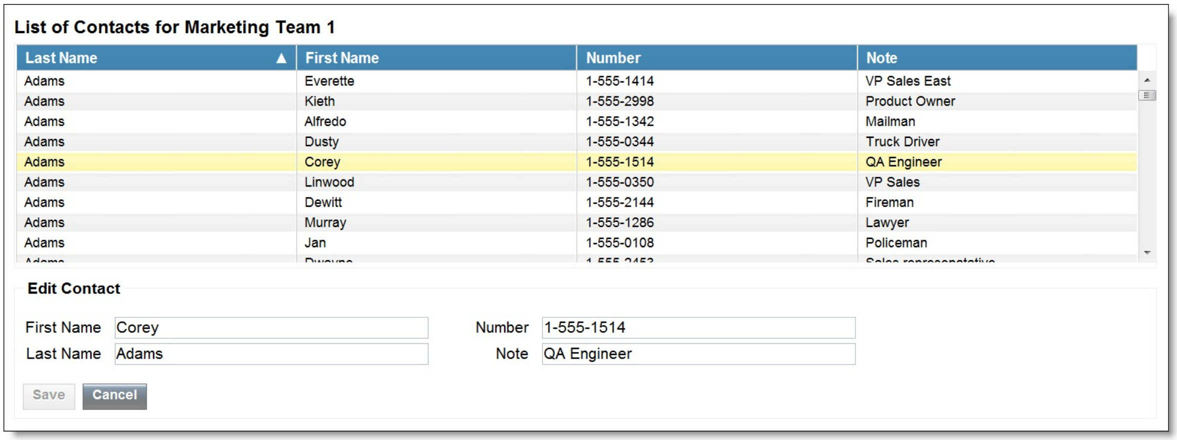
Step 1 In the Manage Phone Books gadget, select the phone book that contains the contact you want to edit.

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

Step 2 Select the contact you want to edit.

Step 3 Click **Edit**.

The Edit Contact area appears.



List of Contacts for Marketing Team 1

Last Name ▲	First Name	Number	Note
Adams	Everette	1-555-1414	VP Sales East
Adams	Kieth	1-555-2998	Product Owner
Adams	Alfredo	1-555-1342	Mailman
Adams	Dusty	1-555-0344	Truck Driver
Adams	Corey	1-555-1514	QA Engineer
Adams	Linwood	1-555-0350	VP Sales
Adams	Dewitt	1-555-2144	Fireman
Adams	Murray	1-555-1286	Lawyer
Adams	Jan	1-555-0108	Policeman
Adams	Dwayne	1-555-2453	Sales representative

Edit Contact

First Name: Corey
Last Name: Adams
Number: 1-555-1514
Note: QA Engineer

345915

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

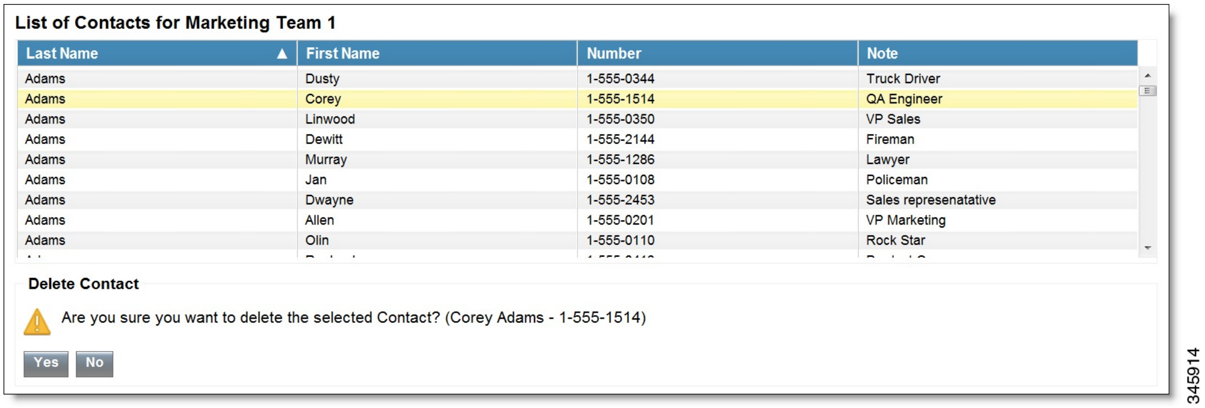
Step 1 In the Manage Phone Books gadget, select the phone book that contains the contact you want to delete.

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.



List of Contacts for Marketing Team 1

Last Name ▲	First Name	Number	Note
Adams	Dusty	1-555-0344	Truck Driver
Adams	Corey	1-555-1514	QA Engineer
Adams	Linwood	1-555-0350	VP Sales
Adams	Dewitt	1-555-2144	Fireman
Adams	Murray	1-555-1286	Lawyer
Adams	Jan	1-555-0108	Policeman
Adams	Dwayne	1-555-2453	Sales represenatative
Adams	Allen	1-555-0201	VP Marketing
Adams	Olin	1-555-0110	Rock Star

Delete Contact

⚠ Are you sure you want to delete the selected Contact? (Corey Adams - 1-555-1514)

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

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

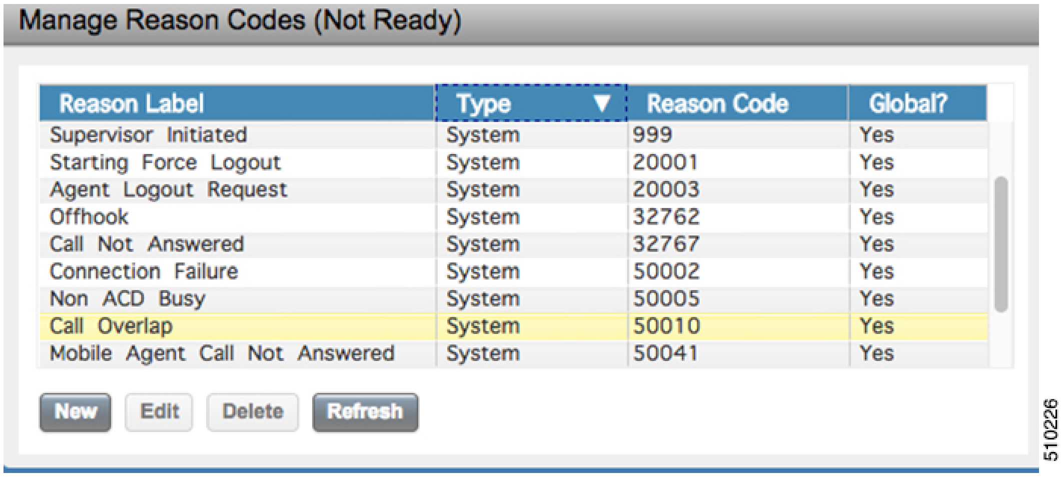
Not Ready Reason Codes

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).

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



Reason Label	Type	Reason Code	Global?
Supervisor Initiated	System	999	Yes
Starting Force Logout	System	20001	Yes
Agent Logout Request	System	20003	Yes
Offhook	System	32762	Yes
Call Not Answered	System	32767	Yes
Connection Failure	System	50002	Yes
Non ACD Busy	System	50005	Yes
Call Overlap	System	50010	Yes
Mobile Agent Call Not Answered	System	50041	Yes

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

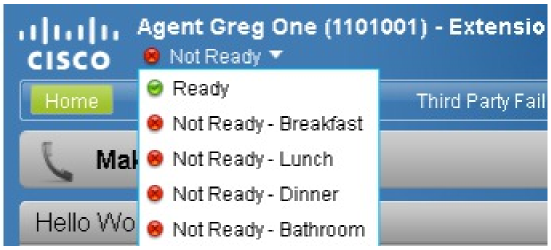
Field	Explanation
Reason Label	The label for the Not Ready reason code. The label has a maximum length of 40 characters and should be unique for each Not Ready reason code. Both alphanumeric and special characters are supported.
Type	The type of reason code (System or Custom). The column is default and can be sorted to display both System reason codes and Custom reason codes.
Reason Code	A code for the Not Ready reason. The code can be any value between 1 and 65535 and must be unique.
Global?	Yes/No. Indicates if the reason code is available globally to all agents (Yes) or to specific teams of agents (No).

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

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

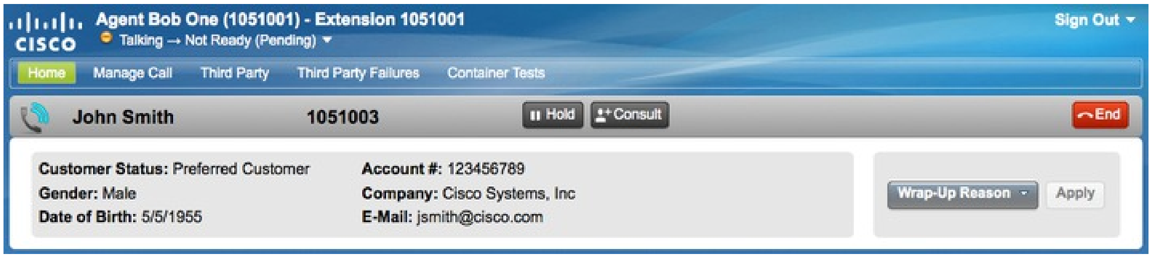
Note When you add, edit, or delete a Not Ready reason code, the changes you make take effect on the Finesse desktop after three seconds. However, agents who are signed in when the changes are made must sign out and sign back in to see those changes reflected on their desktops.

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



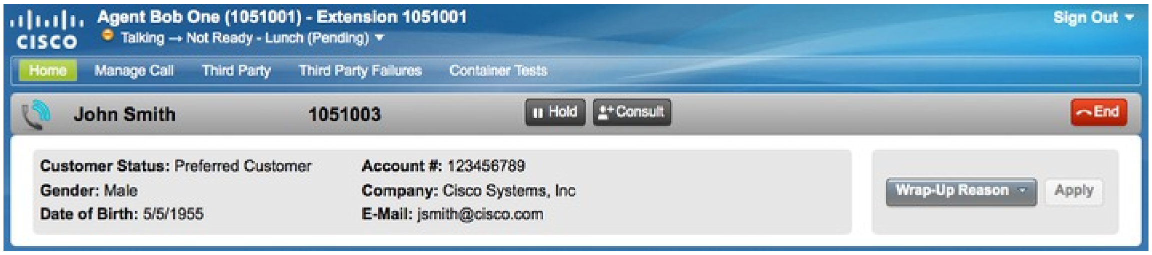
If an agent wants to change from Ready to Not Ready status, that agent can choose the appropriate Not Ready reason code from the list of configured codes.

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.



Customer Status: Preferred Customer
Gender: Male
Date of Birth: 5/5/1955
Account #: 123456789
Company: Cisco Systems, Inc
E-Mail: jsmith@cisco.com

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).



Customer Status: Preferred Customer
Gender: Male
Date of Birth: 5/5/1955
Account #: 123456789
Company: Cisco Systems, Inc
E-Mail: jsmith@cisco.com

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.

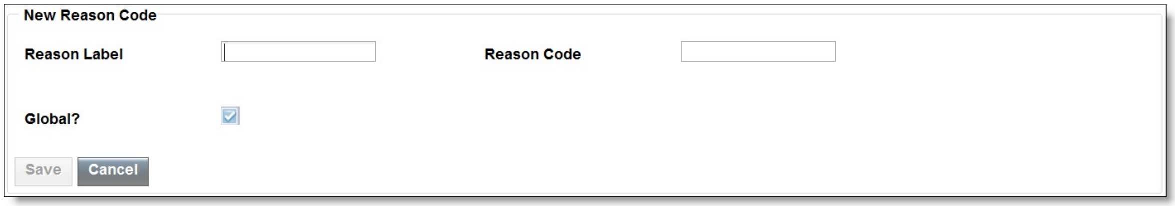
Add Not Ready Reason Code

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

Reason Label

Reason Code

Global? ☑

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

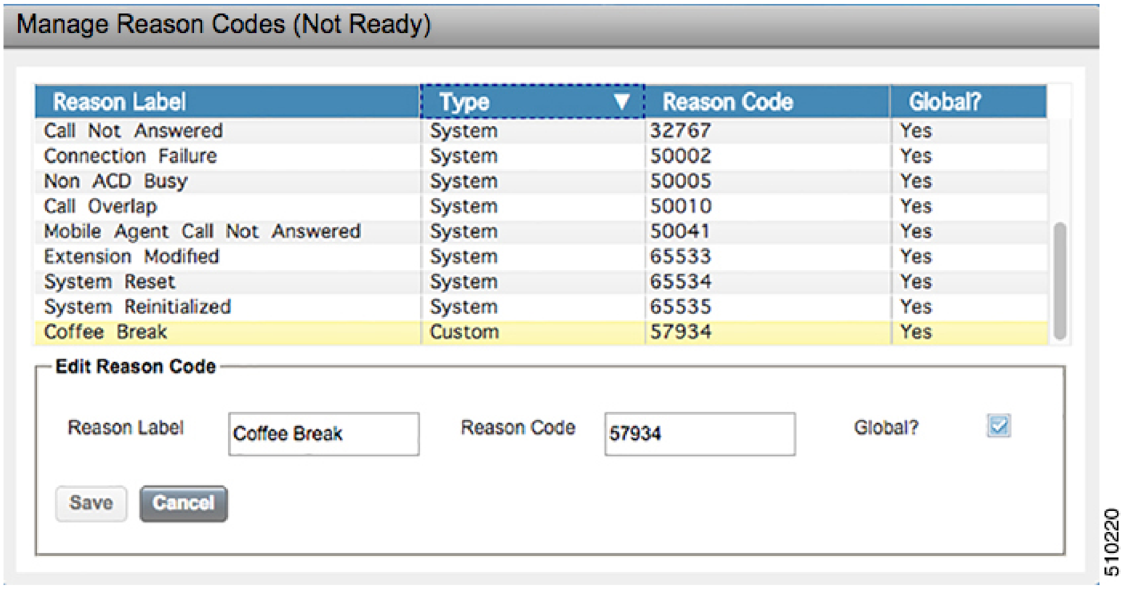
Perform the following procedure to edit the label or code for an existing Not Ready reason code.

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.



Manage Reason Codes (Not Ready)

Reason Label	Type ▼	Reason Code	Global?
Call Not Answered	System	32767	Yes
Connection Failure	System	50002	Yes
Non ACD Busy	System	50005	Yes
Call Overlap	System	50010	Yes
Mobile Agent Call Not Answered	System	50041	Yes
Extension Modified	System	65533	Yes
System Reset	System	65534	Yes
System Reinitialized	System	65535	Yes
Coffee Break	Custom	57934	Yes

Edit Reason Code

Reason Label: Coffee Break
Reason Code: 57934
Global? ☑

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.

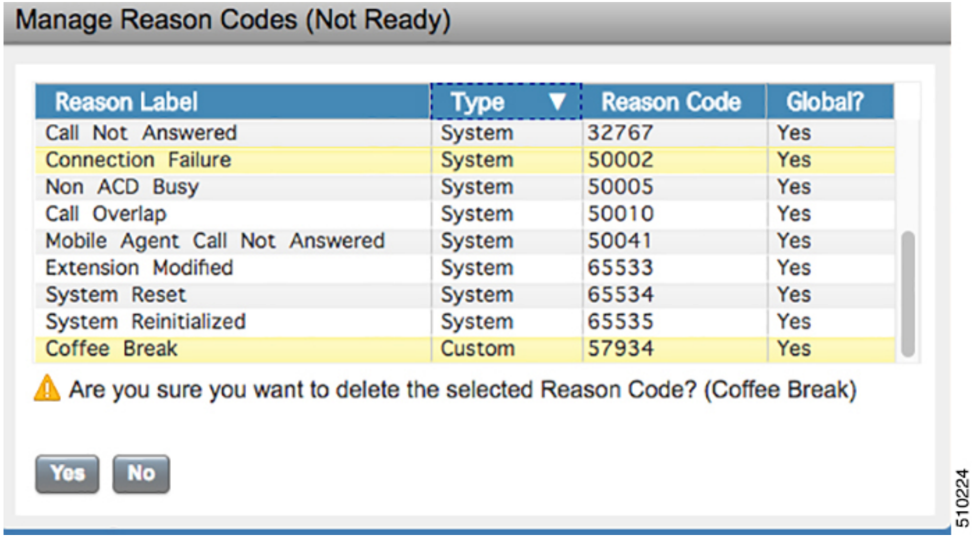
Perform the following procedure to delete a Not Ready reason code.

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.



Manage Reason Codes (Not Ready)

Reason Label	Type ▼	Reason Code	Global?
Call Not Answered	System	32767	Yes
Connection Failure	System	50002	Yes
Non ACD Busy	System	50005	Yes
Call Overlap	System	50010	Yes
Mobile Agent Call Not Answered	System	50041	Yes
Extension Modified	System	65533	Yes
System Reset	System	65534	Yes
System Reinitialized	System	65535	Yes
Coffee Break	Custom	57934	Yes

⚠ Are you sure you want to delete the selected Reason Code? (Coffee Break)

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

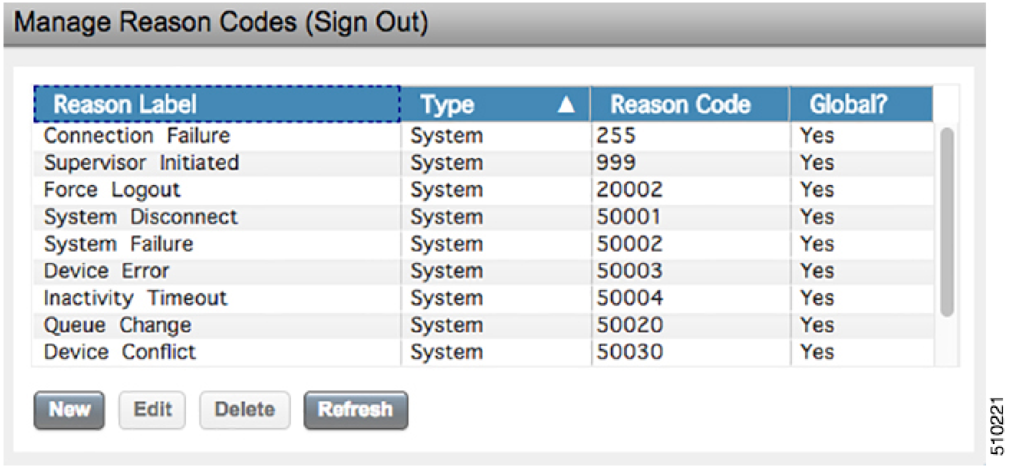
Sign Out Reason Codes

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

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

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

Note Finesse supports 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.



Manage Reason Codes (Sign Out)

Reason Label	Type ▲	Reason Code	Global?
Connection Failure	System	255	Yes
Supervisor Initiated	System	999	Yes
Force Logout	System	20002	Yes
System Disconnect	System	50001	Yes
System Failure	System	50002	Yes
Device Error	System	50003	Yes
Inactivity Timeout	System	50004	Yes
Queue Change	System	50020	Yes
Device Conflict	System	50030	Yes

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

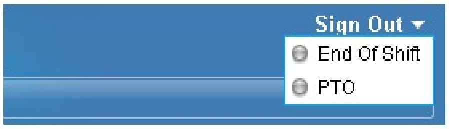
Field	Explanation
Reason Label	The label for the Sign Out reason code. The label has a maximum length of 40 characters and should be unique for each Sign Out reason code. Both alphanumeric and special characters are supported.
Type	The type of reason code (System or Custom). The column is default and can be sorted to display both System reason codes and Custom reason codes.
Reason Code	A code for the Sign Out reason. The code can be any value between 1 and 65535 and must be unique.
Global?	Yes/No. Indicates if the reason code is available globally to all agents (Yes) or to specific teams of agents (No).

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

- **New:** Add a new Sign Out reason code
- **Edit:** Edit an existing Sign Out reason code
- **Delete:** Delete a Sign Out reason code
- **Refresh:** Reload the list of Sign Out reason codes from the server

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

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



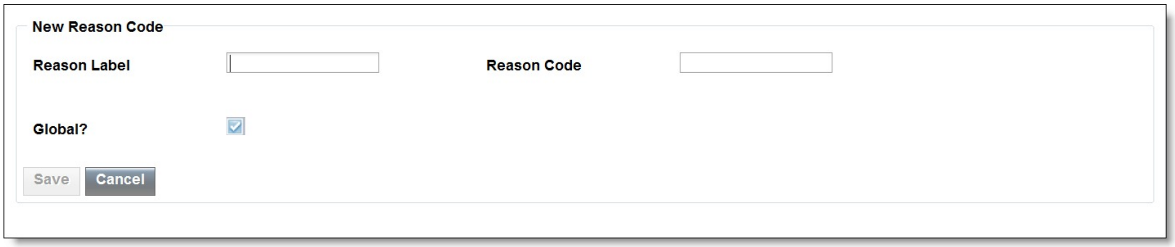
Add Sign Out Reason Code

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

Procedure

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

The New Reason Code area appears.



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

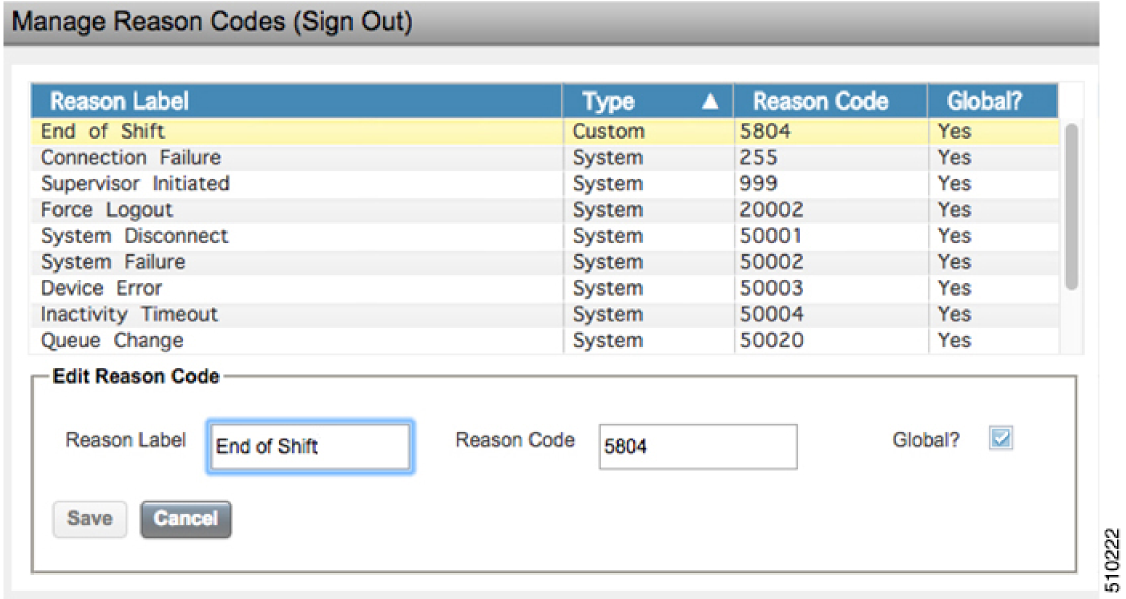
Perform the following procedure to edit the label or code for an existing Sign Out reason code.

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.



Manage Reason Codes (Sign Out)

Reason Label	Type ▲	Reason Code	Global?
End of Shift	Custom	5804	Yes
Connection Failure	System	255	Yes
Supervisor Initiated	System	999	Yes
Force Logout	System	20002	Yes
System Disconnect	System	50001	Yes
System Failure	System	50002	Yes
Device Error	System	50003	Yes
Inactivity Timeout	System	50004	Yes
Queue Change	System	50020	Yes

Edit Reason Code

Reason Label: End of Shift

Reason Code: 5804

Global? ☑

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.

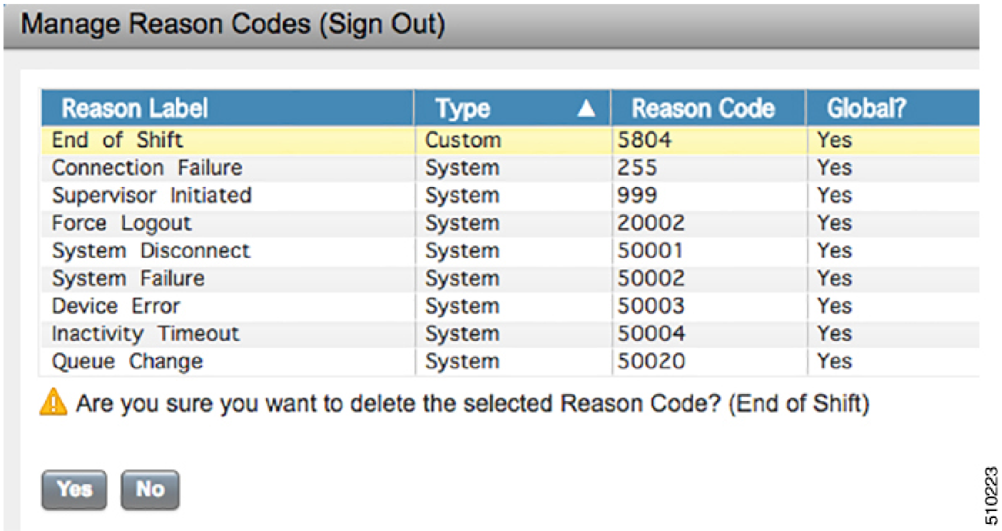
Perform the following procedure to delete a Sign Out reason code.

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.



Manage Reason Codes (Sign Out)

Reason Label	Type ▲	Reason Code	Global?
End of Shift	Custom	5804	Yes
Connection Failure	System	255	Yes
Supervisor Initiated	System	999	Yes
Force Logout	System	20002	Yes
System Disconnect	System	50001	Yes
System Failure	System	50002	Yes
Device Error	System	50003	Yes
Inactivity Timeout	System	50004	Yes
Queue Change	System	50020	Yes

⚠ Are you sure you want to delete the selected Reason Code? (End of Shift)

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:

System Reason Code	Reason Label	Reason Label Description
32767	Not Ready - Call Not Answered	Agent state changed because the agent did not answer the call.
32762	Ready - Offhook Not Ready - Offhook	The system issues this reason code in the following scenarios: • When the agent goes off the hook to place a call. If the agent remembers to do this task the corresponding agent-triggered reason code is displayed. If the agent does not remember to do this task, the system issues this reason code.

		• When the agent is in Ready state and a call is placed from the ACD (Automatic Call Distribution) line, the system issues this reason code.
50001	Logged Out - System Disconnect	The CTI OS client disconnected, logging the agent out.
50002	Logged Out - System Failure	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.
50002	Not Ready - Connection Failure	The system issues this reason code when the agent is forcibly logged out in certain cases.
50003	Logged Out - Device Error	Agent was logged out because the Unified CM reported the device out of service.
50004	Logged Out - Inactivity Timeout	Agent was logged out due to agent inactivity as configured in agent desk settings.
50005	Not Ready - Non ACD Busy	For a Unified CCE agent deployment, where the Agent Phone Line Control is enabled in the peripheral and the Non ACD Line Impact is configured to impact agent state, the agent is set to Not Ready while talking on a call on the Non ACD line with this reason code.
50010	Not Ready - Call Overlap	Agent was set to Not Ready state because the agent was routed two consecutive calls that did not arrive.
50020	Logged Out - Queue Change	Agent was logged out when the agent's skill group dynamically changed on the Administration & Data Server.
50030	Logged Out - Device Conflict	If an agent is logged in to a dynamic device target that is using the same dialed number (DN) as the PG static device target, the agent is logged out.
50040	Logged Out - Mobile Agent Call Fail	Mobile agent was logged out because the call failed.
50041	Not Ready - Mobile Call Not Answered	Mobile agent state changed to Not Ready because the call fails when the mobile agent's phone line rings busy.
50042	Logged Out - Mobile Agent Disconnect	Mobile agent was logged out because the phone line disconnected while using nailed connection mode.
65535	Not Ready - System Reinitialized	Agent reinitialized (used if peripheral restarts).
65534	Not Ready - System Reset	PG reset the agent, normally due to a PG failure.
65533	Not Ready - Extension Modified	An administrator modified the agent's extension while the agent was logged in.

20001	Not Ready - Starting Force Logout	Places the agent in the Not Ready state first before forcefully logging them off.
20002	Logged Out - Force Logout	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).
20003	Not Ready - Agent Logout Request	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.
999	Not Ready - Supervisor Initiated	The system issues this reason code when the agent's state is forcibly changed to Not Ready by the Supervisor.
999	Logged Out - Supervisor Initiated	The system issues this reason code when the agent's state is forcibly changed to Logout by the Supervisor.
255	Logged Out - Connection Failure	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.

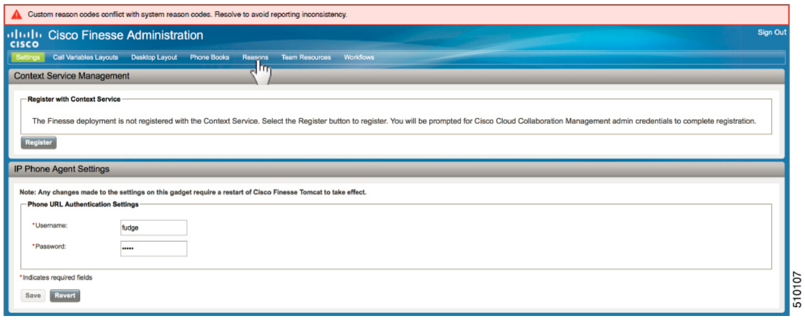
Manage Reason Code Conflicts During Upgrade

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.



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

Context Service Management

Register with Context Service

The Finesse deployment is not registered with the Context Service. Select the Register button to register. You will be prompted for Cisco Cloud Collaboration Management admin credentials to complete registration.

IP Phone Agent Settings

Note: Any changes made to the settings on this gadget require a restart of Cisco Finesse Tomcat to take effect.

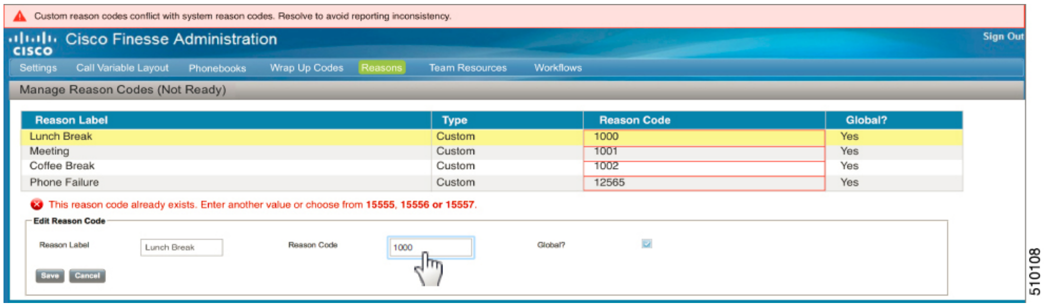
Phone URL Authentication Settings

*Username: fudge

*Password: •••••

*Indicates required fields

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).



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

Manage Reason Codes (Not Ready)

Reason Label	Type	Reason Code	Global?
Lunch Break	Custom	1000	Yes
Meeting	Custom	1001	Yes
Coffee Break	Custom	1002	Yes
Phone Failure	Custom	12565	Yes

This reason code already exists. Enter another value or choose from **15555**, **15556 or 15557**.

Edit Reason Code

Reason Label: Lunch Break

Reason Code: 1000

Global? ☑

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:

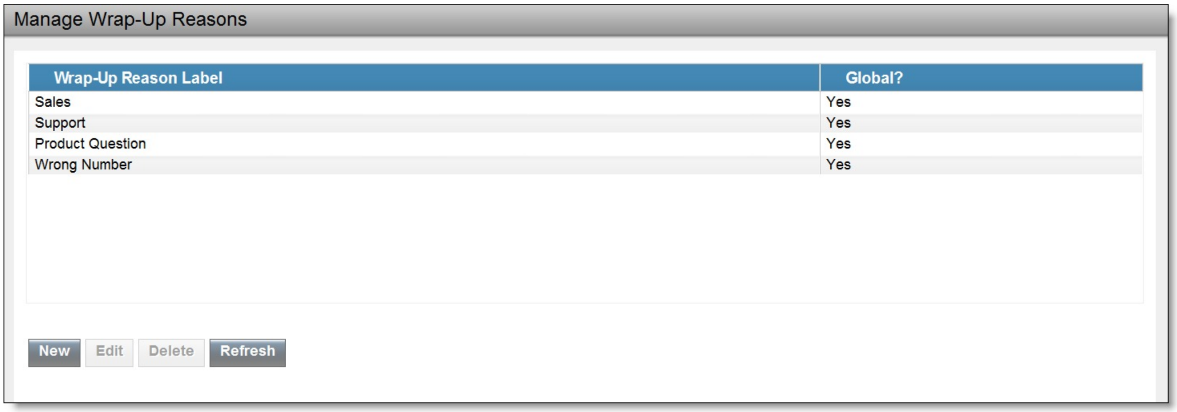
- Set the Work mode on incoming attribute to either *Optional* or *Required*.

- 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.



Manage Wrap-Up Reasons

Wrap-Up Reason Label	Global?
Sales	Yes
Support	Yes
Product Question	Yes
Wrong Number	Yes

345934

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

Field	Explanation
Reason Label	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.
Global?	Yes/No. Indicates if the Wrap-Up reason is available globally to all agents (Yes) or to specific teams of agents (No).

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.

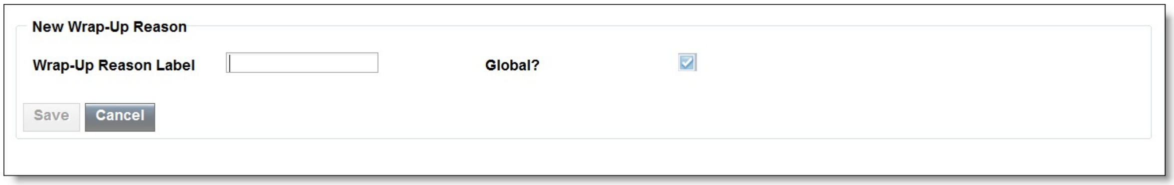
Add Wrap-Up Reason

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.



New Wrap-Up Reason

Wrap-Up Reason Label □ Global? ☑

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

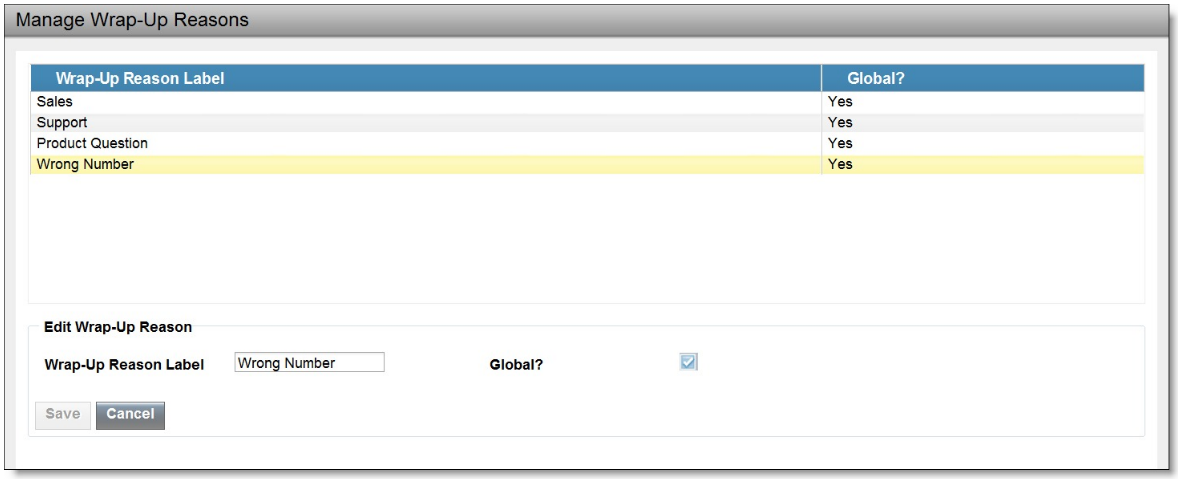
Perform the following procedure to edit an existing Wrap-Up reason.

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.



Manage Wrap-Up Reasons

Wrap-Up Reason Label	Global?
Sales	Yes
Support	Yes
Product Question	Yes
Wrong Number	Yes

Edit Wrap-Up Reason

Wrap-Up Reason Label: Wrong Number

Global? ☑

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

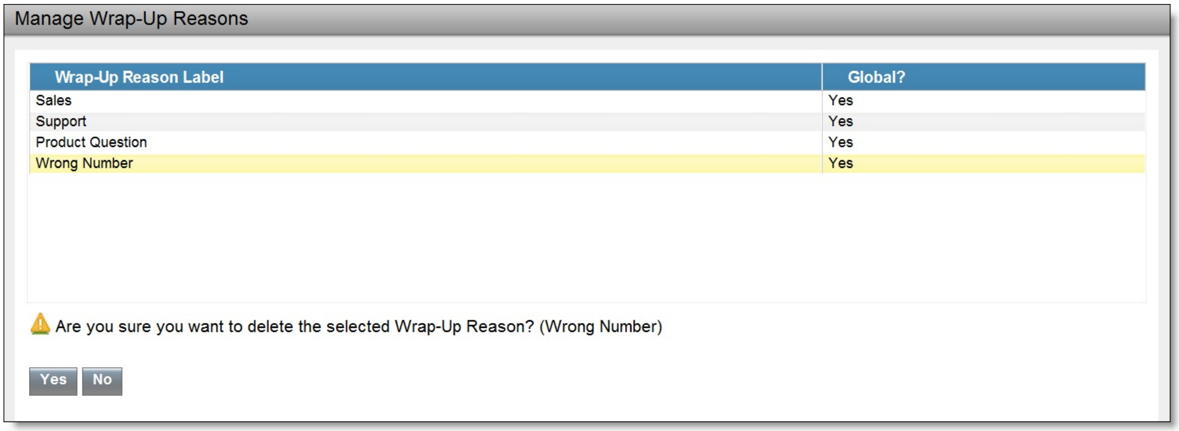
Perform the following procedure to delete a Wrap-Up reason.

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.



Manage Wrap-Up Reasons

Wrap-Up Reason Label	Global?
Sales	Yes
Support	Yes
Product Question	Yes
Wrong Number	Yes

Are you sure you want to delete the selected Wrap-Up Reason? (Wrong Number)

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

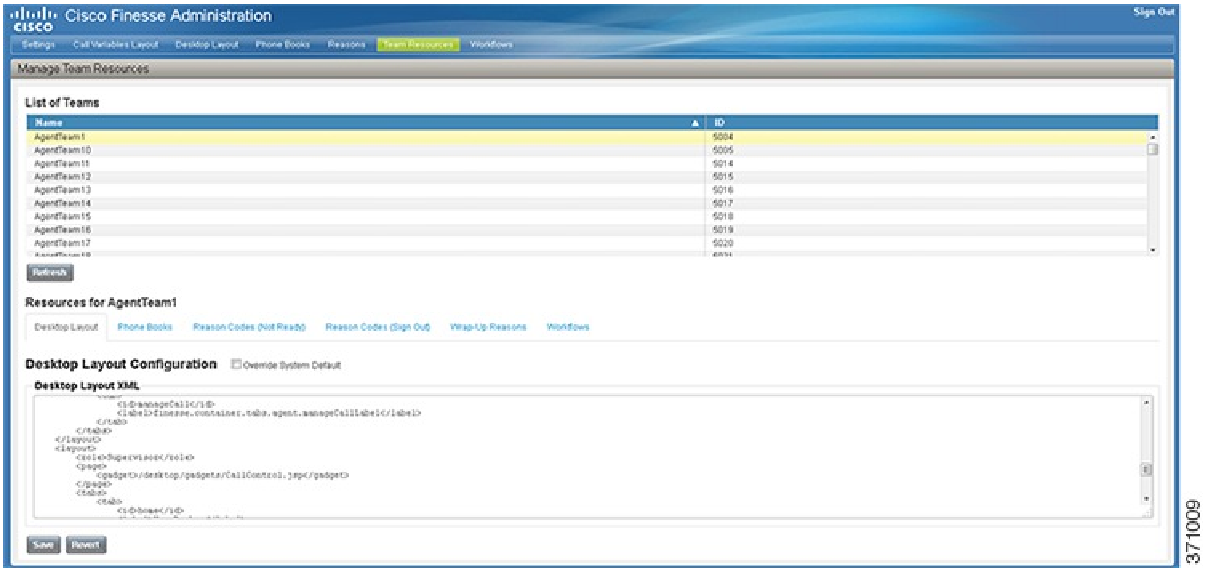
CHAPTER 7

Manage Team Resources

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

Team Resources

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.



List of Teams

Name	ID
AgentTeam1	5004
AgentTeam10	5005
AgentTeam11	5014
AgentTeam12	5015
AgentTeam13	5016
AgentTeam14	5017
AgentTeam15	5018
AgentTeam16	5019
AgentTeam17	5020

Resources for AgentTeam1

Desktop Layout Configuration ☐ Override System Default

Desktop Layout XML

```
                <id>manageCall</id>
                <label>finesse.container.tabs.agent.manageCallLabel</label>
            </tab>
        </tabs>
    </layout>
    <layout>
        <role>Supervisor</role>
        <page>
            <gadget>/desktop/gadgets/CallControl.jsp</gadget>
        </page>
        <tabs>
            <tab>
                <id>home</id>
```

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.

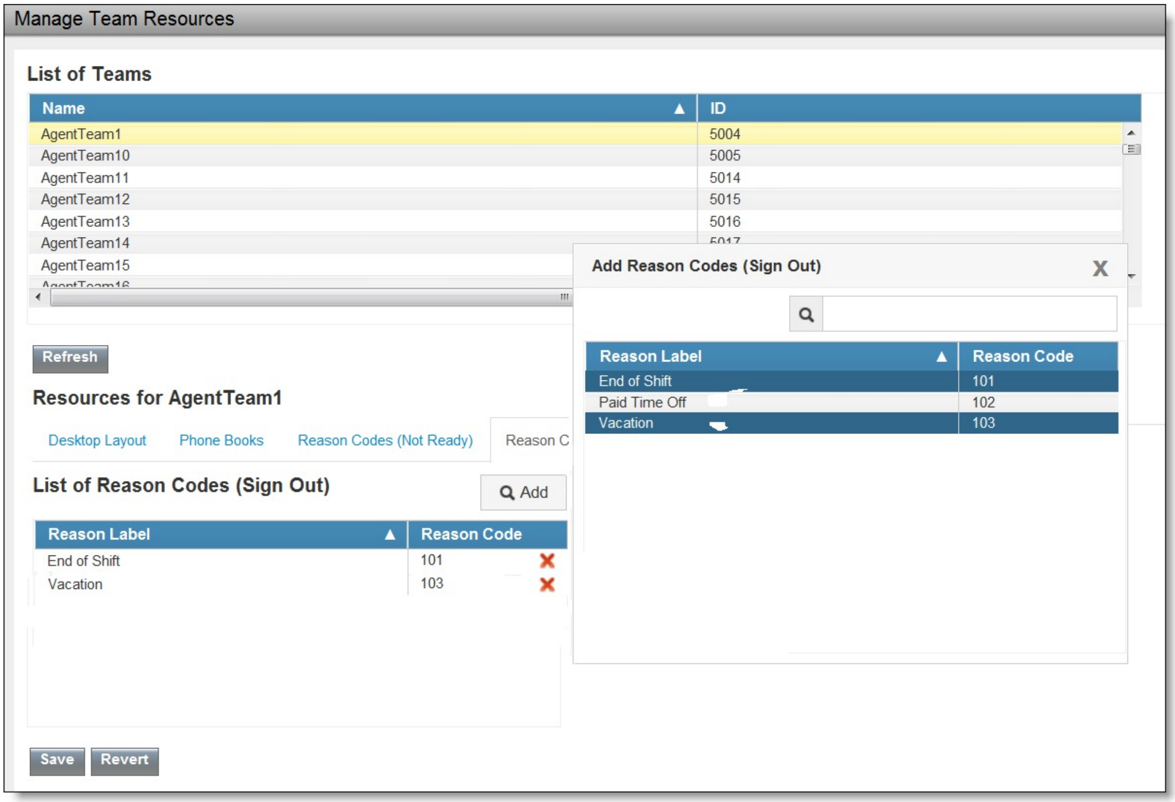
Tabs for each available resource appear.

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.



List of Teams

Name ▲	ID
AgentTeam1	5004
AgentTeam10	5005
AgentTeam11	5014
AgentTeam12	5015
AgentTeam13	5016
AgentTeam14	5017
AgentTeam15	
AgentTeam16	

Resources for AgentTeam1

List of Reason Codes (Sign Out)

Reason Label ▲	Reason Code
End of Shift	101
Vacation	103

Add Reason Codes (Sign Out)

Reason Label ▲	Reason Code
End of Shift	101
Paid Time Off	102
Vacation	103

346069

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.

Note If you clear the Override System Default check box, any changes you made to the XML are lost and the XML in the editing pane reverts to the default desktop layout XML.

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**.

CHAPTER 8

Manage Workflows

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

Workflows and Workflow Actions

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:

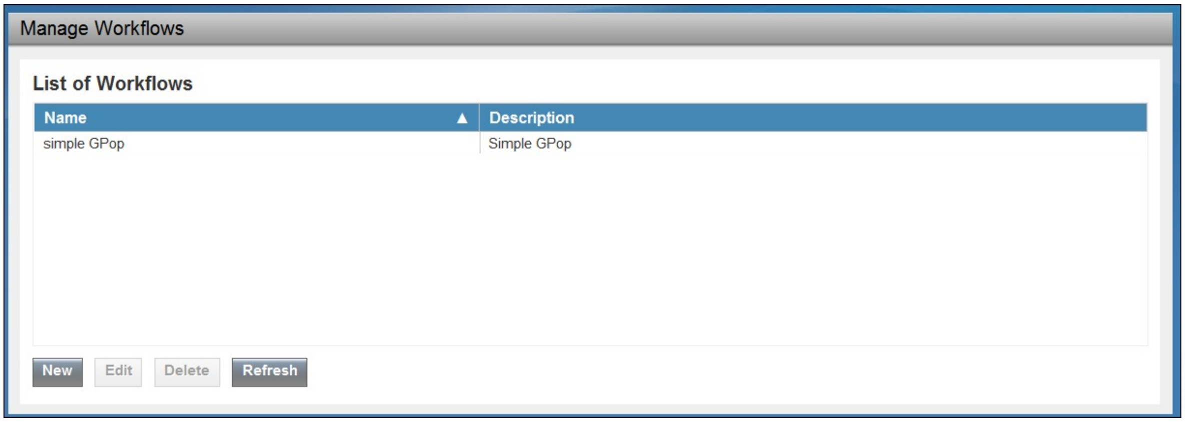
- 100 workflows per Finesse system
- 100 actions per Finesse system
- 20 workflows per team
- 5 conditions per workflow
- 5 actions per workflow
- 5 variables per action

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.

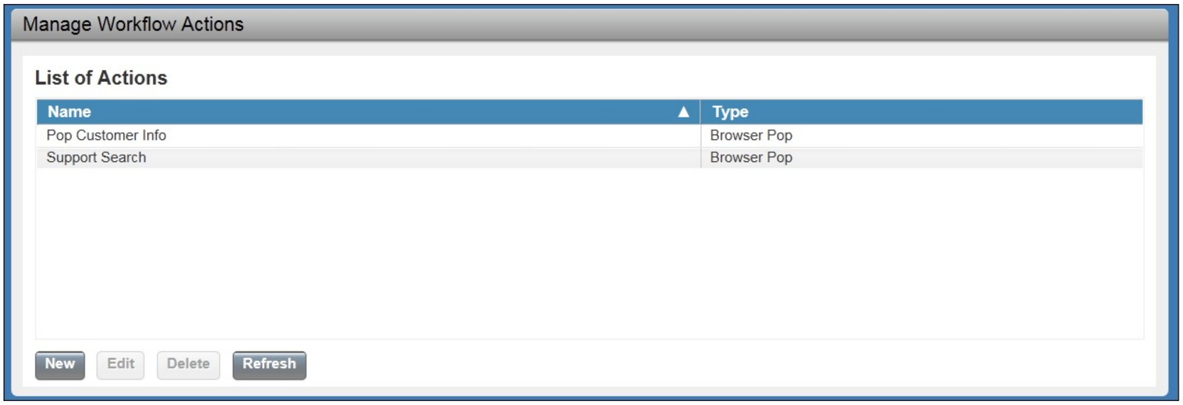

Manage Workflows

List of Workflows

Name ▲	Description
simple GPop	Simple GPop

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

Field	Explanation
Name	The name of the workflow. The name must be unique and can be a maximum length of 40 characters.
Description	The description of the workflow. The description can be a maximum length of 128 characters.


Manage Workflow Actions

List of Actions

Name ▲	Type
Pop Customer Info	Browser Pop
Support Search	Browser Pop

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

Field	Explanation
Name	The name of the workflow action. The name must be unique and can be a maximum length of 64 characters.
Type	The type of workflow. Possible values are Browser Pop, HTTP Request.

Actions on the Manage Workflows and Manage Workflow Actions gadgets:

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

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

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

- When a call arrives
- When a call is answered

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

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

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

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

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

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

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

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

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

You can filter trigger events by the value of the data that comes in the event. You can configure a workflow to execute if any conditions are met or if all conditions are met.

Individual conditions consist of the following:

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

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

Workflows run only for agents and supervisors who are Finesse users. The Workflow Engine is a JavaScript library that runs client-side on a per-user basis within the 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.

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

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

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

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

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

The 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.

Workflow Trigger	Direct Preview Outbound Call	Preview Outbound Call	Progressive/Predictive Outbound Call
While previewing a call	When the agent previews the call (before accepting or rejecting it)	When the agent previews the call (before accepting or rejecting it)	Does not trigger
When a call arrives	Does not trigger	When the agent accepts the call	When the call arrives on the agent desktop
When a call is answered	When the customer answers the call and during failover	When the customer answers the call and during failover	When the customer answers the call
When a call is made	When the customer call is initiated	When the customer call is initiated	When the customer call is initiated, and during failover
When a call ends	When the customer call ends	When the customer call ends	When the customer call ends

Add Browser Pop Workflow Action

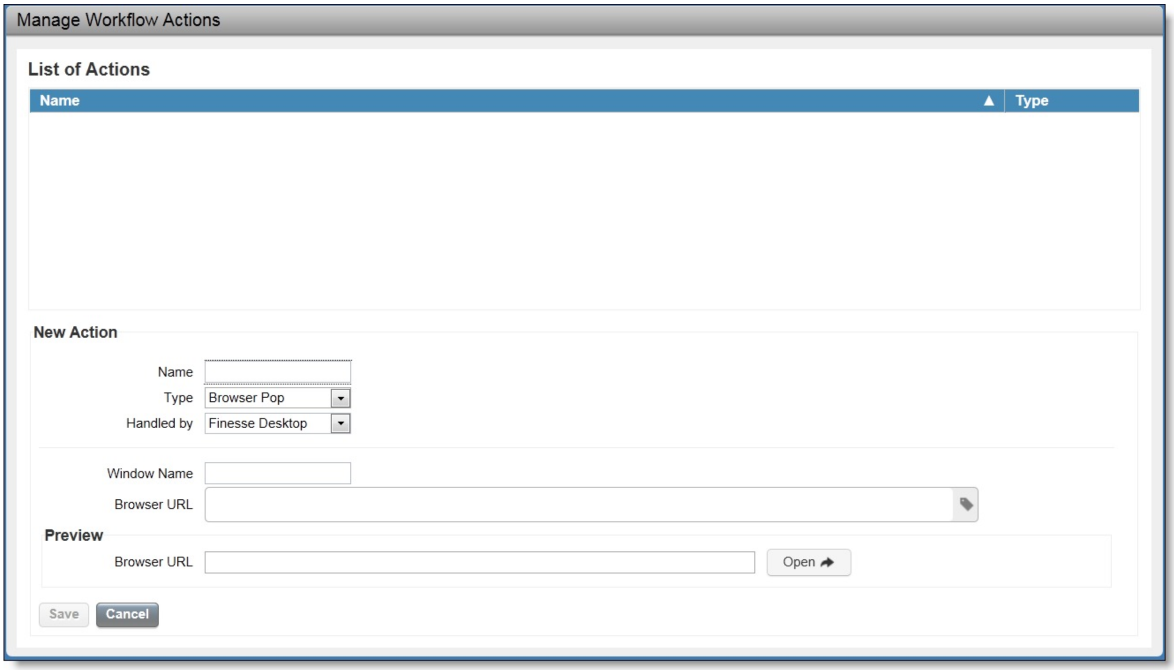
The Browser Pop workflow action opens a browser window or tab on the user's desktop when workflow conditions are met.

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**.

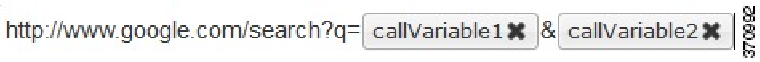
Step 4 From the Handled By drop-down list, select what will execute the action, either the Finesse Desktop or Other (a third-party gadget).

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**.

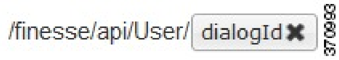
Step 7 In the Content Type box, enter the content type.

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**.

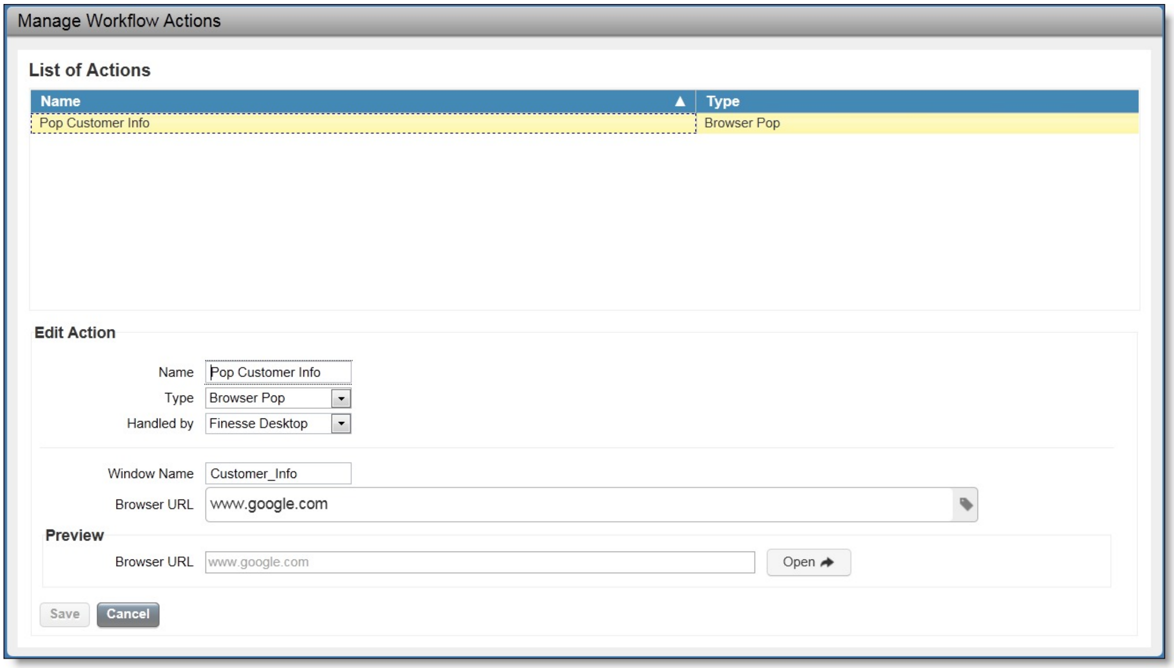
Edit Workflow Action

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.



Manage Workflow Actions

List of Actions

Name	Type
Pop Customer Info	Browser Pop

Edit Action

Name: Pop Customer Info
Type: Browser Pop
Handled by: Finesse Desktop
Window Name: Customer_Info
Browser URL: www.google.com

Preview

Browser URL: www.google.com

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.

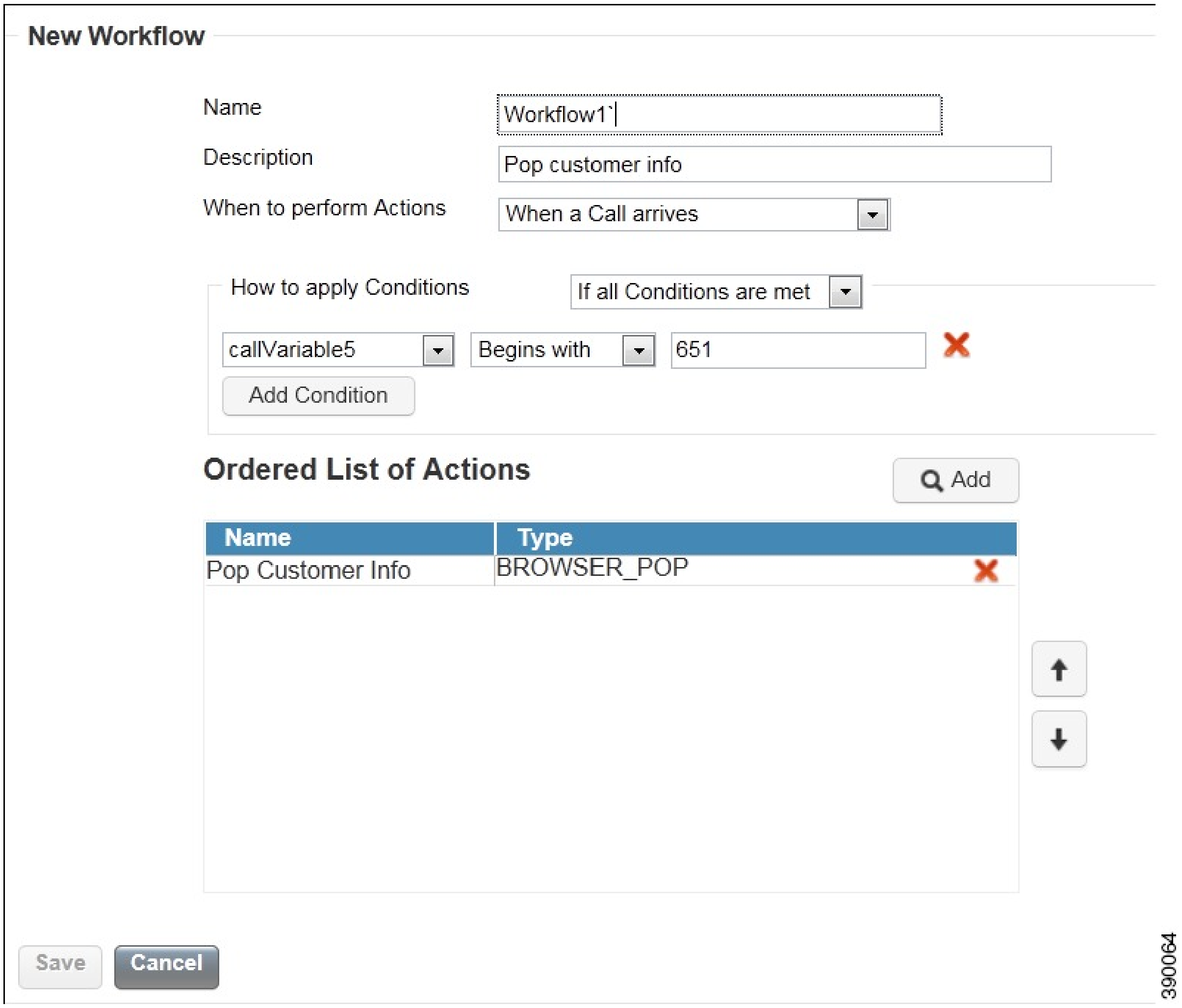
Step 3 Click **Yes** to confirm the deletion of the selected action.

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

Name	Type
Pop Customer Info	BROWSER_POP

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

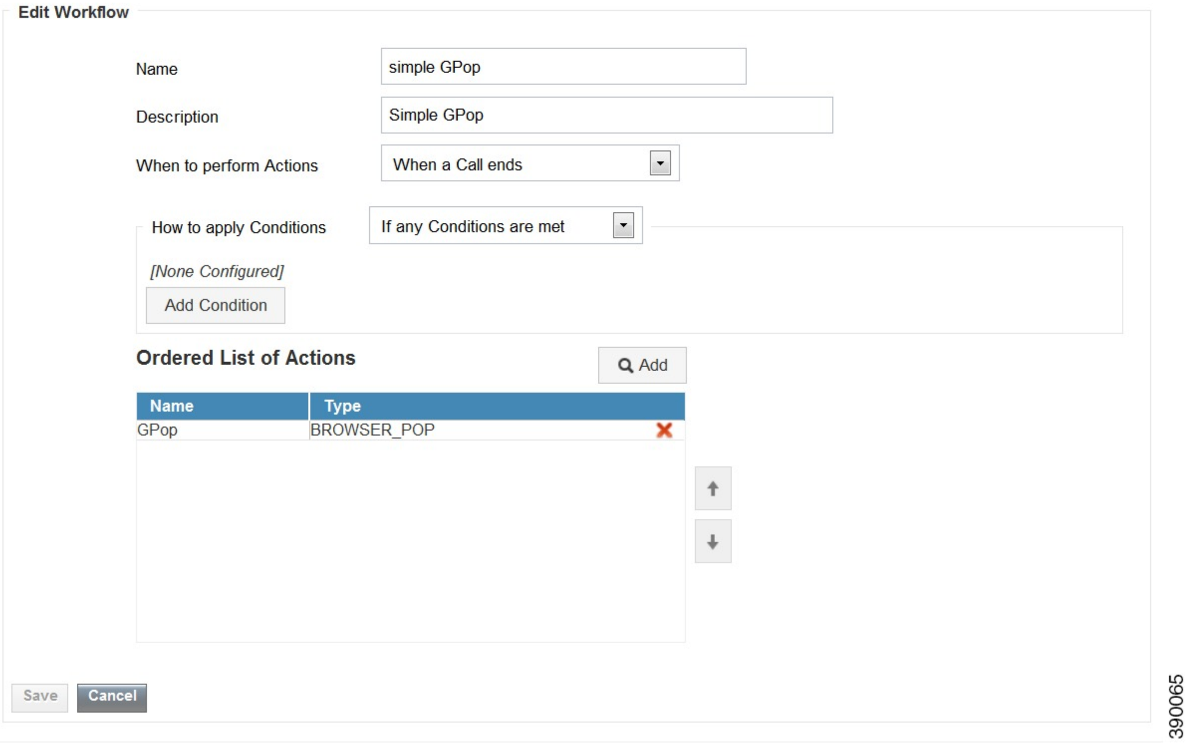
Edit Workflow

Procedure

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

Step 2 Click **Edit**.

The Edit Workflow area appears.



Edit Workflow

Name: simple GPop

Description: Simple GPop

When to perform Actions: When a Call ends

How to apply Conditions: If any Conditions are met

[None Configured]

Ordered List of Actions

Name	Type
GPop	BROWSER_POP

Step 3 Edit the fields that you want to change.

Step 4 Click **Save**.

Delete Workflow

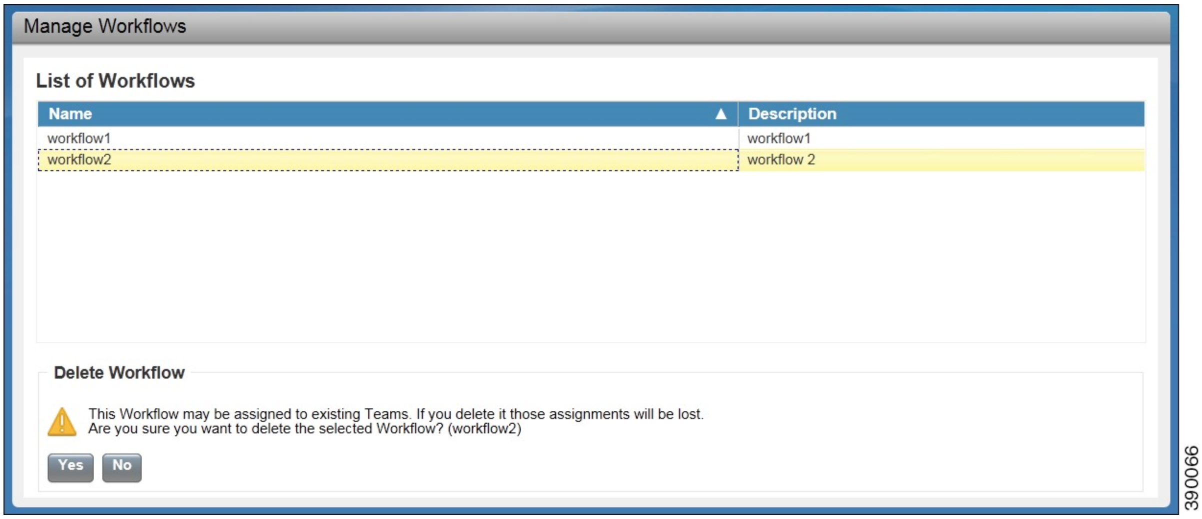
Procedure

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.



Manage Workflows

List of Workflows

Name ▲	Description
workflow1	workflow1
workflow2	workflow 2

Delete Workflow

This Workflow may be assigned to existing Teams. If you delete it those assignments will be lost.
Are you sure you want to delete the selected Workflow? (workflow2)

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

CHAPTER 9

Manage Security

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**.

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 in to the platform window with the following username and password:

pwrecovery/pwreset

The following messages appear:

Welcome to Platform password reset.

Admin and Security password reset are possible.

Press any key when ready.

Step 2 Press any key to continue.

The following messages appear:

If you have a CD or DVD in the disk drive, remove it now.

Press any key to continue.

Step 3 If there is a disk in the disk drive, remove it. When you are ready, press any key to continue.

The system checks to ensure that you have removed the disk from the drive.

The following message appears:

Insert a valid CD or DVD into the disk drive.

Step 4 Connect the CD/DVD drive and point it to the ISO image.

The system checks to ensure you have inserted the disk.

After the system verifies that you have inserted a disk, you are prompted to choose one of the following options:

Enter 'a' for admin password reset.

Enter 's' for security password reset.

Enter 'q' for quit.

Step 5 Select the appropriate option and provide the new password.

The system resets the password.

CHAPTER 10

Manage Finesse IP Phone Agent

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.

Example Set Up	Prepopulated in Unified CM Administration (by Administrator)	Prepopulated in Self Care Portal (by Agent)	Entered at Sign-In (by Agent)
Administrator populates the extension only	extension	-	id password
Administrator populates the ID and extension	id extension	-	password
Agents enter password only using Self Care Portal	id extension	password	-

Example Set Up	Prepopulated in Unified CM Administration (by Administrator)	Prepopulated in Self Care Portal (by Agent)	Entered at Sign-In (by Agent)
Agents enter all credentials using Self Care Portal	-	id extension password	-
Agents enter ID and extension only using Self Care Portal	-	id extension	password

Finesse IP Phone Service Subscription Options

To set up access to Finesse on agent IP phones in Cisco Unified Communications Manager, you must create the Finesse IP Phone service to which the phones can subscribe. To set up the 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.

Finesse IPPA Configuration Procedures	Enterprise Subscription	Manual Subscription	
		Administrator Manually Subscribes the Phones	Agents Manually Subscribe Their Phones Using the Self Care Portal
Set Up Application User, Web Access, and HTTPS Server Parameters, on page 102	Required	Required	Required
Configure Finesse IP Phone Service in Unified CM, on page 103	Required	Required	Required
Add Service Parameters for One Button Sign In, on page 105	Not applicable	Required only with One Button Sign In	Required only with One Button Sign In
Subscribe Agent Phones to Manual Subscription Service, on page 107	Not applicable	Required	Optional. Allows the administrator to enter agent credentials for One Button Sign In.

Finesse IPPA Configuration Procedures	**Enterprise Subscription**	**Manual Subscription**	
		Administrator Manually Subscribes the Phones	**Agents Manually Subscribe Their Phones Using the Self Care Portal**
Set Up Agent Access to the Self Care Portal, on page 108	Not applicable	Optional. Allows agents to enter their own credentials for One Button Sign In.	Required

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 Finesse server.
f) After replication is complete, restart Cisco Finesse Tomcat on the secondary Finesse 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 Finesse 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 Finesse server.

Step 6 Ensure that the **Service Category** is set to **XML Service**, and the **Service Type** is set to **Standard IP Phone Service**.

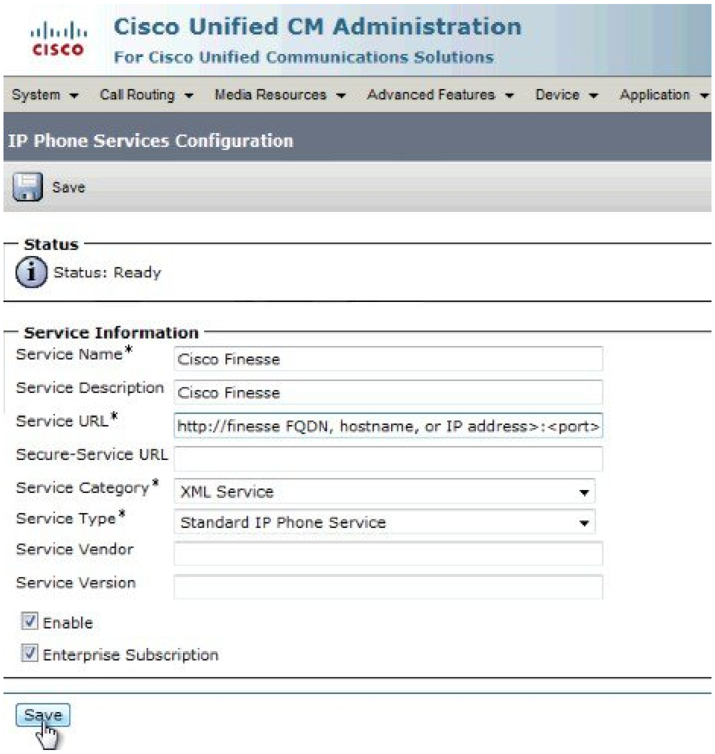
Step 7 Check the **Enable** check box.

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

  
  Cisco
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System
Call Routing
Media Resources
Advanced Features
Device
Application
IP Phone Services Configuration
Save
Save

  Status

  Status: Ready

  Service Information

  Service Name* Cisco Finesse

  Service Description Cisco Finesse

  Service URL* http://finesse FQDN, hostname, or IP address>:<port>

  Secure-Service URL

  Service Category* XML Service

  Service Type* Standard IP Phone Service

  Service Vendor

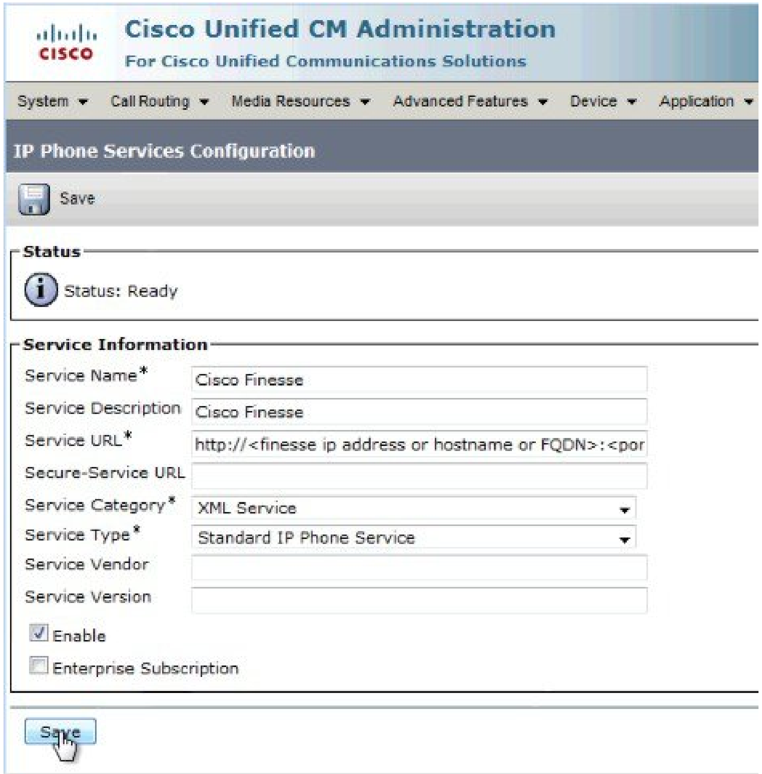
  Service Version

  ☑ Enable

  ☑ Enterprise Subscription

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

Figure 2: Finesse Service Configuration Without Enterprise Subscription


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
System
Call Routing
Media Resources
Advanced Features
Device
Application
IP Phone Services Configuration
Save

Status

Status: Ready

Service Information

Service Name* Cisco Finesse

Service Description Cisco Finesse

Service URL* http://<finesse ip address or hostname or FQDN>:<por

Secure-Service URL

Service Category* XML Service

Service Type* Standard IP Phone Service

Service Vendor

Service Version

☑ Enable

☐ Enterprise Subscription

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**).

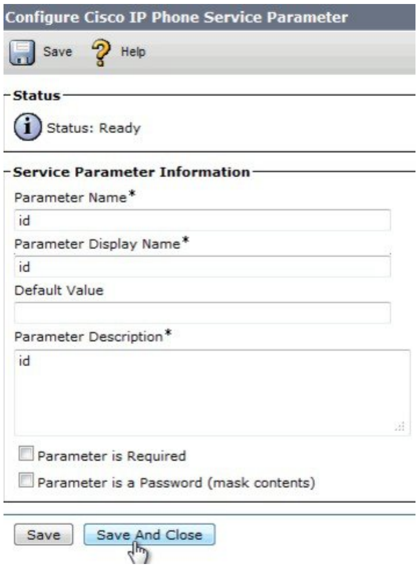
Step 2 Click **New** to the right of the Parameters box.

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.

Field	Description
Parameter Name	Enter one of the following parameter names as follows: • Id • extension • password The values entered are the exact query string parameters used for the subscription URL.
Parameter Display Name	Enter a descriptive parameter name; for example, id, extension, and password.
Default Value	Leave the default value blank for all parameters.
Parameter Description	Enter a description of the parameter. The user can access this text when they subscribe to the service.
Parameter is Required	If the administrator will prepopulate the parameter in Unified CM Administration, check the **Parameter is Required** check box. However, if the agent will prepopulate the parameter in the Self Care Portal, two options are available: • If the agents will prepopulate all defined parameters, check the **Parameter is Required** check box for each parameter. • 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.
Parameter is a Password (mask contents)	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.

When you save the last parameter, click **Save and Close**.



Configure Cisco IP Phone Service Parameter

Status

Status: Ready

Service Parameter Information

Parameter Name* id

Parameter Display Name* id

Default Value

Parameter Description* id

□ Parameter is Required

□ Parameter is a Password (mask contents)

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

Step 1 From the Unified CM Administration page, select **System** > **Enterprise Parameters**.

Step 2 Under the Self Care Portal Parameters, in the **Self Care Portal Default Server** field, select the IP address of the Unified CM Publisher server from the drop-down list and click **Save**.

Step 3 Select **User Management** > **End User**.

Step 4 Select the user that you want to set up with access to the User Care Portal.

Step 5 Under Permissions Information, click **Add to Access Control Group**.

Step 6 From the list of Access Control groups displayed, check **Standard CCM End Users** and click **Add Selected**.

Step 7 Click **Save**.

With access enabled to the Self Care Portal, agents can sign 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

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

Note If the third-party gadget hosted in Cisco Finesse is sending a REST request to the web server via Shindig, using the SHA256 certificate, the maximum key length cannot exceed 2048.

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

Upload Third-Party Gadgets

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

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

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

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

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:

```
<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>
```

Note 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 Finesse desktop, clear your browser cache.

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

admin:utils service restart Cisco Finesse Tomcat

Third-Party Gadget Limitations

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

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

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.
3. Start the Cisco Finesse Notification Service.
4. Start the Cisco Finesse Tomcat service.

View, Start, or Stop Services

Procedure

Step 1 Sign in to the CLI using the credentials for the Administrator User account.

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

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

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

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

Example:

For example, to start Cisco Finesse Tomcat, enter the command **utils service start Cisco Finesse Tomcat**.

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

Example:

For example, to stop Cisco Finesse Tomcat, enter the command **utils service stop Cisco Finesse Tomcat**.

Log Collection

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

To obtain logs:

- Install log: **file get install desktop-install.log**

  Use this command to see the installation log after the system is installed.

  This log is written to the SFTP server and stored as a text file written to this path: *<IP Address>\<date time stamp>\install\desktop-install.log*

- Desktop logs: **file get activelog desktop recurs compress**

Use this command to obtain logs for the Finesse web applications. This command uploads a zip file that contains the following directories:

- **webservices:** contains the logs for the Finesse backend that serves the Finesse REST APIs. The maximum size of an uncompressed desktop log file is 100 MB. The maximum size of this directory is approximately 4.5 GB. After a log file reaches 100 MB, that file is compressed and a new log file is generated. Output to the last compressed desktop log file wraps to the log file created next. The log file wrap-up duration can vary, based on the number of users on the system. Timestamps are placed in the file name of each desktop log.
- **desktop:** contains logs from the Finesse agent desktop gadget container that holds the Finesse desktop gadgets. Any container-level errors with Finesse agent desktop will appear in these log files.
- **admin:** contains logs from the Finesse administration gadget container that holds the administration gadgets. Any container-level errors with the Finesse administration console appear in these log files.
  - **audit-log:** Audit logs contain all admin operations (including Finesse admin UI and REST client operations). 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 Finesse 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 Finesse and openfire.

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

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

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

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

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

  Use this command to obtain logs generated by the platform service manager that manages the starting and stopping of the Finesse services.

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

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

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

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

- Install log: **file get install install.log**

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

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

Collect Logs Using Cisco Unified Real-Time Monitoring Tool

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

Note Finesse supports RTMT only for log collection. Other RTMT features are not supported.

Before you begin

Download and install RTMT on a client computer from the following URL: `https://FQDN:8443/plugins/CcmServRtmtPlugin.exe`, where FQDN is the Fully Qualified Domain Name of the Finesse server.

Procedure

Step 1 Log in to Unified RTMT using Finesse administrator credentials.

Step 2 In the tree hierarchy, select **Trace & Log Central** 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 Finesse nodes for which you want to collect logs, and complete the wizard.

For more information, see *Cisco Unified Real-Time Monitoring Tool Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Syslog Support for Critical Log Messages

Cisco Finesse generates syslogs for critical log messages. Use the following procedure to view the logs using Unified RTMT.

Before you begin

Download and install RTMT on a client computer from the following URL: `https://FQDN:8443/plugins/CcmServRtmtPlugin.exe`, where FQDN is the Fully Qualified Domain Name of the Finesse server.

Procedure

Step 1 Log in to Unified RTMT using Finesse 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.

For more information, see *Cisco Unified Real-Time Monitoring Tool Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Note System log messages generated by Cisco Finesse are also available under **SysLog Viewer** > **System Logs** > **messages**.

The following are the different types of messages and corresponding descriptions that are captured in the **SysLog Viewer** > **System Logs** > **messages**.

- CTI_SOCKET_ERROR

  System has encountered an error connecting to the CTI server.

- CTI_CONNECTION_LOST

  System has lost contact with the CTI server.

- CTI_OPEN_FAILURE

  CTI Server rejected open request.

- CTI_CONNECTION_RETRIES_EXCEEDED

  System has failed to connect to CTI server in the allowed number of retries.

- CTI_CONNECTION_ESTABLISHED

  System has successfully connected to CTI server.

- SUBSYS_INIT_ERROR

  Error initializing subsystem.

- 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

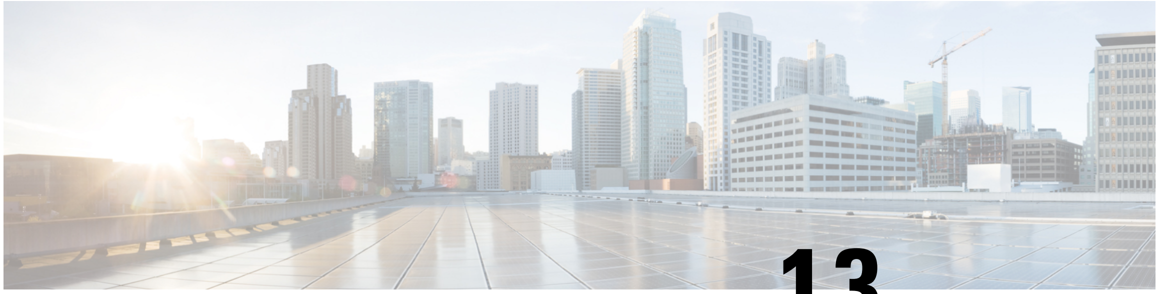
Run the following command to enable, disable, create, and check the status of a remote access account: **utils remote_account**

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

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.

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

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

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

Related Topics

Contact Center Enterprise CTI Server Settings, on 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.
- Finesse can connect to the secondary AWDB host.
- The Distributor service is running on the secondary AWDB host.

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

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

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

If Finesse 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 Finesse desktop receive an “Invalid user ID or password” error message.
- Administrators cannot update or retrieve settings in the Finesse administration console.

- Users who are already signed in to Finesse receive an "Operation timed out" error message.
- Users who make API requests receive an 401 "Unauthorized" HTTP error message.

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

Related Topics

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

Finesse Client Failover

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

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

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

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

- The Finesse desktop receives a SystemInfo event that the current server is OUT_OF_SERVICE.
- The BOSH connection is disconnected.
- The "finesse" XMPP user presence changes to unavailable.

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

1. Poll SystemInfo 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 Finesse Tomcat Service goes down.
- The Finesse Webapp Service goes down.

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

Desktop Behavior

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

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

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

Scenario	Desktop Behavior	Server Action	Results
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.	**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.
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.	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 Finesse setup (primary and secondary Finesse servers), if the server that an agent is connected to goes out of service, the Finesse IP Phone Agent (IPPA) displays a notification that the server is unavailable. Finesse IPPA continues to check whether the current Finesse server recovers its state, and notifies the agent if it reconnects.

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

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

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

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

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

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

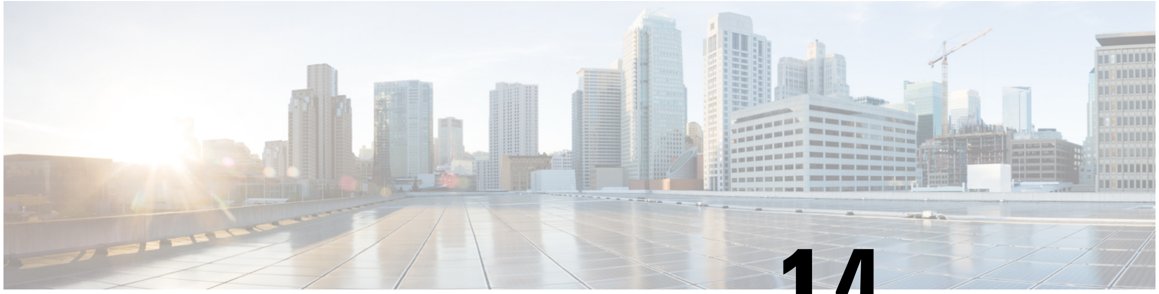
  Finesse IPPA tries every 5 seconds to reconnect with the XMPP server. After three attempts, if the XMPP connection cannot be reestablished, Finesse IPPA displays a server unavailable message to the agent.

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

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

Finesse IPPA failover can occur for the following reasons:

- The Finesse Webapp Service goes down.
- The Cisco Finesse Notification Service goes down.
- If Finesse takes longer to failover to the alternate CTI server than it takes for Finesse IPPA to detect a server failure, then Finesse IPPA declares the Finesse server out of service.



CHAPTER 14

Backup and Restore

Backup and Restore

Cisco Finesse uses the backup and restore tools that are provided by the common Cisco Unified Communications platform services for complete data backup-and-restore capabilities. Cisco DRS allows you to perform regularly scheduled automatic or user-invoked data backups and to restore data if the system fails.

To access the Disaster Recovery System (DRS) application, direct your browser to the following URL: https://*FQDN*:8443/drf, where *FQDN* is the fully-qualified domain name of your Finesse server.

Note Cisco Finesse does not support One-Step Restore with the DRS application.

In the case of high availability (HA), Cisco DRS performs a cluster-level backup, which means that it collects backups for all servers to Cisco Finesse and archives the backup data to a remote SFTP server.

DRS backs up and restores its own settings, that is, backup device settings (saved in file `drfDevice.xml`) and schedule settings (saved in file `drfSchedule.xml`) as part of the platform component. Once a server is restored with these files, you do not need to reconfigure DRS backup device and schedule settings.

Note Cisco DRS uses the SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the publisher and subscriber nodes. Cisco DRS uses the IPSec certificates for its Public/Private Key encryption. If you delete the IPSec truststore (`hostname.pem`) file from the Certificate Management pages, then Cisco DRS will not work as expected. If you delete the IPSec-trust file manually, then you must ensure that you upload the IPSec certificate to the IPSec-trust. For more information about the certificate management, see, *Cisco Unified Communications Manager Security Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Important Considerations

Following are the important considerations when you perform the backup and restore procedures:

- Before you run a backup or a restore, make sure that both nodes in a cluster are running the same version of Cisco Finesse. If different nodes are running different versions, you will have a certificate mismatch and your backup or restore fails.
- Before you restore Cisco Finesse, make sure that the hostname, IP address, DNS configuration, version, and deployment type matches the hostname, IP address, DNS configuration, version, and deployment type of the backup file that you want to restore.
- Before you restore Cisco Finesse, ensure that the version that is installed on the server matches the version of the backup file that you want to restore. Cisco DRS supports restore only for matching versions of Cisco Finesse. For example, Cisco DRS does not allow you to restore from Version 8.5(1).1000-1 to Version 9.0(1).1000-1, or from Version 8.5(2).1000-1 to Version 9.0(1).1000-2.
- Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.
- After you use the recovery disk to bring a server with a corrupted file system into a bootable and semi-functional state, rebuild the server.

Note If you do not rebuild the server, you may notice missing directories, lost permissions, or corrupted soft links.

SFTP Requirements

To back up data to a remote device on the network, you must have an SFTP server that is configured and accessible from the Cisco Finesse node to run the backup. Cisco allows you to use any SFTP server products that have been certified with Cisco through the Interoperability Verification Testing (IVT) process. Cisco Developer Network (CDN) partners, such as GlobalSCAPE, certify their products with a specified version.

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (see http://sshwindows.sourceforge.net/)
- Cygwin (see http://www.cygwin.com/)
- Titan (see http://www.titanftp.com/)

Cisco does not support use of the SFTP product freeFTPD, because it has a 1-GB file-size limit.

Note

- 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.

Note 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.

Note 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

Step 1 Access the DRS application (https://*Finesse server IP*:8443/drf).

Step 2 Select **Backup** > **Backup Device**.

Step 3 Click **Add New** to add a new device or click the device name to edit settings of an existing backup device.

Step 4 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.

Step 5 Click **Save**.

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

Step 1 Access the DRS application (https://*Finesse server IP*:8443/drf).

Step 2 Select **Backup** > **Scheduler**.

Step 3 Click **Add New** to add a new schedule or click the schedule name to edit settings of an existing backup schedule.

Step 4 Enter the backup schedule name, select the backup device, and select feature as **`Finesse`**.

Step 5 Enter the backup date and frequency details as required. For more details on the field description, see the detailed online help provided with the DRS application.

Step 6 Click **Save**.

Step 7 Select a schedule from the **Schedule List** and then click **Enable Selected Schedules**.

Note
- If you plan to schedule a backup on a two-node deployment, ensure that both the servers in the cluster are running the same version of Cisco Finesse and are communicating in the network. Servers that are not communicating at the time of the scheduled backup will not be backed up.
- Do not schedule a backup to run while the **Update Database Statistics** task is running. By default, this task is set to run every Saturday at 3:00 a.m. and Shrink-repack on Sunday at 3:00 a.m..

Perform Manual Backup

Procedure

Step 1 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.

Caution The backup to the remote server to be completed within 20 hours otherwise the backup session times out and you will have to start the fresh backup.

Restore the Nodes in HA Setup with Rebuild

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

Caution Cisco Finesse data can only be retrieved from the backup file. The recent Finesse configuration data, which is not backed up, must be manually configured in the Cisco Finesse administration console after the restore.

Procedure

Step 1 Perform a fresh installation of Finesse. Make sure to install the same version of Finesse, using the same administrator credentials, network configuration, and security password that you used for the initial installation.

Step 2 Access the DRS application (https://*Finesse server IP*:8443/drf).

Step 3 From the Restore menu, select **Restore Wizard**.

Step 4 Select a backup device. Choose the location where your backup is stored.

Step 5 Select the backup file and feature as **`Finesse`**.

Step 6 When prompted to choose the nodes, either choose both nodes or choose each node to individually restore them.

Step 7 After the restore process is complete, restart the node.

Step 8 Run the following command on the primary 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.

Note

After the installation is complete, check that the dbreplication is functioning and allowing the data to propagate from the primary to the secondary node. However, if you need to restore third-party gadgets to the secondary node, you must either upload them again or run the restore process on the secondary node.

Always check the dbreplication status after any restore, using the CLI command **utils dbreplication runtimestate**.

CHAPTER 15

Supported Cisco Unified Communications OS Services

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

- utils csa enable
- utils csa disable
- utils csa status
- utils dbreplication clusterreset
- utils dbreplication dropadmindb
- utils dbreplication forcedatasyncsub
- utils dbreplication reset
- utils dbreplication runtimestate
- utils dbreplication setrepltimeout
- utils dbreplication stop
- utils diagnose test
- utils firewall ipv4
- utils iostat
- utils network arp
- utils network capture eth0
- utils network connectivity
- utils network host
- utils network ping
- utils network traceroute
- utils ntp
- utils ntp config
- utils ntp restart
- utils ntp server add
- utils ntp server delete
- utils ntp server list
- utils ntp status
- utils ntp start
- utils remote_account
- utils reset_application_ui_administrator_name
- utils reset_application_ui_administrator_password
- utils service
- utils system

- utils system boot
- utils system restart
- utils system upgrade
- utils vmtools status

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.

APPENDIX A

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

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.

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 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.

Note The configured timeout for browser notifications depends on the operating system and browser settings. The timeout value is honored in Chrome browser in Windows OS. However, the other supported browsers do not honor the configured notification timeout value consistently.

- **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.

Note 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.

Note 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**

Note Restart Cisco Finesse Tomcat and Cisco Finesse Notification Services for the changes to take effect.

Upgrade

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

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

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 3rdpartygadget 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).

APPENDIX B

Certificates for Live Data

Note 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

For secure Cisco Finesse, Cisco Unified Intelligence Center, and Live Data server-to-server communication, perform any of the following:

- Use the self-signed certificates provided with Live Data.

  Note When using self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

- Obtain and install a Certification Authority (CA) certificate from a third-party vendor.
- Produce a Certification Authority (CA) certificate internally.

Export Self-Signed Live Data Certificates

Live Data installation includes the generation of self-signed certificates. If you choose to work with these self-signed certificates (rather than producing your own CA certificate or obtaining a CA certificate from a third-party certificate vendor), 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 Finesse 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.

Follow the instructions provided in the *Unified CCE Solution: Procedure to Obtain and Upload Third-Party CA certificates (Version 11.x)* technical note at : https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-enterprise-1101/200286-Unified-CCE-Solution-Procedure-to-Obtai.html .