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 or applicable team codes).

- When Finesse IPPA displays reason codes, some IP Phone models truncate the codes due to character length limitations on the phone. To ensure they meet your requirements, verify the display of the reason codes on all phone models in your environment.

Finesse IP Phone Agent Service Access Protocol

Finesse IPPA phone clients communicate with the Finesse server using Secure HTTP (HTTPS) protocol.

Failure Behavior

Unlike the Finesse desktop, the Finesse IP Phone Agent does not automatically failover to the alternate Finesse server. To resume usual 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.

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	Required	Required	Required
Configure Finesse IP Phone Service in Unified CM	Required	Required	Required
Add Service Parameters for One Button Sign In	Not applicable	Required only with One Button Sign In	Required only with One Button Sign In
Subscribe Agent Phones to Manual Subscription Service	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	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. For proper Finesse IPPA operation, you must also set the Web Access and HTTPS Server parameters in Unified CM.

The following steps are required for both manual and enterprise subscriptions:

Before you begin

Set up call capabilities for the agent phones in Cisco Unified Communications Manager.

Procedure

Step 1 Set the following parameters in Unified CM:

- Set the **Web Access** parameter to **Enabled**.
- Set the **HTTPS Server** parameter to **HTTPS Only**.

To set these parameters in Cisco Unified CM Administration, use either of the following pages:

- Phone Configuration page (Product Specific Configuration portion of page): choose **Device > Phone**.
- Enterprise Phone Configuration page: choose **System > Enterprise Phone Configuration**.

Step 2 Configure an application user in Unified Communications Manager.

a) In Cisco Unified Communications Manager Administration, select **User Management** > **Application User**.
b) Click **Add New**.
c) Under User Information, enter a user ID and password for the new user.

The password must be 95 characters or less and must contain ASCII characters only.

d) Under Device Information, in the Available Devices pane, select all phones that Finesse IP Phone Agents will use and move them to the Controlled Devices pane using the arrows.
e) Under Permissions Information, click **Add to Access Control Group**.

f) From the list of search results, select **Standard CTI Enabled** and **Standard CTI Allow Control Of All Devices** and then click **Add Selected**.

The application user is added to the Standard CTI Enabled and Standard CTI Allow Control Of All Devices groups.

g) Click **Save** at the bottom of the page.

Note In UCCX deployments, usage of an existing RMCM User for Finesse IPPA is known to cause problems in functionality, however, the physical phones must be associated with the RMCM User.

Step 3 Enter the application user's credentials in the Finesse IP Phone Agent Settings gadget.

a) Sign in to the Cisco Finesse Administration Console.
b) Choose **Settings** > **IP Phone Agent Settings**.
c) Under Phone URL Authentication Settings, enter the same username and password that you entered in Unified CM for the application user.

The password must be 95 characters or less and must contain ASCII characters only.

d) Click **Save**.
e) Restart Cisco Finesse Tomcat on the primary Finesse server.
f) After replication is complete, restart Cisco Finesse Tomcat on the secondary Finesse server.

Note For Finesse IP Phone Agent (IPPA) from 11.0 (1) onwards, the User Device Profile (UDP) must be associated with the Finesse IP Phone Agent Application User along with the physical phones for agents using Extension Mobility. The Finesse Service URL must use the complete FQDN of the Unified CCX server.

Configure Finesse IP Phone Service in Unified CM

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

Procedure

Step 1 Log in to the Unified CM Administration using administrator credentials.

Step 2 Select **Device** > **Device Settings** > **Phone Services**.

Step 3 Click **Add New** to create a new IP phone service.

Step 4 In the **Service Name** field, enter **`Cisco Finesse`** (or another service name that is appropriate for your environment).

Step 5 In the **Service URL** field, enter: `http://Finesse FQDN:8082/fippa/#DEVICENAME#`

Note The **Service URL** entry is mandatory for Unified CM.

Step 6 In the **Secure-Service URL** field, enter: `https://Finesse FQDN:8445/fippa/#DEVICENAME#` to configure Finesse IP Phone Agent.

Note

- Support to HTTP is disabled from Cisco Finesse, Release 12.5(1) onwards. Step 5 and Step 6 are mandatory to save the Finesse IP Phone Agent settings.
- Import certificates for Finesse IP Phone Agent to communicate with the Finesse server using Secure HTTP (HTTPS) mode. For more information, see *Finesse IP Phone Agent Certificate Management*.

Step 7 Ensure that the **Service Category** is set to **XML Service**, and the **Service Type** is set to **Standard IP Phone Service**.

Step 8 Check the **Enable** check box.

Step 9 Perform one of the following:

- To automatically subscribe all phones in the cluster to the 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.

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

Step 10 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 and Step 6, replace *Finesse FQDN* with the FQDN of the secondary server.

Note The language used in Finesse IPPA is selected based on the User Locale field in Unified CM. The language selected based on the User Locale must be available in the Unified CCX language pack for Unified CCX deployments and Unified CCE pack for Unified CCE deployments.

If the language selected based on the User Locale in Unified CM is not available in the respective deployments , Finesse IPPA displays all content in the default language (U.S. English).

Finesse IP Phone Agent Certificate Management

The administrator must perform the following operations to enable Finesse IP phones to communicate with the Finesse server using HTTPS.

- For a CA-signed certificate, see CA-Signed Certificate, on page 7.
- For a self-signed certificate, see Self-Signed Certificate, on page 7.

CA-Signed Certificate

Procedure

Step 1 Obtain the CA-signed certificate from the signed authority for both Cisco Finesse and CUCM server.

Step 2 Import the CA-signed certificate of CUCM to the Cisco Finesse server trust store as **tomcat-trust**. For more information, see Import CUCM Certificate , on page 8.

Step 3 Import the CA-signed certificate of Cisco Finesse certificate to the CUCM trust store as **Phone-trust**. For more information, see Import Certificate into CUCM Trust Store, on page 9.

Self-Signed Certificate

Procedure

Step 1 Export the self-signed CUCM certificate from the Cisco Unified Operating System Administration. For more information, see Export CUCM Certificate, on page 7.

Step 2 Import the downloaded self-signed CUCM certificate to the Cisco Finesse trust store as **tomcat-trust**. For more information, see Import CUCM Certificate , on page 8.

Step 3 Export the self-signed Cisco Finesse certificate from the Cisco Unified Operating System Administration. For more information, see Export Cisco Finesse Certificate, on page 8.

Step 4 Import the downloaded self-signed Cisco Finesse certificate to the CUCM trust store as **Phone-trust**. For more information, see Import Certificate into CUCM Trust Store, on page 9.

Export CUCM Certificate

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the CUCM server using the following URL: `https://FQDN of CUCM server:8443/cmplatform`.

Step 2 Select **Security** > **Certificate Management**.

Step 3 Enter the search criteria as **`tomcat`** and then click **Find** to filter the certificate.

The tomcat certificates list is displayed. If you do not find the tomcat certificate for your server in the **Certificate List**, then click **Generate Self-signed**. When the certificate generation is complete, reboot your server. Then restart this procedure. For more information on generating the self-signed certificate, see *Cisco Unified Operating System Administration Online Help*.

Step 4 Click the tomcat certificate hyperlink in the **Common Name** column.
The tomcat **Certificate Details** dialog box is displayed.

Step 5 Click **Download .PEM File**.

Step 6 Save the .PEM file in your local machine.

What to do next

Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

Import CUCM Certificate

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the Cisco Finesse server using the following URL: `https://FQDN of Finesse server:8443/cmplatform`.

Step 2 Select **Security** > **Certificate Management** > **Upload Certificate/Certificate chain**.

Step 3 From the **Certificate Purpose** drop-down list, select **tomcat-trust**.

Step 4 In the **Upload File** field, click **Choose File** and browse to the tomcat.pem or CA-signed certificate file that you saved on your system.

Step 5 Click **Upload**.

Step 6 Restart Cisco Finesse tomcat and Cisco Finesse Notification Service.

Note Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

Export Cisco Finesse Certificate

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the Cisco Finesse server using the following URL: `https://FQDN of Finesse server:8443/cmplatform`.

Step 2 Select **Security** > **Certificate Management**.

Step 3 Enter the search criteria as **`tomcat-trust`** and then click **Find** to filter the certificate.

The tomcat-trust certificates list is displayed. If you do not find the tomcat certificate for your server in the **Certificate List**, then click **Generate Self-signed**. When the certificate generation is complete, reboot your server. Then restart this procedure. For more information on generating the self-signed certificate, see *Cisco Unified Operating System Administration Online Help*.

Step 4 Click the tomcat-trust certificate hyperlink in the **Common Name** column.
The tomcat **Certificate Details** dialog box is displayed.

Step 5 Click **Download .PEM File**.

Step 6 Save the .PEM file in your local machine.

What to do next

Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

Import Certificate into CUCM Trust Store

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the CUCM server using the following URL: `https://FQDN of CUCM server:8443/cmplatform`.

Step 2 Select **Security** > **Certificate Management** > **Upload Certificate/Certificate chain**.

Step 3 From the **Certificate Purpose** drop-down list, select **Phone-trust**.

Step 4 In the **Upload File** field, click **Browse** and browse to the tomcat.pem or CA-signed certificate file that you saved on your system.

Step 5 Click **Upload**.

Step 6 Reboot the Cisco Unified Communications Manager (CUCM) server.

Note Follow the same steps for both publisher and subscriber nodes. It is also to be followed for all the CUCM node certificates.

Add Service Parameters for One Button Sign In

With One Button Sign In, for any agent credentials that you want prepopulated, you must set up corresponding service parameters in Unified CM.

Only perform this procedure if you are setting up One Button Sign In. Otherwise, skip this.

Procedure

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.

Step 3 Set up service parameters for the agent id, extension, and password credentials as per the following table. Enter only the parameters that you want prepopulated for the agents. For each parameter, enter the required field values and click **Save**. To add parameters, click **Add New** and enter the required values.

Field	Description
Parameter Name	Enter a parameter name in lower case exactly similar to — id, extension, and password. The values entered are the exact query string parameters used for the subscription URL.

Field	Description
Parameter Display Name	Enter a descriptive parameter name; for example, id, extension, and password.
Default Value	Leave the default value blank for all parameters.
Parameter Description	Enter a description of the parameter. The user can access this text when they subscribe to the service.
Parameter is Required	If the administrator prepopulates the parameter in Unified CM Administration, check the **Parameter is Required** box. However, if the agent prepopulates the parameter in the Self Care Portal, two options are available: • If the agents prepopulates all defined parameters, check the **Parameter is Required** box for each parameter. • If the agent and administrator share the responsibility of prepopulating the parameters, set only the administrator-defined parameters as required. This configuration ensures that the administrator can save the subscription without prepopulating all parameters. In this case, the administrator first prepopulates the required parameters, and then the agents prepopulate the nonrequired parameters.
Parameter is a Password (mask contents)	Check this box for the password only. This check box masks the password entries in the Self Care Portal, to display asterisks rather than the user entry.

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

What to do next

You can prepopulate the agent credentials when you subscribe the agent phones, or the agents can prepopulate their own credentials using the Unified CM Self Care Portal.

Subscribe Agent Phones to Manual Subscription Service

If you set up the 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 to 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 the primary and secondary Finesse services.

Finesse IP Phone Agent Login During Maintenance Mode

Maintenance Mode for Cisco Finesse servers is supported starting from release 12.6(1) in order to support unscheduled down times. When the Cisco Finesse node is in maintenance mode, Finesse IPPA users are not allowed to login. Finesse IPPA users receive the following message if they attempt to login to a Cisco Finesse node which is currently under maintenance mode:

```
This Finesse Service is unavailable due to maintenance in progress. Please
sign in using the alternate Finesse service.
```