Manage System Settings

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

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

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

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

Contact Center Enterprise Administration and Data Server Settings

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

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

After you change and save any value on the Contact Center Enterprise Administration & Data Server Settings gadget, restart the Cisco Finesse Tomcat Service on the primary and secondary Finesse server. If you restart the Cisco Finesse Tomcat Service, agents must sign out and sign in again. To avoid this, you can make Contact Center Enterprise Administration & Data Server settings changes and restart the Cisco Finesse Tomcat service during hours when agents are not signed in to the Cisco Finesse desktop.

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

Table 1: Field Descriptions

Field	**Description**
Primary Host/IP Address	The hostname or IP address of the Unified CCE Administration & Data Server.
Backup Host/IP Address	(Optional) 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** Cisco Finesse expects the primary and backup Administration & Data Server ports to be the same, hence the Finesse administration console exposes one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers.
AW Database Name	The name of the AW Database (AWDB). For example, *ucceinstance*_awdb).
Domain	(Optional) The domain name of the AWDB. For example, cisco.com.

Field	Description
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 Unified CCE Administration & Data Server Settings gadget:

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

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

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

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

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

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

Configure Contact Center Enterprise Administration and Data Server Settings

Configure the Unified CCE Administration & Data Server settings to enable authentication for Finesse agents and supervisors.

Procedure

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

Step 2 In the Unified CCE Administration & Data Server Settings area, enter the Administration & Data Server settings as described in the preceding table. For more information, see Table 1: Field Descriptions, on page 2. Refer to your configuration worksheet if necessary.

Step 3 Click **Save**.

What to do next

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

Contact Center Enterprise CTI Server Settings

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

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

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

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

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

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

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

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

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

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

Actions on the Contact Center Enterprise CTI Server Settings gadget:

- **Save:** Saves your configuration changes.
- **Revert:** Retrieves the most recently saved server settings.
- **Test Connection:** Tests the CTI connection.

CTI Test Connection

When you click **Test Connection**:

1. Input validation is done on the request attributes.

   Host/IP Address must not be empty. Port and Peripheral IDs must be within the valid range.

2. Validation is done to check if the provided Host/IP is resolved by Finesse box.

3. Validation is done to check if AW Database is reachable and if a valid path ID is configured for the provided Peripheral ID.
4. Socket connection is established to the provided Host/IP and port. The connection might fail if there is no route to the provided IP. If SSL encryption box is checked, this step also checks for successful TLS handshake. For TLS handshake to be successful, mutual trust has to be established between Finesse and CTI server.

   For information on how to establish trust between Finesse and CTI server, see *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html
5. After successful socket connection, a CTI initialization request is sent to check if the provided host is a CTI host.

   If the CTI response is a success for the CTI initialization request and peripheral provided is configured with Unified CCE, it is confirmed to be a CTI host.
6. CTI connection is closed by sending a CTI session close request.

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

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

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

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

Configure Contact Center Enterprise CTI Server Settings

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

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

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

Procedure

Step 1 Sign in to the administration console on the primary Finesse server:

https://*FQDN of Finesse server*/cfadmin

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

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

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 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.

Step 4 Click **Save**.

Cluster Settings

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

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

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

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 Sign in to the administration console with the Application User credentials.

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

Step 3 Click **Save**.

Desktop Chat Server Settings

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

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

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

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

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

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

Field	Explanation
Primary Chat Server	Enter the IM&P primary server URL of Desktop Chat.
Secondary Chat Server	Enter the IM&P secondary server URL of Desktop Chat.

Actions on the Desktop Chat Server gadget:

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

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

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

Note Desktop Chat requires the Cisco IM and Presence certificates to be trusted. To start the Desktop Chat without experiencing an exception, you must add the certificate to the browser trust store, or configure IM and Presence with CA-signed certificate, or push self-signed certificate through group policies in supported browsers. For more information on accepting certificates, see the *Accept Security Certificates* section, in the *Common Tasks* chapter of *Cisco Finesse Agent and Supervisor Desktop User Guide for Cisco Unified Contact Center Express* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html.

For more information on adding certificates to the browser trust store, see Certificate Management.

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

Configure Desktop Chat Server Settings

Procedure

Step 1 Sign in to the administration console with the Application User credentials.

Step 2 In the **Desktop Chat Server Settings** area, enter the IM&P primary and secondary server URL of the Desktop Chat.

Step 3 Click **Save**.

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

Cloud Connect Server Settings

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

For more information, see the Cisco Webex Experience Management Integration section in *Cisco Unified Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html.

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

Field	Explanation
Username	(mandatory) The Cloud Connect administrator username required to sign in to Cloud Connect.
Password	(mandatory) The Cloud Connect administrator password required to sign in to Cloud Connect.
Publisher Address	(mandatory) The FQDN of the Cloud Connect publisher.
Subscriber Address	(optional) The FQDN of the Cloud Connect subscriber.

Actions on the Cloud Connect Server Settings gadget:

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

For more information on importing Cloud Connect certificates, see the *Cloud Connect Certificates* section in *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html.

Configure Cloud Connect Server Settings

Procedure

Step 1 Sign in to the administration console on the primary Finesse server using the URL: https://FQDN of Finesse server:8445/cfadmin.

Step 2 Select **Settings** > **Cloud Connect Server Settings**.

Step 3 Enter the **Username**, **Password**, and **Publisher Address** of the Cloud Connect server.

(optional) Enter the **Subscriber Address** for multinode deployment.

Step 4 Click **Save**.

Update Cloud Connect Connection Time

When there is a low bandwidth, the default value that is used for an HTTP client for obtaining the Cloud Connect token may not be sufficient and result in timeout. The following CLI commands can be used to view and update the connection timeout values. The default value for `cloudconnectHttpConnectionTimeout` is 5000 milliseconds and the default value for `cloudconnectHttpReadTimeout` is 10000 milliseconds.

To view the current values, use the following commands:

```
utils finesse show_property webservices cloudconnectHttpConnectionTimeout
```

```
utils finesse show_property webservices cloudconnectHttpReadTimeout
```

To update the values, use the following commands:

```
utils finesse set_property webservices cloudconnectHttpConnectionTimeout
<time_value_in_milliseconds>
```

```
utils finesse set_property webservices cloudconnectHttpReadTimeout
<time_value_in_milliseconds>
```

For example, the `utils finesse set_property webservices cloudconnectHttpConnectionTimeout 8000` command updates the HTTP connection timeout value to 8000 milliseconds.

The `utils finesse set_property webservices cloudconnectHttpReadTimeout 12000` command updates the HTTP connection read timeout value to 12000 milliseconds.

Keyboard Shortcuts

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

Keyboard Shortcut Conflicts

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

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

Keyboard shortcut conflict can occur in the following scenarios:

Conflict Scenario	Resolution
Conflicts can occur between keyboard shortcuts at the page level and gadget level.	This conflict cannot be resolved by the Finesse administrator.
Conflicts can occur when two gadgets have the same keyboard shortcut, and both are in the same tab.	Move one of the gadgets to another tab.

Conflict Scenario	Resolution
Conflicts can occur when there are multiple instances of the same gadget and focus is on the active tab*.	Move one of the gadgets to another tab.

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

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

Note

- After deploying the third-party gadgets, the administrator must sign in as an agent and a supervisor to check if there are any keyboard shortcut conflicts and resolve them.
- The third-party gadget providers can use the keyboard shortcuts JavaScript library as a guideline to provide a consistent desktop user experience.
- The ECE (Enterprise Chat and Email) keyboard shortcuts are available only if ECE gadget is configured in the Unified CCE deployment. If it is not configured, the third-party gadget developers can use the ECE shortcut keys that are listed in **Keyboard Shortcuts List**. For more information, see the *Cisco Finesse Agent and Supervisor Desktop User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html.