# 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.



# 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.


**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.<br>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.<br>This field is required and accepts values between 1 and 65535.<br>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*.<br>The default value is 42027. |
| Peripheral ID | The ID of the Agent PG Routing Client (PIM).<br>The Agent PG Peripheral ID should be configured to the same value for the A Side and B Side CTI server.<br>This field is required and accepts values between 1 and 32767.<br>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.<br>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

# 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.<br>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).<br>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

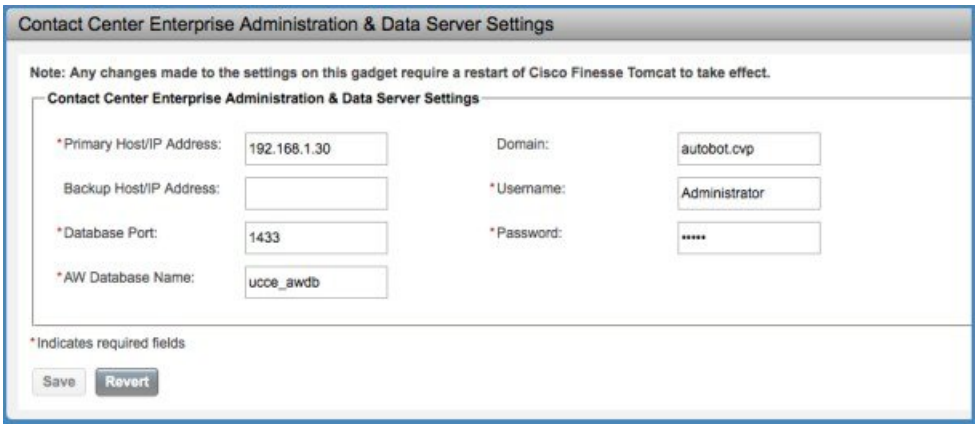
Use the Contact Center Enterprise Administration & Data Server Settings gadget to configure the database settings. These settings are required to enable authentication for Finesse agents and supervisors.

**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.




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.<br>The default value is 1433.<br>**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.<br>**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.<br>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

# 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.<br>**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.<br>Default: 1000 milliseconds<br>Range: 200 to 15,000 milliseconds. |
| Lab Mode | Radio button indicates if the Context Service is in production mode or lab mode.<br>• Enable—Context Service switches to lab mode.<br>• 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.