



## Initial Configuration

---

- [Configure Contact Center Enterprise Administration & Data Server Settings, on page 1](#)
- [Configure Contact Center Enterprise CTI Server Settings, on page 2](#)
- [Configure Cluster Settings, on page 3](#)
- [Restart Cisco Finesse Tomcat, on page 3](#)
- [Check Replication Status, on page 4](#)
- [Install Language Pack, on page 4](#)
- [Configure IPv6 Settings, on page 5](#)
- [Ensure Agents Have Passwords, on page 6](#)
- [Ensure Logout Non-Activity Time for Agents is Configured, on page 7](#)
- [Configure Agent Phones, on page 7](#)
- [Configure Finesse IP Phone Agent, on page 7](#)
- [Browser Settings for Agent and Supervisor Desktop, on page 8](#)
- [Ensure Agents Can Sign in to Desktop, on page 8](#)
- [Configure DNS on Clients, on page 9](#)
- [Load Balancing for Finesse, on page 10](#)
- [Initial Configuration Troubleshooting, on page 11](#)

## Configure Contact Center Enterprise Administration & Data Server Settings

Configure the Contact Center Enterprise Administration & Data Server settings to enable authentication for Cisco 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	The hostname or IP address of the Unified CCE Administration & Data Server. For example, <b>abcd12-5-aw-a</b> .
Backup Host/IP Address	The hostname or IP address of the backup Unified CCE Administration & Data Server. For example, <b>abcd12-5-aw-b</b> .
Database Port	The port of the Unified CCE Administration & Data Server. The default value is 1433. <b>Note</b> 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, <b>ucceinstance_awdb</b> .
Domain	The domain name of the AWDB. For example, <b>cisco.com</b> .
Username	The username required to sign in to the AWDB. <b>Note</b> 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.

**Step 3** Click **Save**.

## 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**.

## 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**.

## Restart Cisco Finesse Tomcat

After you make changes to the Contact Center Enterprise CTI Server, Contact Center Enterprise Administration & Data Server, or cluster settings, restart Cisco Finesse Tomcat for the changes to take effect.



---

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

---

### Procedure

---

- Step 1** Access the CLI and run the following command:
- ```
utils service restart Cisco Finesse Tomcat
```
- Step 2** You can enter the command **utils service list** to monitor the Cisco Finesse Tomcat Service. After Cisco Finesse Tomcat changes to STARTED, the configured agents can sign in to the desktop.
- 

## Check Replication Status

### Procedure

---

- Step 1** Access the CLI on the primary Finesse server.
- Step 2** Sign in with the Administrator User credentials that are defined during installation.
- Step 3** Run the following command:
- ```
utils dbreplication runtimestate
```
- This command returns the replication status on both the primary and secondary Finesse servers.
- 

## Install Language Pack

Download and install a language pack only if you want to use the Finesse desktop interface in a language other than English.

The language pack for Finesse is delivered as a single Cisco Option Package (COP) file. The file is available to download from Cisco.com and contains a single installer for all language variants.

You can download the language pack for Finesse at the following link:

<https://software.cisco.com/download/release.html?mdfid=283613135&softwareid=284259728&relind=AVAILABLE&rellifecycle=&reltype=latest>

COP files can generally be installed on an active, running system. However, language COP files cannot be removed or rolled back.



**Note** If the ReadMe file for a specific COP file contradicts these general guidelines, follow the instructions provided with the file.

For more information about supported languages, see the *Cisco Finesse Administration Guide* (<https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html>).

### Procedure

- Step 1** Download the Finesse COP file from the Cisco Software site <https://software.cisco.com/download/type.html?mdfid=283613135&i=rm> to a local source or an SFTP server that can be accessed by the Finesse server.
- Step 2** Use SSH to log in to your Finesse system with the platform administration account.
- Step 3** Use the CLI to run the command **utils system upgrade initiate**.
- Step 4** Follow the instructions provided by the **utils system upgrade initiate** command.
- Step 5** Reboot the server.
- Step 6** Repeat step 2 through step 5 on the secondary Finesse server.
- Step 7** When the installation is complete on both Finesse servers, agents and supervisors must clear their browser cache and cookies.

## Configure IPv6 Settings

Cisco Finesse supports IPv6 using dual stack (IPv4 and IPv6). By default, only IPv4 is enabled at installation. You can enable IPv6 after installation using either Cisco Unified Communications Operating System Administration or the CLI.

With IPv6 enabled, the Finesse Administration Console, Finesse Desktop Interface, and Finesse REST APIs can connect to the Finesse server using IPv4 or IPv6. However, the Finesse server can connect to Unified CCE and the CTI server using IPv4 only.

When you set up IPv6 on Finesse, restart the system for the updates to take effect.

## Set Up IPv6 Using Cisco Unified Communications Operating System Administration

To set up IPv6 using Cisco Unified Operating System Administration, perform the following procedure on both the primary and secondary Finesse servers.

### Procedure

- Step 1** Sign in to Cisco Unified Operating System Administration on the Finesse server (<http://FQDN:8080/cmplatform>, where *FQDN* is the fully qualified domain name of the Finesse server).

- Step 2** Navigate to **Settings > IP > Ethernet IPv6**.
  - Step 3** To enable IPv6, check the **Enable IPv6** check box (or uncheck the box to disable IPv6).
  - Step 4** Enter values for **IPv6 Address**, **Prefix Length**, and **Default Gateway**.
  - Step 5** To restart after you save the changes, check the **Update with Reboot** check box.
  - Step 6** Click **Save**.
- 

## Set Up IPv6 Using the CLI

To set up IPv6 using the CLI, perform the following procedure on both the primary and secondary Finesse servers.

### Procedure

---

- Step 1** Access the CLI on the Finesse server.
  - Step 2** To enable or disable IPv6, enter:  
**set network ipv6 service {enable | disable}**
  - Step 3** Set the IPv6 address and prefix length:  
**set network ipv6 static\_address *addr mask***  
**Example:**  

```
set network ipv6 static_address 2001:db8:2::a 64
```
  - Step 4** Set the default gateway:  
**set network ipv6 gateway *addr***
  - Step 5** Restart the system for the changes to take effect.  
**utils system restart**
  - Step 6** To display the IPv6 settings, enter:  
**show network ipv6 settings**
- 

## Ensure Agents Have Passwords

Agents who do not have a password defined in Unified CCE Configuration Manager cannot sign in to Finesse.

Agent password is an optional field in Unified CCE, but it is mandatory for Cisco Finesse.

For agents who do not have passwords, you must perform the following steps:

### Procedure

---

- Step 1** Launch Unified CCE Configuration Manager.
- Step 2** Locate the record for the agent (Agent Explorer > Agent tab).

- Step 3** Enter a password, and save the record.
- 

## Ensure Logout Non-Activity Time for Agents is Configured

The Logout non-activity time specifies how long an agent can remain inactive in the Not Ready state before that agent is signed out of Finesse.

Perform the following steps to configure Logout non-activity time for an agent.

### Procedure

---

- Step 1** Launch the Unified CCE Configuration Manager.
- Step 2** Launch Agent Desk Settings List (**Tools > List Tools**).
- Step 3** Select **Agent Desk Settings List**.
- Step 4** In the Logout non-activity time field, enter the number of seconds of agent inactivity while in the Not Ready state before the system software signs the agent out. You can enter a value between 10 seconds and 7200 seconds.
- Step 5** Click **Save**.
- The modified settings are applied to all of the agents who use these agent desktop settings.
- 

## Configure Agent Phones

Before agents can sign in to the Finesse desktop, you must ensure that the agent phones are configured in Unified Communications Manager. For more information about configuring agent phones, see the “Agent Phones” section of the *Cisco Unified Contact Center Enterprise Design Guide* (<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html>).

## Configure 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.

To set up Finesse IPPA, see the *Cisco Finesse Administration Guide* (<https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html>).



---

**Note** The Finesse IPPA setup requires a Cisco Finesse Tomcat restart.

---

## Browser Settings for Agent and Supervisor Desktop

To ensure that all features of the Cisco Finesse agent and supervisor desktop work properly, you must disable popup blockers from the following supported browsers:

- Chrome (version 60 or higher)




---

**Note** Ensure to disable the **Automatic tab discarding** feature in Chrome (version 74 and earlier) to avoid exiting the Cisco Finesse desktop tab when the system memory is low.

---

- Firefox (version 52 and higher ESR)
- Edge Chromium (Microsoft Edge v79 and later)
- Internet Explorer 11.0 (Native Mode)

Apart from disabling popup blockers, to configure the privacy and advanced settings in Internet Explorer, go to **Tools > Internet Options > Privacy**. Enter the domain name of Side A and B Finesse servers, and click **Allow**.

## Ensure Agents Can Sign in to Desktop

After the system administrator defines configuration settings and restarts services, agents who have passwords and operational handsets can sign in to the Finesse Agent Desktop.




---

**Note** Finesse agents can enter either their `AgentID` or `Login name` (in the **Username** field of the desktop login screen) to sign in. Ensure that each agent's `AgentID` and `Login name` are unique across both sets of data. If one agent's `AgentID` matches another agent's `Login name`, neither agent can sign in.

---




---

**Note** After you restart Finesse, it takes approximately 6 minutes for all server-related services to restart. Therefore, you should wait 6 minutes before you attempt to sign in to the desktop.

---




---

**Note** If you are using HTTPS, the first time you access the agent desktop, 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** Enter the following URL in the address bar of your browser:  
http://FQDN of Finesse server/desktop
- Step 2** If you installed the language pack COP file, on first login, select the language you want to appear on the desktop from the drop-down menu in the language selector screen and click **Next**. If you did not install the language pack COP file, the language selector drop-down list does not appear in the user interface.
- Note** If you installed the language pack COP file, you can also select a language by passing the locale as part of the URL (for example, http://FQDN of Finesse server/desktop?locale=fr\_FR) or by changing your browser preferred language. The default language is English (en\_US).
- Step 3** Enter your username, password, and extension, and then click **Sign In**.
- Note** The Sign In button is enabled once the username, password and extension fields are entered. If any field is incomplete, the Sign In button will remain disabled.
- Step 4** If you wish to change the language that appears on your desktop, use the **Change the Language** link to return to the language selector screen and choose the language.
- If your agent is signed into the Agent Desktop in Single Sign-On Mode or Hybrid Mode, refer to the sections *Sign In to Finesse Desktop Single Sign-On Mode* or *Sign In to Finesse Desktop Hybrid Mode* in the *Cisco Finesse Desktop User Guide for Unified Contact Center Enterprise*.
- 

# Configure DNS on Clients



- Note** This procedure is required for uncommon environments where non-hierarchical DNS configuration exists. If your environment has hierarchical DNS configuration, you do not need to perform this procedure. This procedure applies to clients that use a Windows operating system. For information about configuring DNS on Mac clients, see your Apple documentation ([www.apple.com/mac](http://www.apple.com/mac)).
- 

Configuring DNS on client computers allows the clients to resolve the fully-qualified domain name (FQDN) of the active Finesse server during a failover.

## Procedure

---

- Step 1** Go to **Control Panel > Network and Internet > Network and Sharing Center**. (Open the Control Panel, enter Network Connections in the search bar, and then click **View network connections**.)
- Step 2** Click the appropriate network connection.  
A dialog box showing the status of the connection appears.
- Step 3** Click **Properties**.

- Step 4** On the Networking tab, select Internet protocol version 4 (TCP/IPv4) or Internet protocol version 6 (TCP/IPv6) if the client is IPV6, and then click **Properties**.
  - Step 5** Click **Advanced**.
  - Step 6** On the DNS tab, under DNS server addresses, in order of use, click **Add**.
  - Step 7** Enter the IP address of the DNS server that was entered during installation and click **Add**.
  - Step 8** If a secondary DNS was entered during installation, repeat Step 5 and Step 6 to add its IP address.
- 

## Load Balancing for Finesse

After agents sign in to the Finesse desktop, Finesse desktop client manages the failover. For example, if a Finesse server goes out of service, the Finesse client automatically redirects and signs the agent into the other Finesse server. The client can manage various network and server failure use cases. Given this client-side logic, the use of a load balancer after sign-in is not required nor supported.

However, the following are two scenarios in which you can use a load balancer with Finesse. These scenarios apply only to the Finesse desktop and not to Finesse IP Phone Agents.



---

**Note** Starting from the Finesse 12.6.1 ES05 release, the allowed hosts must not contain the hostname or IP address of the load balancer. It should contain only the internal and external hostname and IP address of the reverse-proxy.

---

### When Agents Navigate to the Finesse Sign-In Page

If agents attempt to navigate to a Finesse server that is down or not reachable, agents cannot access the sign-in page. Agents receive an error and must manually sign in to the other Finesse server. To avoid this manual step, you can use a load balancer using URL redirect mode to direct the agents to a Finesse server that is operational. One option is to use the Finesse `SystemInfo` REST API, which provides the status of the Finesse server. For details about this API, see the [Cisco Finesse Web Services Developer Guide](#).

When you configure a load balancer to determine the status of the Finesse servers, the call flow is as follows:

1. When agents sign in to Finesse, they point their browsers to the load balancer.
2. The load balancer redirects the agent browser to an appropriate Finesse server.
3. The agent signs in to the Finesse server directly. At this stage, the load balancer is no longer part of the call flow.

### When Customers Use the Finesse API Directly

If you use the Finesse REST API directly, the Finesse client-side failover logic is not in the call flow. In this case, you can opt to use a load balancer to manage high availability. This load balancer is considered part of a custom application which, like all custom applications, Cisco does not support. You must provide the required support for the load balancer.

Before you configure the load balancer, remember that there are two connections between Finesse clients and the Finesse server:

- A REST channel for request and response.
- An XMPP channel that the server uses to send notifications to the client.

Both channels for a given client must connect to the same Finesse server.

You cannot connect the load balancer to the REST connection for one Finesse server and to the XMPP channel connection for the other Finesse server. This setup provides unpredictable results and is not supported.

## Initial Configuration Troubleshooting

If	Then
The administration console does not load after a fresh installation.	<ol style="list-style-type: none"><li>1. Clear your browser cache (delete browsing history and cookies).</li><li>2. If the problem persists, restart the Cisco Finesse Tomcat service or restart the Finesse server.</li></ol>

<b>If</b>	<b>Then</b>
Agents cannot sign in to the desktop after a fresh installation.	

If	Then
	<ol style="list-style-type: none"> <li>1. Verify that the agent ID and password are correct.           <p><b>Note</b> Finesse agents can use either their <code>loginID</code> or <code>loginName</code> to sign in. Ensure that each agent's <code>loginID</code> and <code>loginName</code> are unique across both sets of data. If one agent's <code>loginID</code> matches another agent's <code>loginName</code>, neither agent can sign in.</p> </li> <li>2. Verify that a valid domain was configured during installation and that forward and reverse DNS are set up correctly. To check whether DNS was configured during installation, check the <code>install.log</code> for the following:           <pre>InstallWizard USER_ACTION_BTN_PUSH: Screen = DNS Client Configuration, button pushed = No &lt;LVL::Info</pre> <p>The preceding message indicates that DNS was not configured during the installation. Reinstall Finesse and configure the DNS with a valid domain.</p> </li> <li>3. Verify that the agent is configured in Unified CCE.</li> <li>4. Verify that the AWDB is configured correctly.           <ol style="list-style-type: none"> <li>a. Check the <code>realm.log</code> for the following line:               <pre>"ERROR com.cisco.ccbu.finesse.realms.ccerealm.CCERealmConfig - Cannot connect to any AWDB! Ensure that at least one AWDB is configured properly and running!"</pre> <p>This line indicates that Finesse cannot connect to the AWDB.</p> </li> <li>b. Check that the values entered in the Contact Center Enterprise Administration &amp; Data Server Settings gadget are correct.               <ul style="list-style-type: none"> <li>• Verify that the username entered is a Windows domain user.</li> <li>• Verify that the username is not prepended with the domain (for example, <code>domain\username</code>).</li> <li>• Verify that the port configured is open to the Finesse server.</li> </ul> </li> <li>c. Check that the AWDB is set up correctly and running.               <ul style="list-style-type: none"> <li>• The AWDB SQL server must use Windows authentication.</li> <li>• Verify that the AWDB server is up and that the Distributor service is running.</li> </ul> </li> </ol> </li> <li>5. Restart Cisco Finesse Tomcat on the primary and secondary Finesse servers.</li> <li>6. Verify that the agent's device is properly configured in Unified</li> </ol>

If	Then
	Communications Manager and is active.