This chapter describes failover and redundancy mechanisms for Cisco Finesse.

- CTI Failover, on page 1
- AWDB Failover, on page 2
- Finesse Client Failover, on page 3
- Desktop Behavior, on page 4
- Finesse IP Phone Agent Failover, on page 7

## 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.
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

## 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

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 for current server every 20 seconds and the other Finesse server between 10-45 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 20 seconds, the desktop also checks the availability of the alternate server every 10-45 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.

---

Note

After Finesse failover, the pending state of an agent will not be displayed once the agent fails over to the secondary Finesse node. The pending state change is reflected on the desktop only after the call ends.

---

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.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Desktop Behavior</th>
<th>Server Action</th>
<th>Results</th>
</tr>
</thead>
</table>
| 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. |
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.

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.