Cisco Finesse CLI

The CLI provides a set of commands applicable to the operating system and to Cisco Finesse. These commands allow basic maintenance and failure recovery and enable some system administration.

Although Finesse provides access to all Cisco Unified Communications Manager CLIs, many commands are not applicable to Finesse and most have not been validated for Finesse.

You can access the CLI directly, using the monitor and keyboard at the server console, or by SSH. Sign in with the Administrator User credentials created during installation.

• Commands Supported for Cisco Finesse, on page 1

Commands Supported for Cisco Finesse

Finesse supports the following CLI commands and has qualified their use.

Cisco Finesse HTTPS Redirect

Enable Cisco Finesse HTTPS Redirect to enforce HTTPS to access the Finesse desktop and administration console. If Cisco Finesse HTTPS Redirect is enabled, agents and supervisors who attempt to access the desktop with HTTP are redirected to HTTPS. Administrators who attempt to access the administration console with HTTP are also redirected to HTTPS.

If Cisco Finesse HTTPS Redirect is disabled, the desktop and the administration console can be accessed with HTTP or HTTPS.

Note This command does not impact the Finesse REST APIs.

In a two-node setup, if you enable or disable HTTPS Redirect only on the primary Finesse server, the setting does not replicate to the secondary Finesse server. You must enter the required commands on both the primary and secondary Finesse server.

To view the status of, enable, or disable Cisco Finesse HTTPS Redirect:

- To retrieve the status of Cisco Finesse HTTPS Redirect: **utils finesse application_https_redirect status**

  This command displays whether Cisco Finesse HTTPS Redirect is currently enabled or disabled on the system.

Note On the secondary server, the HTTPS redirect status appears as enabled for the Finesse Agent Desktop only. For Finesse Admin, the HTTPS redirect status always appears as disabled on the secondary server because Finesse Admin is not available on the secondary server.

- To enable Cisco Finesse HTTPS Redirect: **utils finesse application_https_redirect enable**

  You must stop the Cisco Finesse Tomcat Service before you can enable Cisco Finesse HTTPS Redirect. You can use the following command to stop this service: **utils service stop Cisco Finesse Tomcat**.

  If the Cisco Finesse Tomcat Service is not stopped, the command to enable Cisco Finesse HTTPS Redirect fails. This command also fails if Cisco Finesse HTTPS Redirect is already enabled.

  After you enable Cisco Finesse HTTPS Redirect, start the Cisco Finesse Tomcat Service using the command **utils service start Cisco Finesse Tomcat**.

- To disable Cisco Finesse HTTPS Redirect: **utils finesse application_https_redirect disable**

  You must stop the Cisco Finesse Tomcat Service before you can disable Cisco Finesse HTTPS Redirect. You can use the following command to stop this service: **utils service stop Cisco Finesse Tomcat**.

  If the Cisco Finesse Tomcat Service is not stopped, the command to disable Cisco Finesse HTTPS Redirect fails. This command also fails if Cisco Finesse HTTPS Redirect is already disabled.

  After you disable Cisco Finesse HTTPS Redirect, start the Cisco Finesse Tomcat Service using the command **utils service start Cisco Finesse Tomcat**.

Finesse Services

To view, start, or stop services:

- To view the platform TCP/IP services, UDP services, and Unix domain sockets used by Cisco Finesse: **show network all detail**
- To retrieve the status of services: **utils service list**

  This command retrieves a list of all services and their status.

  Services are shown in one of the following states: STOPPED, STARTING, or STARTED.

  STOPPED means the service is not running. STARTING means the service is starting operation and performing any necessary initialization. STARTED means the service has successfully initialized and is operational.

- To start a service: **utils service start** *service name*

  This command starts the named service.

- To stop a service: **utils service stop** *service name*

  This command stops the named service.

- To start Cisco Finesse Tomcat: **utils service start Cisco Finesse Tomcat**
- To stop Cisco Finesse Tomcat: **utils service stop Cisco Finesse Tomcat**

- To restart Cisco Finesse Tomcat: **utils service restart Cisco Finesse Tomcat**

Note If a Cisco Finesse service-related problem exists, restart the Finesse service. Note that most service-related problems cannot be corrected by restarting a service.

Cisco Finesse Notification Service Logging

To view the status of, enable, or disable Cisco Finesse Notification Service logging:

- To retrieve the status of Cisco Finesse Notification Service logging: **utils finesse notification logging status**

  This command displays whether Cisco Finesse Notification Service logging is currently enabled or disabled on the system.

Note Ensure the Cisco Finesse Notification Service is running before you run the command to retrieve the status of Cisco Finesse Notification Service logging. If the service is not running, this command fails.

- To enable Cisco Finesse Notification Service logging: **utils finesse notification logging enable**

Note Ensure that the Cisco Finesse Notification Service is running before you run the command to enable Cisco Finesse Notification Service logging. If the service is not running, this command fails. This command also fails if Cisco Finesse Notification Service logging is already enabled.

If you enable logging and then restart the Cisco Finesse Notification Service, logging is automatically disabled.

- To disable Cisco Finesse Notification Service logging: **utils finesse notification logging disable**

Note Ensure that the Cisco Finesse Notification Service is running before you run the command to disable Cisco Finesse Notification Service logging. If the service is not running, this command fails. This command also fails if the Cisco Finesse Notification Service logging is already disabled.

Related Topics

Log Collection

Cisco Finesse Trace Logging

Use the following commands to toggle trace logs for Cisco Finesse, enable trace logs for Finesse IPPA, and enable debug logs for realm.

Note Enabling trace logging may cause an overload in the system and must be used for debugging purposes only.

- **utils finesse trace enable**

  This command allows you to:

  - Enable trace logs for Cisco Finesse.
  - Turn on command dispatcher logs.
  - Enable trace logs for Finesse IPPA.
  - Enable debug logs for Realm.

- **utils finesse trace disable**

  This command allows you to:

  - Disable trace logs for Cisco Finesse.
  - Turn off command dispatcher logs.
  - Disable trace logs for Finesse IPPA.
  - Disable debug logs for Realm.

  Note After execution of each command, wait for 60 seconds for the changes to take effect.

- **utils finesse trace status**

  This command allows you to displays status as:

  - Enabled - When all four actions are enabled.
  - Disabled - When all four actions are disabled.

If all actions are not enabled or disabled, a warning message is displayed.

Cisco Finesse Toaster Notifications

Toaster notifications are enabled by default after a fresh installation of Cisco Finesse. Use the following CLI commands to disable, enable, and check the status of the toaster notifications:

- **utils finesse toaster enable [closeTimeout]:** Enable Cisco Finesse toaster notification.

While enabling toaster notification, use the **closeTimeout** parameter (timeout in seconds) to set the time interval after which toaster automatically closes. If no parameter is specified, timeout is set to 8 seconds by default. The valid range for timeout activity is between 5-15 seconds. The browser must be refreshed for timeout changes to take effect.

Note The configured timeout for browser notifications depends on the operating system and browser settings. The timeout value is honored in Chrome browser in Windows OS. However, the other supported browsers do not honor the configured notification timeout value consistently.

- **utils finesse toaster disable:** Disable Cisco Finesse toaster notification.
- **utils finesse toaster status:** Display the status (enable or disable) of the Cisco Finesse toaster notification.

Note Cisco Finesse toaster notifications do not work with Internet Explorer browser.

Cisco Finesse IPPA Inactivity Timeout

Use the following CLI commands to enable or disable the Inactivity Timeout feature in Cisco Finesse IPPA. You must either disable the Cisco Finesse Inactivity Timeout feature or increase the timeout in the range of 120 seconds to one day (in seconds) so that the Finesse IPPA agent does not get logged out of Cisco Finesse IPPA if the agent is on any other screen:

- **utils finesse ippa_inactivity_timeout enable:** To enable Cisco Finesse IPPA Inactivity Timeout feature.

Note The default time set for Cisco Finesse IPPA Inactivity Timeout is 120 seconds.

- **utils finesse ippa_inactivity_timeout disable:** To disable Cisco Finesse IPPA Inactivity Timeout feature.

Note When Cisco Finesse IPPA Inactivity Timeout is disabled, you will not be logged out of Cisco Finesse IPPA, if the agent is on any other screen.

- **utils finesse ippa_inactivity_timeout enable inactivity_timeout:** To enable Cisco Finesse IPPA Inactivity Timeout with timeout set to n seconds.

Note Minimum value of n must be 120 seconds and maximum value can be up to one day (86400 seconds).

- **utils finesse ippa_inactivity_timeout status:** To check the status of Cisco Finesse IPPA Inactivity Timeout.

Note The Finesse IPPA Inactivity Timeout CLIs should be run on both the primary and secondary Finesse servers. Enabling or disabling the Cisco Finesse Inactivity Timeout feature requires a restart of Cisco Finesse Tomcat, and restart must be done in the maintenance window. During upgrade, the Inactivity Timeout configuration is not retained and should be re-configured post upgrade.

To know how this feature works on specific IP phone models, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html

Service Properties

Configure the service properties using the following CLI.

Enable or Disable Secure XMPP Socket—Port 5223

To run this CLI in Cisco Finesse, install Release 11.6(1) ES10 COP or higher.

To run this CLI in Cisco Finesse, install Finesse 12.0(1) ES4 COP or higher.

Use the following CLI commands to enable or disable the external access to the Cisco Finesse Notification Service XMPP port (5223). The port must be enabled for external access only if you have third-party solutions that connect directly to the Cisco Finesse Notification Service over this port. By default, the port is enabled (value is set to *true*).

When the port is enabled, it can be accessed by the Cisco Finesse nodes (primary and secondary) and by external clients. When the port is disabled, it cannot be accessed by external clients.

- To enable: **utils finesse set_property webservices enableExternalNotificationPortAccess true**
- To disable: **utils finesse set_property webservices enableExternalNotificationPortAccess false**
- To display the current status: **utils finesse show_property webservices enableExternalNotificationPortAccess**

Note Restart Cisco Finesse Tomcat and Cisco Finesse Notification Services for the changes to take effect.

Upgrade

Upgrade-related commands are grouped under **utils system upgrade**.

To initiate an upgrade: **utils system upgrade initate**

This command allows you to install upgrades and Cisco Option Package (COP) files from both local and remote directories.

To cancel an upgrade: **utils system upgrade cancel**

Shutdown

To shut down Finesse: **utils system shutdown**

If the virtual hosts running the Finesse servers are also shut down during a maintenance event, to power up Finesse after the maintenance event is complete, you must sign in to the ESXi host or its vCenter with vSphere Client and power up the virtual machines for both the primary and secondary Finesse servers.

Remote Account Management

Run the following command to enable, disable, create, and check the status of a remote access account: **utils remote_account**

A remote account generates a passphrase that allows Cisco support personnel to get access to the system for the specified life of the account.

- **utils remote_account create** *account life*

  account is the account name. *life* indicates the life of the account in days.

- **utils remote_account disable**
- **utils remote_account enable**
- **utils remote_account status**

Replication Status

To check replication status, run the following command on the *primary* Finesse server:

- **utils dbreplication runtimestate**

  This command returns the replication status on both the primary and secondary Finesse servers.

- Check the RTMT counter value for replication. If all nodes in the cluster show a replication status of 2, replication is functioning correctly.
- If the RTMT counter value for replication status is 3 or 4 for all nodes in the cluster, replication is set up but an error occurred and replication is not functioning properly.
- If the majority of the nodes show a value of 0 or 1, run the command **utils dbreplication reset all** from the primary Finesse server.
- If any node shows any replication value other than 1 or 2, replication is not set up correctly.
- To fix replication, contact Cisco Technical Support.

3rdpartygadget Account

The 3rdpartygadget account is used to upload third-party gadgets to the Finesse server. Before you can use this account, you must set the password.

Note If you plan to upload third-party gadgets to the Finesse server, you must have a developer support services contract or work with a Cisco partner who has a developer support services contract. For more information about uploading third-party gadgets, see the *Cisco Finesse Web Services Developer Guide*.

To set (or reset) the 3rdpartygadget account password, access the CLI and run the following command:

utils reset_3rdpartygadget_password

You are prompted to enter a password. After you enter a password, you are prompted to confirm the password.

The password for the 3rdpartygadget account must be between 5 and 32 characters long and cannot contain spaces or double quotes (").

Note Third-party gadgets are migrated across upgrades and included in DRS backup and restore.

Configuring Queue Statistics

The Queue Statistics gadget is enabled by default as part of Cisco Finesse new installation (Unified CCE only). When performing a system upgrade from Cisco Finesse 11.5(1), the desktop custom layout needs to be modified by the administrator for the Queue Statistics gadget to be displayed on the Agent and Supervisor desktop.

Use the following CLI commands to enable and disable the queue statistics polling or check the status of the queue statistics polling:

- **utils finesse queue_statistics enable**
- **utils finesse queue_statistics disable**
- **utils finesse queue_statistics status**

After performing a system upgrade, during switch-version the queue statistics polling will be enabled by default. The procedure to disable the queue statistics polling remains the same.

Note When enabled, Queue Statistics supports a maximum of 1500 users (Agents and Supervisors).