Cisco Finesse CLI

Commands Supported for Cisco Finesse

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

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 the primary and secondary Finesse server.

Use the folloing commands to view the status of, enable, or disable Cisco Finesse HTTPS Redirect:

- **utils finesse application_https_redirect status**: This command retrieves the status of Cisco Finesse HTTPS Redirect. It 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.

- **utils finesse application_https_redirect enable**: This command enables Cisco Finesse HTTPS Redirect.

  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** .

- **utils finesse application_https_redirect disable**: This command disables Cisco Finesse HTTPS Redirect.

  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**.

Cisco Finesse Services

To view, start, or stop services:

- **show network all detail** : View the platform TCP/IP services, UDP services, and Unix domain sockets used by Cisco Finesse:
- **utils service list**: This command retrieves a list of all services and their status.

  Services are shown in one of the following states:

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.

- **utils service start** *service name*: This command starts the named service.
- **utils service stop** *service name*: This command stops the named service.
- **utils service start Cisco Finesse Tomcat**: This commans starts Cisco Finesse Tomcat.
- **utils service stop Cisco Finesse Tomcat**: This commans stops Cisco Finesse Tomcat.
- **utils service restart Cisco Finesse Tomcat**: This commans restarts 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 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.

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]**: This command enables the 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**: This command disables the Cisco Finesse toaster notification.
- **utils finesse toaster status**: This command displays the status (enable or disable) of the Cisco Finesse toaster notification.

Note Cisco Finesse Toaster Notification does not work with Internet Explorer browser.

Finesse IPPA Inactivity Timeout

Use the following CLI commands to enable or disable the Inactivity Timeout feature in Finesse IPPA. You must either disable the 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 is not logged out if on any other screen:

- **utils finesse ippa_inactivity_timeout enable**: This command enables Finesse IPPA Inactivity Timeout.

Note The default time set for inactivity timeout is 120 seconds.

- **utils finesse ippa_inactivity_timeout disable**: This command disables Finesse IPPA Inactivity Timeout.

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

- **utils finesse ippa_inactivity_timeout enable inactivity_timeout**: This command enables the 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**: This command checks the status of Finesse IPPA Inactivity Timeout.

Note The Finesse IPPA Inactivity Timeout CLIs should be run on primary and secondary Finesse servers. Enabling or disabling this 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

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).

Cross-Origin Resource Sharing (CORS)

CORS support to the third-party web server is disabled by default for Cisco Finesse and OpenFire. Use the following CLIs to enable CORS for Cisco Finesse and OpenFire and configure the allowed origin list:

Note CORS support to third-party clients is enabled for all origins by default in Cisco Finesse and OpenFire. This corresponds to the **enable_all** mode.

Important After you make changes to the CORS status or to the allowed origin list, restart Cisco Finesse Tomcat and Notification Services for the changes to take effect.

- **utils finesse cors enable**: This command allows CORS for Cisco Finesse APIs and OpenFire requests for allowed origin list. It responds to browser CORS preflight requests and allows valid domains to make Finesse API/OpenFire requests.

  Note
  - Use the **utils finesse cors allowed_origin** CLI to customize the allowed origin list.
  - Any custom headers used in the CORS requests must be added using **utils finesse cors allowed_headers** CLI.

- **utils finesse cors enable_all**: This command allows all origins to make cross domain requests. It responds and allows CORS preflight requests from any domain to make Finesse API/OpenFire requests.

  Note This isn't a secure configuration and is included only to support backward compatibility.

- **utils finesse cors disable**: This command restricts CORS for Cisco Finesse APIs and OpenFire requests. It disallows or prevents CORS preflight requests from any external domain to make Finesse API and OpenFire requests.

  Note If the allowed origin list is already present, the list is preserved and used when CORS is enabled. The CLI changes are reflected only after you clear your cache and close and reopen the browser.

- **utils finesse cors status**: This command displays the CORS status (enable_all, enabled, or disabled) on the console.

For allowing any other header, the following set of CLI commands are added to enable CORS for both Cisco Finesse and OpenFire and to configure the allowed origin list:

- **utils finesse cors allowed_origin list**: This command lists all the origins in the allowed origin list.
- **utils finesse cors allowed_origin add**: This command adds origins to the allowed origin list. Origins can be added by using a comma-separated string. For example:

  utils finesse cors allowed_origin add http://origin1.com:[port]

  utils finesse cors allowed_origin add http://origin1.com: [port], http://origin2.com:[port]

Note
- The wildcard character star (*) isn't a valid origin in the allowed origin list.
- The maximum number of characters (cumulative) that are permissible in allowed origin is 4000.

- **utils finesse cors allowed_origin delete**: This command deletes origins from the allowed origin list.

Note Delete lists all the origins in the allowed origin list. The origins can be deleted by selecting the appropriate ones from the list. For example:

utils finesse cors allowed_origin delete

1: http://google.com

2: https://www.cisco.com

3: https://def.com

4: https://abc.com:8082

a: all

q: quit

Select the index of origin(s) to be deleted [1-4 or a,q]

By default the following headers are allowed and exposed:

- **allowed_headers**: Content-Type, X-Requested-With, accept, Origin, Authorization, Access-Control-Request-Method, Access-Control-Request-Headers, requestId, Range.
- **exposed_headers**: Access-Control-Allow-Origin, Access-Control-Allow-Credentials, Access-Control-Allow-Methods, Access-Control-Allow-Headers, Access-Control-Max-Age.

Note These headers can't be modified. Custom headers can be added or removed using the following CLIs:

- **utils finesse cors allowed_headers list**: This command lists all the allowed headers for CORS. The list is used to validate incoming requests to Finesse.
- **utils finesse cors allowed_headers add**: This command adds one or more allowed headers for CORS. Multiple headers can be added as a comma-separated string. For example:
  - utils finesse cors allowed_headers add header1
  - utils finesse cors allowed_headers add header1,header2,header3

Note The wildcard character star (*) isn't supported.

- **utils finesse cors allowed_headers delete**: This command lists the choices for deleting the allowed headers. The choice should be an index as displayed in the list of allowed headers. The list provides the option to delete a single header or all configured custom headers. For example:

  utils finesse cors allowed_headers delete

  1: header1

  2: header2

  a: all

  q: quit

  Select the index of the allowed header to be deleted [1-2 or a,q]: 1

- **utils finesse cors exposed_headers list**: This command lists all the exposed headers for CORS. The list will be used by the browser to validate the accessible headers in the response.
- **utils finesse cors exposed_headers add**: This command adds one or more exposed headers for CORS. Multiple headers can be added by a comma-separated string. For example:

  utils finesse cors exposed_headers add header1

  utils finesse cors exposed_headers add header1,header2,header3

Note The wildcard character star (*) isn't supported

- **utils finesse cors exposed_headers delete**: This command lists the choices for deleting the exposed headers. The choice should be an index as displayed in the list of allowed headers. The list provides option to delete a single header or all configured custom headers. For example:

  utils finesse cors exposed_headers delete

  1: header1

  2: header2

  a: all

  q: quit

  Select the index of the exposed header to be deleted [1-2 or a,q]: 1

All CLIs are node specific and must be run on all nodes in the cluster.

Gadget Source Allowed List

Shindig proxies requests from the Finesse desktop to external servers and this introduces the possibility of server side request forgery (SSRF). To prevent SSRF, you can choose to allow outgoing connections for specified sources to be used in the gadgets by adding URLs to the allowed list. Note that this functionality is disabled by default for Cisco Finesse.

Use the following CLIs to enable or disable Gadget Source allowed list functionality and to configure source(s) in the allowed list:

- **utils finesse gadget_source_check enable**: This command enables allowed list for Cisco Finesse.
- **utils finesse gadget_source_check disable**: This command disables allowed list for Cisco Finesse.
- **utils finesse gadget_source_check status**: This command prints the allowed list status (enabled or disabled) on Cisco Finesse console.
- **utils finesse gadget_source_check whitelist list**: This command lists all the source(s) in the allowed list.
- **utils finesse gadget_source_check whitelist add**: This command adds source(s) to the allowed list. For example,
  - **utils finesse gadget_source_check whitelist add** https://www.abc.com:8445.
  - **utils finesse gadget_source_check whitelist add** https://www.abc.com:8445, http://www.abc.com.

Note Wildcard character * is not supported.

The allowed list feature does not perform hostname resolutions. The format of the allowed list entry should match the format in which the gadget requests for a resource.

If **utils finesse gadget_source_check** is enabled, you must add the CUIC URLs to **utils finesse gadget_source_check allowed_list** for the stock gadgets to load. For example,

- utils finesse gadget_source_check enable
- utils finesse gadget_source_check allowed_list add https://<CUIC_Pub_FQDN>
- utils finesse gadget_source_check allowed_list add https://<CUIC_Pub_FQDN>:8444
- utils finesse gadget_source_check allowed_list add https://<CUIC_Sub_FQDN>
- utils finesse gadget_source_check allowed_list add https://<CUIC_Sub_FQDN>:8444

If you do not add the CUIC URLs, Finesse Desktop fails to load and an appropriate error message is displayed.

- **utils finesse gadget_source_check whitelist delete**: This command deletes source(s) from the allowed list. For example:
  - **utils finesse gadget_source_check whitelist delete**

- 1: http://origin1:8080
- 2: https://origin2:8082
- a: all
- q: quit

Select the index of origin to be deleted [1-2 or a,q]: 1

Note All CLIs are node-specific and must be run on all nodes in the cluster.

After any changes are done to gadget source status or to the allowed list, restart Cisco Finesse Tomcat for changes to take effect.

Supported Content Security Policy Directives

Note To enable this feature in Cisco Finesse, install Finesse 12.0(1) ES4 COP or higher.

Content Security Policy (CSP) is a standardized set of security directives that can inform the browser of the policies to be used to help mitigate various forms of attacks. CSP frame-ancestor policy defines the allowable locations from where the Finesse desktop can be accessed as an embedded HTML content, which can help prevent click-jacking attacks.

Use the following CLI commands to view, add, or delete the frame-access sources in the response header of Cisco Finesse. This ensures that only the configured sources can embed the Cisco Finesse in an iFrame within their HTML pages.

Note Internet Explorer does not support frame-ancestors, and therefore will not block any websites from loading Cisco Finesse within it.

- **utils finesse frame_access_whitelist add** *[source1,source2]*—This command adds one or more frame sources, thereby allowing the configured sources to embed the Cisco Finesse in their iFrames. Multiple sources can be provided as a comma-separated list. The source should be of the following format:
  - https://<fqdn>:[port]
  - https://IP:[port]
  - https://<fqdn1>:port, https://<fqdn2>:port

Note

- Wildcard character * is also supported for the FQDN and port entries, which indicates that all the legal FQDN or ports are valid.
- The maximum number of characters (cumulative) that are permissible in allowed list is 2000.

```
admin:utils finesse frame_access_whitelist add
https://www.abc.com:8445,https://*.abc.com,https://*.abc.com:*,https://10.21.255.25

Source(s) successfully added.
Ensure Source(s) is added to the frame access list in all Finesse nodes in the cluster.

Restart Cisco Finesse Tomcat and Cisco Finesse Notification Service for the changes to
 take effect:
utils service restart Cisco Finesse Tomcat
utils service restart Cisco Finesse Notification Service
```

- **utils finesse frame_access_whitelist delete**—This command displays an indexed list of all the configured frame sources that have been allowed to access Cisco Finesse. Enter the corresponding index number to delete a single source or all the configured sources.

```
admin:utils finesse frame_access_whitelist delete

1: https://www.abc.com:8445
2: https://*.abc.com
3: https://*.abc.com:*
4: https://10.21.255.25
a: all
q: quit

Select the index of source to be deleted [1-4 or a,q]: 1
Sources deleted successfully.

Restart Cisco Finesse Tomcat and Cisco Finesse Notification Service for the changes to
 take effect:
 utils service restart Cisco Finesse Tomcat
 utils service restart Cisco Finesse Notification Service
```

- **utils finesse frame_access_whitelist list**—This command lists all the frame sources that are allowed to access Cisco Finesse.

```
admin:utils finesse frame_access_whitelist list

The following source(s) are configured in the frame access list:
1: https://www.abc.com:8445
2: https://*.abc.com
3: https://*.abc.com:*
4: https://10.21.255.25
```

Finesse System Commands

Configure the following Cisco Finesse system CLIs:

Notifications

Use the following CLI commands to enable or disable the Cisco Finesse notifications. By default, this feature is disabled.

- To enable: **utils finesse notification logging enable**
- To disable: **utils finesse notification logging disable**

Node Statistics

Use the following CLI command to view the run-time statistics for the current node.

- To view: **utils finesse node_statistics list**

```
admin:utils finesse node_statistics list

Warning: Running this command frequently will affect system performance.
Press ENTER to continue. Press any other key to exit :

Wait while the statistics (updated every 5 secs) are being fetched...

The following are the runtime statistics for the current node.

Active Dialogs Count: 0

Active Tasks Count: 0

Average Configured Media per Agent Count: 0

Average Logged in Media per Agent Count: 0

Average Skill Groups per Agent Count: 0

Max Skill Groups per Agent Count: 0

Total Time for Finesse to Start (in seconds): 32

Logged in Agents on current node: 0

Unique Configured Skill Groups per Agent Count: 0
```

For more information, see *RuntimeConfigInfo API Parameters* section in the *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/docs/finesse/.

Desktop Properties

Configure the desktop properties using the following CLIs for the features:

Active Call Details in the Team Performance Gadget

Use the following CLI commands to enable or disable the active call details.

- To enable: **utils finesse set_property desktop showActiveCallDetails true**
- To disable: **utils finesse set_property desktop showActiveCallDetails false**

View History in the Team Performance Gadget

Use the following CLI commands to enable or disable the agent history.

- To enable: **utils finesse set_property desktop showAgentHistoryGadgets true**

- To disable: **utils finesse set_property desktop showAgentHistoryGadgets false**

Force Wrap-Up Reason

Use the following CLI commands to enable or disable the force wrap-up reason.

- To enable: **utils finesse set_property desktop forceWrapUp true**
- To disable: **utils finesse set_property desktop forceWrapUp false**

Show Wrap-Up Timer

Use the following CLI commands to show or hide the timer in wrap-up state. By default the showWrapUpTimer property is set to true.

- To hide the timer in wrap-up state:**utils finesse set_property desktop showWrapUpTimer false**
- To display the timer in wrap-up state: **utils finesse set_property desktop showWrapUpTimer true**

Wrap-Up Timer Count Down

Use the following CLI commands to set the wrap-up timer to count down or count up the time. By default the wrapUpCountDown property is set to true.

- To count up the time:**utils finesse set_property desktop wrapUpCountDown false**
- To count down the time: **utils finesse set_property desktop wrapUpCountDown true**

Notification Connection Type

Use the following CLI commands to update the desktop notification connection type as WebSockets or BOSH. By default the connection type is WebSockets.

- For WebSockets: **utils finesse set_property desktop notificationConnectionType websocket**
- For BOSH: **utils finesse set_property desktop notificationConnectionType bosh**

Desktop Chat Attachment

Use the following CLI commands to enable or disable the attachment support in Desktop Chat. Attachments are enabled by default in Desktop Chat.

- To enable: **utils finesse set_property desktop desktopChatAttachmentEnabled true**
- To disable: **utils finesse set_property desktop desktopChatAttachmentEnabled false**

Desktop Chat Maximum Attachment Size

Use the following CLI commands to configure the attachment size in Desktop Chat. If you do not configure the maximum attachment size, then it is set to 5 MB by default.

- **utils finesse set_property desktop desktopChatMaxAttachmentSize** *Attachment Size*

  For example, to set the maximum attachment size to 2 MB, use:

  utils finesse set_property desktop desktopChatMaxAttachmentSize 2097152

Note The maximum attachment size configurable is up to 10 MB.

Desktop Chat Unsupported File Types

The .exe, .msi, .sh, and .bat file types are not supported by default. Use the following CLI commands to override the default list and customize the file types that will not be supported in the Desktop Chat. Multiple file types can be added using a comma separated string.

- **utils finesse set_property desktop desktopChatUnsupportedFileTypes** *File Types*

  For example, to set the .jar and .bin as unsupported file types, use:

  utils finesse set_property desktop desktopChatUnsupportedFileTypes jar,bin

Configure Desktop Chat Organization Unit (OU) Search

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

Use the following CLI commands to configure the OU based user search for the base LDAP context for desktop chat in HCS for CC. By default, the whole LDAP base context is configured in Cisco Unified Communications Manager IM and Presence Service LDAP search settings. For more details on desktop search see, *Desktop Chat Server Settings*.

To set field key: **utils finesse set_property desktop desktopChatOUSearchFieldKey** *<value>*

To set field value: **utils finesse set_property desktop desktopChatOUSearchFieldValue** *<value>*

The following example displays the search criteria set for chat users who belong to specific OU.

```
admin:utils finesse set_property desktop desktopChatOUSearchFieldKey "OU"

Property successfully updated.
Ensure property is updated in all Finesse nodes in the cluster.

No service restart required. Ensure browser is refreshed for the changes to take effect.

admin:utils finesse set_property desktop desktopChatOUSearchFieldValue "chat"

Property successfully updated.
Ensure property is updated in all Finesse nodes in the cluster.

No service restart required. Ensure browser is refreshed for the changes to take effect.
```

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**.

utils system upgrade initate: This command allows you to initiate and install upgrades and Cisco Option Package (COP) files from both local and remote directories.

utils system upgrade cancel: This command allows you to cancel an upgrade.

Shutdown

Use the following command 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 primary and secondary Finesse servers.

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 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.

View Property

Use the following CLIs to view the property values across all property files.

- **utils finesse show_property fippa property_name**: To view the specified Finesse IPPA property's value.
- **utils finesse show_property desktop property_name**: To view the specified desktop property's value.
- **utils finesse show_property webservices property_name**: To view the specified web service property's value.

Note The View property CLIs do not support multiple values.

Update Property

Use the following CLIs to update the property values across all property files.

- **utils finesse set_property desktop property_name property_value**: To update an existing property value used by the Finesse desktop service.
- **utils finesse set_property fippa property_name property_value**: To update an existing property value used by the Finesse IPPA service.
- **utils finesse set_property webservices property_name property_value**: To update an existing property value used by the Finesse web service.

Signout from Media Channels

The CLI **utils finesse user_signout_channel** is used by the Administrator to configure the media channels from which the users are signed out.

When signing out from Cisco Finesse, the CLI **utils finesse user_signout_channel type** lists all the choices of media channels from which the user is signed out. For example:

utils finesse user_signout_channel type

1: signout user from voice channel.

2: signout user from voice and non-voice media channels configured for Cisco Finesse.

a: signout from all media channels configured for the user.

Note This is default behavior. It is suitable if the non-voice media is running as a gadget within Finesse Desktop and hence, it is valid to assume that the desktop user cannot handle tasks when signing out of Finesse.

q: quit.

Select the choice of media [1-2 or a,q]: 2

User signout channel type is now changed to "signout user from voice and non-voice media channels configured for Cisco Finesse."

Note **user_signout_channel type** must be updated for all Cisco Finesse nodes in the cluster.

For any changes done to media channels, it will take fifteen minutes for the new media channels signout to take effect.

The CLI **utils finesse user_signout_channel status** displays the type of media channels from which the user is signed out.