Cisco Finesse

Note A new Service Update (SU) release is available for Cisco Finesse 12.5(1). You can perform a fresh installation or upgrade to Cisco Finesse 12.5(1) SU on supported virtual machines from previous versions. For more information, see the ReadMe.

New Features

Edge Chromium Browser Support

This release supports Edge Chromium (Microsoft Edge). For information about supported versions, see the *Contact Center Enterprise Solution Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Improvements to Finesse Failover

This release optimizes the Cisco Finesse CTI failover and Desktop failover performances.

- CTI Failover—When deployed with Agent PG 12.5(1), CTI server/Agent PG failover varies approximately from 35 seconds to 75 seconds. When deployed with Agent PG 12.0(1) or 11.6(1), CTI server/Agent PG failover varies approximately from 75 seconds to 120 seconds.
- Desktop Failover—When deployed with Agent PG 12.5(1), desktop failover with the default desktop layout varies approximately from 50 seconds to 110 seconds. When deployed with Agent PG 12.0(1) or 11.6(1), desktop failover is approximately 40 seconds more when compared to Agent PG 12.5(1).

When OVA with 8 vCPUs is configured for Cisco Finesse, the time taken for CTI server/Agent PG failover and desktop failover improves by 20 percent. This configuration is supported on all deployment types including the 24000 Agent deployment type. For more information on OVA with 8 vCPUs, see *Virtualization for Cisco Finesse* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-finesse.html.

The total failover time varies depending on the WAN bandwidth, the number of signed-in users, network latency, number of vCPUs configured, Agent PG version, and the number of gadgets configured on the Finesse desktop. Most of the desktop failover improvements (as opposed to CTI failover) are also available with earlier versions of the Agent PG.

For more information on deployment practices and guidelines to ensure optimal failover performance, see *Guidelines for Optimal Desktop Failover* and *Failover Planning* sections in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

For more information on ensuring how the custom gadgets improve failover performance, see *Best Practices for Gadget Development* section in *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

Desktop Performance Improvements

This release optimizes the Finesse desktop performance in the following areas:

- Uses HTTP/2 by default for loading resources. This provides significant improvement when starting up the desktop compared to the older HTTP 1.1.
- Consumes significantly lesser desktop bandwidth when reloading the Finesse desktop (without gadgets) from the cache.
- Uses fewer requests for loading resources.
- Serves static resources much faster using client-side resource caching.
- Provides cached REST responses at a team-level for configuration data to improve the desktop loading.
- Improves gadget loading by caching the gadget definitions.

Finesse Server Performance Improvements

This release optimizes the Finesse server performance in the following areas.

- Significantly reduces the average CPU consumption while the server is under load.
- Optimizes the server performance by avoiding dynamic server pages, using SSL termination, faster CTI message parsing, and cached static resources.
- Provides access to more memory and reduces GC latencies as the Cisco Finesse server uses 64-bit Java 8.
- Optimizes CTI request processing to reduce the latencies in sending requests to the server.
- Reduces overall latencies for CTI communication.

Keyboard Shortcuts

This release provides keyboard shortcuts for easy access to the Finesse desktop features. The keyboard shortcuts define an alternate way to perform a specific action on the Finesse agent and supervisor desktop. The administrator can set the **utils finesse set_property desktop enableShortCutKeys** to *true* to enable this feature.

For more information, see *Access Keyboard Shortcuts* section in *Cisco Finesse Agent and Supervisor Desktop User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html.

Desktop Chat Search

This release allows you to refine the desktop chat search to display the user details based on the Organization Unit (OU) defined in Cisco Unified Communications Manager IM and Presence Service. The administrator can use the following CLIs to configure the OU-based user search in Cisco Finesse.

- **utils finesse set_property desktop desktopChatOUSearchFieldKey** <*value*>
- **utils finesse set_property desktop desktopChatOUSearchFieldValue** <*value*>

For more information, see *Desktop Chat Server Settings* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Edit Call Variables

This release allows agents and supervisors to edit the call variable values from the Finesse desktop. The administrator can configure any of the callVariable values, including ECC variables as editable. The agent and the supervisor can edit the call variable values during an active call or in the wrap-up state.

Note Call variables edit operation updates the values of the variables within the particular call. All entities listening to dialog events receive the updated call variables through the Cisco Finesse notifications. If any CTI clients are connected to the same Agent PG, they also receive notifications of the changed call data though CTI call events. However, application scripts or databases that are used to populate the call variables are not directly affected by this edit.

For more information, see *Edit Call Variables* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html and *Cisco Finesse Agent and Supervisor Desktop User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html.

Drag-and-Drop and Resize Gadget or Component

This release allows agents and supervisors to drag-and-drop or resize the gadgets or components in the Finesse desktop. The administrator can customize the desktop property value of these features through the desktop layout:

- Default layout (**Desktop Layout**)
- Team-specific layouts (**Manage Team Resources** > **Desktop Layout**)

Alternatively, the administrator can also set the **utils finesse set_property desktop enableDragDropAndResizeGadget** to *true* to enable these features.

For more information, see *Drag-and-Drop and Resize Gadget or Component* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Gadget Expand and Collapse

This release supports to expand and collapse of gadgets dynamically in the Finesse desktop to optimize available screen space.

For more information, see *Container Services* section in JavaScript Library at https://developer.cisco.com/docs/finesse/#!javascript-library.

Desktop Layout Editors

This release provides two types of editors in the **Desktop Layout** and **Team Resources** of the Cisco Finesse administration console.

- **Text Editor**—A plain text editor. It is the default editor. Use the **Expand All** option to see all the code details and **Search** box to refine results.
- **XML Editor**—An XML editor. The administrator cannot add or edit comments (<!-- -->) in this editor.

For more information, see *Default Layout XML* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Customize Desktop Properties

This release allows the administrator to customize the desktop properties for individual Teams through the desktop layout using the following layouts:

- Default layout (**Desktop Layout**)
- Team-specific layouts (**Manage Team Resources** > **Desktop Layout**)

For more information, see *Customize Desktop Properties* and *Customize Desktop Properties at Team Level* sections in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Configuration for Cloud Connect

This release allows the administrator to configure the Cloud Connect server settings in the Finesse administration console to contact the Cisco Cloud Services, such as Cisco Webex Experience Management.

For more information, see *Cloud Connect Server Settings* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

WebProxy Service

This release introduces WebProxy Service within the Finesse server to provide SSL termination and caching services to the Finesse service to reduce latency and improve performance. For more information, see *WebProxy Service* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Gadget developers must bypass the proxy to access the updated gadget responses for testing purposes. For more information, see *Best Practices for Gadget Development* section in *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

Security Banner Message

This release provides custom banner messages in the administrator and desktop Sign In pages. The administrator can use the following CLIs to define the custom security banner message.

- **utils finesse set_property desktop desktopSecurityBannerMessage** <*value*>
- **utils finesse set_property admin adminSecurityBannerMessage** <*value*>

For more information, see *Desktop Properties* and *Service Properties* sections in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Automatic Desktop Login Retries

This release supports automatic desktop login retries when the desktop login fails due to device-related errors. The administrator can use the following CLIs to enable, define the number of attempts and intervals in seconds for the retry login mechanism. By default, the value of this property is set to true.

- **utils finesse set_property desktop enableRetryLoginFeature** {*true*|*false*}
- **utils finesse set_property desktop loginFailureRetryAttempts** <*value*>
- **utils finesse set_property desktop loginFailureRetryInterval** <*value*>

For more information, see *Desktop Properties* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Finesse IP Phone Agent Certificate Management

This release requires HTTPS for Finesse IP Phone Agent (IPPA) to address the security vulnerabilities across the solutions. The administrator must ensure to import the following certificates and configuration changes to use the FIPPA functionality.

- Import the Cisco Unified Communications Manager (CUCM) certificate to the trust store as **tomcat-trust**.
- Import the Cisco Finesse certificate to the CUCM trust store as **Phone-trust**.

For more information, see *Finesse IP Phone Agent Certificate Management* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

HTTP Secure Support

This release supports only HTTP Secure (HTTPS). Support for HTTP is disabled for the administration console, desktop (agent and supervisor), Web Services, Desktop Modules (gadgets), and Finesse IPPA. All the HTTP requests are automatically redirected to HTTPS.

For HTTPS access, enter: `https://FQDN of Finesse server:8445/`

For more information on disabled ports, see Cisco Finesse Important Notes, on page 11.

HTTP/2 Support

This release supports HTTP/2 protocol by default.

Enhanced Log Collection

3rdpartygadget Log Directory

This release provides the 3rdpartygadget log directory, which contains information, error, startup, and shutdown-related logs for the Finesse 3rdpartygadget server.

WebProxy Service Logs

The administrator can use the **file get activelog webproxy recurs compress** CLI to obtain logs for the WebProxy Service.

For more information, see *Log Collection* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Automatic Log Collection for Desktop Users

The administrator can use the following CLI to create, list, and delete automatic desktop log collection schedules for agents and supervisors.

utils finesse desktop_auto_log_collection {*create*|*list*|*delete*}

For more information, see *Log Collection Schedule* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Set Commands

The following CLIs have been introduced in this release:

Call Variables Logging

The administrator can use the following CLIs to enable or disable the call variables logging.

- **utils finesse set_property webservices logCallVariables** {*true*|*false*}
- **utils finesse set_property fippa logCallVariables** {*true*|*false*}

Enforcement of X.509 Certificate Trust Validation

The administrator can set the **utils finesse set_property webservices trustAllCertificates** to *false* to enable the validation of the X.509 CA or the self-signed certificate.

Mobile Agent

The administrator can set the **utils finesse set_property desktop enableMobileAgentLogin** to *true* to enable Sign in as a Mobile Agent feature on the Finesse desktop Sign In page.

Preloading of the Secondary Resources

The administrator can set the **utils finesse set_property desktop preLoadSecondaryResources** to *true* to enable the preloading of static resources from the secondary server to ensure faster failover.

XMPP Socket and BOSH/WebSocket (HTTP)

The administrator can set the **utils finesse set_property webservices enableInsecureOpenfirePort** to *true* to enable the Cisco Finesse Notification Service unsecure XMPP port (5222) and HTTP-BOSH/WebSocket port (7071).

Update Cisco Unified Intelligence Center Gadget URL

JSP format for Cisco Unified Intelligence Center gadgets is not supported. To change the JSP format references to the XML format, the administrator can run the CLI **utils finesse layoutupdateCuicGadgetUrl** on the Finesse server.

User Authentication Discovery API

The administrator can set the **utils finesse set_property webservices enableUserAuthMode** to *true* to enable the `UserAuthMode` API.

For more information, see *User APIs* section in *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/.

WORK Mode Retention for Non-Voice

The administrator can set the **utils finesse set_property desktop enableAutoWorkModeStateChange** to *false* to enable the agent to retain WORK mode after CTI reconnection (non-voice).

For more information, see *Cisco Finesse Failover Mechanisms* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

WebProxy Service

The administrator can use the following CLIs to clear, set access log-level and log-severity for the logs that are generated by the WebProxy Service.

- **utils webproxy cache clear**
- **set webproxy access-log-level**
- **set webproxy log-severity**
- **show webproxy access-log-level**

- **show webproxy log-severity**

For more information, see *Cisco Finesse CLI* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

REST APIs

The following APIs have been introduced in this release:

- CompressedClientLog—Post Compressed Log to Finesse
- Cloud Connect Configuration—Get
- Cloud Connect Configuration—Set
- Cloud Connect Integration—Delete
- ECCVariableConfig—Get ECC Variable Configuration
- Media—Change Agent from Work State to Active
- Single Sign-On—Get User Authentication Mode
- TeamResource—Get Reason Codes
- TeamResource—Get Wrap-Up Reasons
- TeamResource—Get Media Properties Layouts
- TeamResource—Get Phone Books
- TeamResource—Get Workflows
- User—Get User Id from loginName

REST API Response Caching

In order to improve login performance, the Finesse webproxy caches the following REST API responses:

- ChatConfig
- ECCVariableConfig
- MediaDomain
- TeamResource APIs include Reason Codes, Wrap-Up Reasons, Media Properties Layouts, Phone Books, and Workflows. The responses of the TeamResource API are cached at the team-level.

For more information, see *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

JavaScript APIs

The following APIs have been introduced in this release:

- finesse.shortcutkey.ShortcutKeyService

- finesse.utilities.DesktopCache

For more information, see *JavaScript Library* at https://developer.cisco.com/docs/finesse/#!javascript-library.

Updated Features

None.

Security Enhancements

This release implements the following security changes:

- By default, Cisco Finesse Notification Service unsecure XMPP port 5222 and BOSH/WebSocket (HTTP) port 7071 are disabled.

  For more information on enabling the ports, see *Service Properties* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

- Validation of the X.509 certificate is enforced. It is mandatory to have the following valid non-expired X.509 CA or self-signed certificates, which must be imported into the Cisco Finesse trust store.
  - Cisco Finesse node certificates are available by default. The administrator must verify the validity of the certificates, as non-expired certificates are invalid.
    - Valid non-expired Cisco Finesse primary certificate must be present on the secondary Cisco Finesse.
    - Valid non-expired Cisco Finesse secondary certificate must be present on the primary Cisco Finesse.
  - Import the CUCM certificate to both the primary and secondary Finesse nodes.
  - Import the IdS certificate to both the primary and secondary Finesse nodes.
  - Import the Customer Collaboration Platform server certificates to both the primary and secondary Finesse nodes in Unified CCE.
  - Import the LiveData server certificates to both the primary and secondary Finesse nodes in Unified CCE.
  - Import the Cloud Connect server certificates to both the primary and secondary Finesse nodes in the Unified CCE.

For more information, see *Security Enhancements* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Failure Message for Login

This release displays detailed error messages corresponding to login failures on the Finesse desktop. This allows the administrator to respond to client login failures without referring to the logs.

The error messages are updated for both UI and API.

- The Finesse desktop UI is updated to include the 2nd Level Text error messages provided by CTI operations for sign-in scenarios.

  Peripheral error codes 12004 and 12005 are replaced with desktop sign-in retries. When the sign-in retry fails, it displays the 2nd Level Text error messages provided by CTI operations.

- The Cisco Finesse API payloads are updated to include the peripheral error codes and 2nd Level Text error messages provided by CTI operations. The newly added parameters are:
  - peripheralErrorCode
  - peripheralErrorMsg
  - peripheralErrorText

For more information, see *Cisco Finesse API Errors* section in *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

Example

13036 PERERR_GW_E_JTAPIOBJ_PERFORMANSWERCALL_NO_TERMINAL_CONNECTION

```
1st Level Text = 'JTAPI Gateway - Error on ANSWER operation'
2nd Level Text = 'The routine performAnswerCall in class JTapiObj got a null connection
from a call to 'findTerminalConnection'
```

Prevent Non-Voice Task RONAs during CTI Reconnect

This release provides `Media—Change Agent from Work State to Active` API to signal the availability of media channels explicitly, after CTI reconnection. This can significantly reduce RONAs, since tasks are not routed to the agent until the agent is available in the non-voice MRD.

The CLI command **utils finesse set_property desktop enableAutoWorkModeStateChange** is introduced to enable or disable the feature.

For more information, see *CTI Failover* and *Desktop Properties* sections in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

For more information, see *Media APIs* section in *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

Team Performance Gadget

In the Team Performance gadget, supervisors can use the **Search** box to refine any agent details by using the search criteria such as Agent Name, State, or Extension.

Queue Statistics Support

The maximum number of agents and supervisors that are supported in Queue Statistics is increased from 1500 to 2000.

Phone Book Contact Limit

The maximum number of contacts per agent across all phone books is increased from 1500 to 6000.

Changes in REST APIs

The following payloads are updated:

- MediaPropertiesLayout APIs—The `uiEditable` payload indicates if the call variable values can be edited in the Finesse desktop (agent and supervisor).

Dialog—Create a New Dialog (Make a Call)

The `MAKE_CALL` API is updated to make a call from Ready state. When an agent goes off-hook to place a call, the Unified CCE changes the agent status to Not Ready with 50006 reason code.

Login Name Support

The `User—Get User Id from loginName` API is updated to accept the **`loginName`** in URI and authentication for both SSO and non-SSO deployments.

Phone Book Contact Limit

The maximum number of contacts per agent is increased from 1500 to 6000 in the `Phone Book` and `Contact` APIs.

For more information, see *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

Changes in JavaScript APIs

The following functions are updated:

- ContainerServices—The `collapseMyGadget` and `expandMyGadget` functions, that hide and display the gadget contents respectively.
- DialogBase—The `updateCallVariables` function updates the dialog's call variables.

For more information, see *JavaScript Library* at https://developer.cisco.com/docs/finesse/#!javascript-library.

Important Notes

Deprecated Features

GET APIs

The following GET User APIs are deprecated. These APIs are available for backward compatibility and have lower performance compared to the TeamResouce APIs.

- ReasonCode
- WrapUpReason
- MediaPropertiesLayout
- PhoneBook
- WorkFlow

Internet Explorer 11

In this release, Internet Explorer version 11 is deprecated. Edge Chromium (Microsoft Edge v79 and later) is the replacement. For more information, see the *Contact Center Express Solution Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html

Notifications over BOSH (Long Polling)

In this release, support for notifications over BOSH (long polling) is deprecated. Notifications over direct XMPP (over TCP) and Websocket-based transports are the replacements.

Removed and Unsupported Features

Context Service Management

The Context Service Management feature is removed from the Cisco Finesse administration console.

HTTP Support

The HTTP support for Cisco Finesse is removed. You can now securely communicate to Cisco Finesse over HTTPS.

The following CLIs are removed:

- **utils finesse application_https_redirect status**
- **utils finesse application_https_redirect enable**
- **utils finesse application_https_redirect disable**

Third Party Software Impacts

None.