



Cisco Finesse

- [New Features, on page 1](#)
- [Updated Features, on page 2](#)
- [Deprecated Features, on page 3](#)
- [Removed and Unsupported Features, on page 3](#)
- [Third-Party Software Impacts, on page 3](#)

New Features

The following sections describe new features that are pertinent to Cisco Finesse Release 11.5(1).

Toaster Notifications

In Cisco Finesse 11.5, on first login to the Cisco Finesse Desktop, you are prompted to set your preference for notifications. Choose the option to always receive or allow toaster notifications.

Team Performance Gadget Height

In this release of Cisco Finesse, Admin is enabled to resize the team performance gadget height based on the number of agents. Admin can specify the height of the team performance gadget in the desktop layout XML file.

Single Sign-On

Single Sign-On (SSO) is an authentication process. SSO allows users to sign in to one application and then securely access other authorized applications without a prompt to resupply user credentials. SSO permits Cisco supervisors or agents to sign on only once with a username and password to gain access to all of their Cisco browser-based applications and services within a single browser instance. By using SSO, Cisco administrators can manage all users from a common user directory and enforce password policies for all users consistently.



Note SSO is an optional feature. The implementation requires you to use only HTTPS protocol to access all the web applications. The HTTP access to web applications is not supported when the SSO is enabled.

You can choose from different Single Sign-On modes when deciding about implementing Single Sign-On:

- **SSO** - Enable *all* agents and supervisors in the deployment for SSO.
- **Non-SSO** - Use existing Active Directory-based and local authentication.

SSO supports agents and supervisors as follows:

- **Agents** - Includes Cisco Finesse and Cisco Finesse-hosted gadgets.
- **Supervisors** - Includes Cisco Finesse, Cisco Unified Intelligence Center (CUIC) by using Unified CCX Web Administration.

Integrate Third-Party Applications with Single Sign-On

Third-party developers can enable their gadgets and certain Java applications for Single Sign-On by using the IdSClient SDK, which also includes a Javascript library.

Chrome Support

Cisco Finesse Release 11.5(1) now supports Chrome browser for Agents, Supervisors and Administrators.

Operating System	Chrome Version
Windows 7	Chrome (version 48 or later)
Windows 10	Chrome (version 48 or later)
Mac OS X	Chrome (version 48 or later)

SHA-256 Support

Support for SSL certificates signed with SHA-256 in Cisco Finesse is now default in 11.5(1).

New Languages Support

Finesse desktop supports the following new languages from this release onward, Bulgarian, Catalan, Czech, Croatian, Hungarian, Slovak, Slovenian, Serbian, and Romanian.



Note An exception error is encountered when you view the following live data reports, Agent CSQ Statistics Report, Agent State Log Report, Chat Agent Statistics Report, and Email Agent Statistics Report in the above mentioned new languages. You may click **X** to close the error dialog box and proceed further.

Updated Features

This release has no updated features.

Deprecated Features

This release has no deprecated features.

Removed and Unsupported Features

This release has no removed or unsupported features.

Third-Party Software Impacts

CORS Support for Finesse REST API

Cross-Origin Resource Sharing (CORS) is now supported when third-party web applications instantiated from a third-party web server need to make calls to the Finesse Desktop. Finesse REST APIs can be directly invoked with an additional HTTP Request Header "Origin" that specifies the origin domain of the HTTP request. For more information, see *Cisco Finesse Web Services Developer Guide Release* .

Import Finesse JS API

All 3rd party gadget developers must load finesse.js dynamically. For gadgets to work properly, import the Finesse JS library hosted on the finesse server. Note that if the latest JS library is not imported, gadgets will not work in the especially in the Single-Sign-On mode. For more information, see the *Cisco Finesse Web Services Developer Guide*.

TLS 1.2 Support

For gadget development in Finesse 11.5, Finesse server and client connections support TLS 1.2 by default. Earlier versions are not supported.

