Manage Security

HTTPS Support

Cisco Finesse supports only Secure HTTP (HTTPS). HTTP is permanently disabled. If you access Finesse using HTTP (unsecure port: 80 or 8082), then the 301 HTTP redirect status response is issued to the secure port 8445.

Note Cisco Finesse supports HTTP/2 protocol by default.

To access the administration console using HTTPS, enter the following URL in your browser:

`https://FQDN:8445/cfadmin`

Where FQDN is the name of your primary Finesse server and 8445 is the port number.

Similarly, agents and supervisors can access their desktops using HTTPS as follows:

`https://FQDN:8445/desktop`

To eliminate browser security warnings each time you access the administration console or agent desktop through HTTPS, you can obtain and upload a CA certificate or you can use the self-signed certificate that is provided with Finesse.

If you add custom gadgets that perform HTTPS requests to Finesse, you must add a certificate to the Finesse server for that gadget.

HSTS

Finesse supports HTTP Strict Transport Security (HSTS) for increased security. HSTS is automatically enabled, in which case the Finesse server sends HTTPS responses indicating to browsers that Finesse can only be accessed using HTTPS. If users then try to access Finesse using HTTP instead of HTTPS, the browser changes

the connection to HTTPS before generating any network traffic. This functionality prevents browsers from sending requests to Finesse using unencrypted HTTP before the server can redirect them.

Reset Security or Admin Password

If you need to reset the security or admin password, you must perform the following steps on the console of the system using VSphere. You cannot ssh to the system to run the command.

Procedure

Step 1 Sign in to the platform window with the following username and password:

pwrecovery/pwreset

The following messages appear:

Welcome to Platform password reset.

Admin and Security password reset are possible.

Press any key when ready.

Step 2 Press any key to continue.

The following messages appear:

If you have a CD or DVD in the disk drive, remove it now.

Press any key to continue.

Step 3 If there is a disk in the disk drive, remove it. When you are ready, press any key to continue.

The system checks to ensure that you have removed the disk from the drive.

The following message appears:

Insert a valid CD or DVD into the disk drive.

Step 4 Connect the CD/DVD drive and point it to the ISO image.

The system checks to ensure you have inserted the disk.

After the system verifies that you have inserted a disk, you are prompted to choose one of the following options:

Enter 'a' for admin password reset.

Enter 's' for security password reset.

Enter 'q' for quit.

Step 5 Select the appropriate option and provide the new password.

The system resets the password.

Cross-Origin Resource Sharing (CORS)

Finesse supports CORS requests and allows the customization of the domains which are allowed to make CORS requests to the Finesse desktop. Once CORS is enabled via the CLI **utils finesse cors enable**, the CORS origin request from external domains is blocked by the browser. To enable specific domains to access Finesse desktop via CORS, the domains need to be added to the CORS origin allowed list using the CLI **utils finesse cors allowed_origin add**. For more information on the CORS CLIs, see *Cisco Finesse CLI*.

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 restrict outgoing connections requested by the gadgets to specific URIs by enabling shindig allowed list CLIs and adding the required URIs to the allowed list. For more information on Gadget Source Allowed List CLIs, see *Cisco Finesse CLIs*.

Security Enhancements

The security enhancements in Cisco Finesse are as follows:

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

  Use the CLI command **utils finesse set_property webservices enableInsecureOpenfirePort true** to enable these ports.

- 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 the Unified CCE.
  - Import the LiveData server certificates to both the primary and secondary Finesse nodes in the Unified CCE.
  - Import the Cloud Connect server certificates to both the primary and secondary Finesse nodes in the Unified CCE.

You can override the trust certificate enforcement by using the CLI command **utils finesse set_property webservices trustAllCertificates true**.

For more information on CLI commands, see *Service Properties*.