Manage Security

HTTP and HTTPS Support

The Cisco Finesse administration console and agent desktop support both HTTP and secure HTTP (HTTPS). 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.

To access the administration console using HTTP, enter the following URL:

http://*FQDN*/cfadmin

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

- http://*FQDN*/desktop
- https://*FQDN:8445*/desktop

For HTTPS access, you can eliminate browser security warnings by choosing to trust the self-signed certificate provided with Finesse or uploading a CA certificate.

By default, HTTPS access is enabled. You can run the Cisco Finesse HTTPS Redirect CLI command to disable HTTPS and allow HTTP access for the Finesse administration console and the agent desktop.

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

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**.

HSTS

Finesse supports HTTP Strict Transport Security (HSTS) for increased security. HSTS is automatically enabled when you enable HTTPS Redirect, 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, 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*.