Certificates for Live Data

Certificates and Secure Communications

For secure Cisco Finesse, Cisco Unified Intelligence Center, and Live Data server-to-server communication, perform any of the following:

- Use the self-signed certificates provided with Live Data.

> **Note** When using self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

- Obtain and install a Certification Authority (CA) certificate from a third-party vendor.
- Produce a Certification Authority (CA) certificate internally.

Obtain and Upload Third-party CA Certificate

You can use a Certification Authority (CA) certificate provided by a third-party vendor to establish an HTTPS connection between the Live Data, Cisco Finesse, and Cisco Unified Intelligence Center servers.

To use third-party CA certificates:

- From the Live Data servers, generate and download a Certificate Signing Requests (CSR).
- Obtain root and application certificates from the third-party vendor.
- Upload the appropriate certificates to the Live Data, Unified Intelligence Center, and Cisco Finesse servers.

Follow the instructions provided in the *Unified CCE Solution: Procedure to Obtain and Upload Third-Party CA certificates (Version 11.x)* technical note at https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-enterprise-1101/200286-Unified-CCE-Solution-Procedure-to-Obtai.html .

Export Self-Signed Live Data Certificates

Live Data installation includes the generation of self-signed certificates. If you choose to work with these self-signed certificates (rather than producing your own CA certificate or obtaining a CA certificate from a third-party certificate vendor), you must first export the certificates from Live Data and Cisco Unified Intelligence Center, as described in this procedure. You must export from both Side A and Side B of the Live Data and Cisco Unified Intelligence Center servers. You must then import the certificates into Finesse, importing both Side A and Side B certificates into each side of the Finesse servers.

As is the case when using other self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration on Cisco Unified Intelligence Center (https://*hostname of Cisco Unified Intelligence Center server*/cmplatform).

Step 2 From the **Security** menu, select **Certificate Management**.

Step 3 Click **Find**.

Step 4 Do one of the following:

- If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)
- If you are using self-signed certificate, do the following:

  a. Click **Generate New**.

  b. When the certificate generation is complete, restart the Cisco Tomcat service and the Cisco Live Data NGNIX service.

  c. Restart this procedure.

Step 5 Click **Download .pem file** and save the file to your desktop.

Be sure to perform these steps for both Side A and Side B.

Step 6 After you have downloaded the certificates from Cisco Unified Intelligence Center, sign in to Cisco Unified Operating System Administration on the Live Data server (http://hostname of LiveData server/cmplatform), and repeat steps 2 to 5. This is applicable only for Standalone LiveData.

What to do next

You must now import the Live Data and Cisco Unified Intelligence Center certificates into the Finesse servers.

Import Self-Signed Live Data Certificates

To import the certificates into the Finesse servers, use the following procedure.

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration on the Finesse server using the following URL:

http://*FQDN of Finesse server*:8443/cmplatform

Step 2 From the **Security** menu, select **Certificate Management**.

Step 3 Click **Upload Certificate**.

Step 4 From the **Certificate Name** drop-down list, select **tomcat-trust**.

Step 5 Click **Browse** and browse to the location of the Cisco Unified Intelligence Center certificate (with the **.pem** file extension).

Step 6 Select the file, and click **Upload File**.

Step 7 After you have uploaded the Cisco Unified Intelligence Center certificate repeat steps 3 to 6 for Live Data certificates.This is applicable only for standalone Live Data.

Step 8 After you upload both the certificates, restart Cisco Finesse Tomcat on the Finesse server.

What to do next

Be sure to perform these steps for both Side A and Side B.

Produce Certificate Internally

Set up Microsoft Certificate Server for Windows Server

This procedure assumes that your deployment includes a Windows Server Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows Server domain controller.

Before you begin

Before you begin, Microsoft .Net Framework must be installed. See Windows Server documentation for instructions.

Procedure

Step 1 In Windows, open the **Server Manager**.

Step 2 In the **Quick Start** window, click **Add Roles and Features** .

Step 3 In the **Set Installation Type** tab, select **Role-based or feature-based installation** , and then click **Next**.

Step 4 In the **Server Selection** tab, select the destination server then click **Next**.

Step 5 In the **Server Roles** tab, check the **Active Directory Certificate Services** box, and then click the **Add Features** button in the pop-up window.

Step 6 In the **Features** and **AD CS** tabs, click **Next** to accept default values.

Step 7 In the **Role Services** tab, verify that **Certification Authority** box is checked, and then click **Next**.

Step 8 In the **Confirmation** tab, click **Install**.

Step 9 After the installation is complete, click the **Configure Active Directory Certificate Service on the destination server** link.

Step 10 Verify that the credentials are correct (for the domain Administrator user), and then click **Next**.

Step 11 In the **Role Services** tab, check the **Certification Authority** box, and then click **Next**.

Step 12 In the **Setup Type** tab, select **Enterprise CA**, and then click **Next**.

Step 13 In the **CA Type** tab, select **Root CA**, and then click **Next**.

Step 14 In the **Private Key**, **Cryptography**, **CA Name**, **Validity Period**, and **Certificate Database** tabs, click **Next** to accept default values.

Step 15 Review the information in the **Confirmation** tab, and then click **Configure**.

Download CA certificate

This procedure assumes that you are using the Windows Certificate Services. Perform the following steps to retrieve the root CA certificate from the certificate authority. After you retrieve the root certificate, each user must install it in the browser used to access Finesse.

Procedure

Step 1 On the Windows domain controller, run the CLI command certutil -ca.cert *ca_name*.cer, in which *ca_name* is the name of your certificate.

Step 2 Save the file. Note where you saved the file so you can retrieve it later.

Deploy Root Certificate for Browsers

In environments where group policies are enforced via the Active Directory domain, the root certificate can be added automatically to each user's browser. Adding the certificate automatically simplifies user requirements for configuration.

Note To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

Procedure

Step 1 On the Windows domain controller, navigate to **Administrative Tools** > **Group Policy Management**.

Note Users who have strict Group Policy defined on the Finesse Agent Desktop are required to disable **Cross Document Messaging** from **Group Policy Management** to ensure proper functioning of Finesse on browser.

Step 2 Right-click Default Domain Policy and select **Edit**.

Step 3 In the Group Policy Management Console, go to **Computer Configuration** > **Policies** > **Window Settings** > **Security Settings** > **Public Key Policies**.

Step 4 Right-click Trusted Root Certification Authorities and select **Import**.

Step 5 Import the *ca_name*.cer file.

Step 6 Go to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Certificate Services Client - Auto-Enrollment**.

Step 7 From the Configuration Model list, select **Enabled**.

Step 8 Sign in as a user on a computer that is part of the domain and open browser.

Step 9 If the user does not have the certificate, run the command **gpupdate.exe /target:computer /force** on the user's computer.

Set Up CA Certificate for Internet Explorer Browser

After obtaining and uploading the CA certificates, either the certificate must be automatically installed via group policy or all users must accept the certificate.

In environments where users do not log directly in to a domain or group policies are not utilized, every Internet Explorer user in the system must perform the following steps once to accept the certificate.

Procedure

Step 1 In Windows Explorer, double-click the *ca_name*.cer file (in which *ca_name* is the name of your certificate) and then click **Open**.

Step 2 Click **Install Certificate** > **Next** > **Place all certificates in the following store**.

Step 3 Click **Browse** and select **Trusted Root Certification Authorities**.

Step 4 Click **OK**.

Step 5 Click **Next**.

Step 6 Click **Finish**.

A message appears that states you are about to install a certificate from a certification authority (CA).

Step 7 Click **Yes**.

A message appears that states the import was successful.

Step 8 To verify the certificate was installed, open Internet Explorer. From the browser menu, select **Tools** > **Internet Options**.

Step 9 Click the **Content** tab.

Step 10 Click **Certificates**.

Step 11 Click the **Trusted Root Certification Authorities** tab.

Step 12 Ensure that the new certificate appears in the list.

Step 13 Restart the browser for certificate installation to take effect.

Note If using Internet Explorer 11, you may receive a prompt to accept the certificate even if signed by private CA.

Set Up CA Certificate for Firefox Browser

Every Firefox user in the system must perform the following steps once to accept the certificate.

Note To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

Procedure

Step 1 From the Firefox browser menu, select **Options**.

Step 2 Click **Advanced**.

Step 3 Click the **Certificates** tab.

Step 4 Click **View Certificates**.

Step 5 Click **Authorities**.

Step 6 Click **Import** and browse to the *ca_name*.cer file (in which *ca_name* is the name of your certificate).

Step 7 Check the **Validate Identical Certificates** check box.

Step 8 Restart the browser for certificate installation to take effect.