Certificates for Live Data Coresident

Add Self-Signed Certificates for Live Data

Both Finesse and Unified Intelligence Center are installed with 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 the Unified Intelligence Center Publisher and Subscriber. You must then import the certificates into Finesse, importing the Publisher certificate to the Finesse Primary node and the Subscriber certificate to the Finesse Secondary node.

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 the tomcat certificate for your server is not on the list, do the following:

  a. Click **Generate New**.

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

    c.   Restart this procedure.

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

You must download the certificates that contain the hostnames Cisco Unified Intelligence Center publisher and Cisco Unified Intelligence Center subscriber.

Step 6   Sign in to Cisco Unified Operating System Administration on the primary Finesse server (https://*FQDN of Finesse server*:8443/cmplatform).

Step 7   From the **Security** menu, select **Certificate Management**.

Step 8   Click **Upload Certificate**.

Step 9   From the **Certificate Name** drop-down list, select **tomcat-trust**.

Step 10   Click **Browse** and browse to the location of the .pem files (Cisco Unified Intelligence Center publisher and subscriber certificates).

Step 11   Click **Upload File**.

Step 12   Restart Cisco Finesse Tomcat on the Finesse server.

Obtain and Upload CA Certificate for Live Data from a Third Party Vendor

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

Follow the instructions in the TechNote *Procedure to Obtain and Upload CA Certificate from a Third-party Vendor*, available 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.

Produce Certificate Internally

Set up Microsoft Certificate Server for Windows 2008 R2

This procedure assumes that your deployment includes a Windows Server 2008 R2 (Standard) Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows 2008 R2 (Standard) domain controller.

Procedure

Step 1   Click **Start**, right-click **Computer**, and select **Manage**.

Step 2   In the left pane, click **Roles**.

Step 3   In the right pane, click **Add Roles**.

The Add Roles Wizard opens.

Step 4	On the Select Server Roles screen, check the **Active Directory Certificate Services** check box, and then click **Next**.
Step 5	On the Introduction to Active Directory Certificate Services screen, click **Next**.
Step 6	On the Select Role Services screen, check the **Certification Authority** check box, and then click **Next**.
Step 7	On the Specify Setup Type screen, select **Enterprise**, and then click **Next**.
Step 8	On the Specify CA Type screen, select **Root CA**, and then click **Next**.
Step 9	Click **Next** on the Set Up Private Key, Configure Cryptography for CA, Configure CA Name, Set Validity Period, and Configure Certificate Database screens to accept the default values.
Step 10	On the Confirm Installations Selections screen, verify the information, and then click **Install**.

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 Internet Explorer

In environments where group policies are enforced via the Active Directory domain, the root certificate can be added automatically to each user's Internet Explorer. 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 Internet Explorer 11.

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 Internet Explorer.

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.