Security in Cisco Unity Connection Survivable Remote Site Voicemail

Introduction

This chapter contains information on how to secure communication between central Cisco Unity Connection and Cisco Unity Connection SRSV. In addition, it explains about Unity Connection SRSV passwords and PINs.

Using Self-Signed Certificate

You can use the self-signed certificate to secure communication between central Unity Connection server and Unity Connection SRSV. By default, central Unity Connection server and Unity Connection SRSV does not accept self-signed certificates.

Accessing Self-Signed Certificates on Central Unity Connection Server

Step 1 Run the following command on the Linux console for Command Line Interface (CLI) using administrator credentials:

```
run cuc dbquery unitydirdb EXECUTE PROCEDURE
csp_ConfigurationModify(pFullName='System.SRSV.AcceptSrsvSelfSignedCertificates', pValue='1')
```

Step 2 Run the following command to confirm that the value of “System.SRSV.AcceptSrsvSelfSignedCertificates” field is set to 1:

```
run cuc dbquery unitydirdb select objectid,fullname,value from vw_configuration where fullname like
 '%SRSV%'
```

After changing the value of System.SRSV.AcceptSrsvSelfSignedCertificates to 1, you need to restart the Connection Branch Sync Service and Tomcat Service on the central Unity Connection server to reflect the changes and allow the self-signed certificate access.

Restarting the Cisco Tomcat Service

Step 1 Sign in to the Unity Connection server using an SSH application.

Step 2 Run the following CLI command to restart the Tomcat service:

```
utils service restart Cisco Tomcat
```

Ignoring Certificate Error

You can enable this functionality in Unity Connection SRSV to ignore errors related to SSL certificate of the central server. With this feature enabled, Unity Connection SRSV works even if any certificate error occurs.

Following are the certificate errors that may occur:

- The certificate is missing or has not been provided.
- The certificate is not yet valid.
- The certificate has expired.
- The name on the certificate does not match the host name.

Enabling the Ignoring Certificate Error Feature in Unity Connection SRSV

Step 1 Run the following command on Unity Connection SRSV:

```
run cuc dbquery unitydirdb EXECUTE PROCEDURE
csp_ConfigurationModify(pFullName='System.SRSV.IgnoreSrsvCertificateErrors', pValue='1')
```

Step 2 Run the following command to confirm that the value of "System.SRSV.IgnoreSrsvCertificateErrors" field is set to 1.

```
run cuc dbquery unitydirdb select objectid,fullname,value from vw_configuration where fullname like
 '%SRSV%'
```

Note Make sure to restart the Connection Branch Sync service and Connection Tomcat service to reflect the changes.

Restarting the Cisco Tomcat Service

Step 1 Sign in to the Unity Connection server using an SSH application.

Step 2 Run the following CLI command to restart the Tomcat service

```
utils service restart Cisco Tomcat
```

Securing Communication between Unity Connection and Unity Connection SRSV

Unity Connection SRSV uses both Secure Sockets Layer (SSL) certificate and shared secrets to secure communication between the central Unity Connection and the branch. Following are the ways to secure communication between central Unity Connection server and Unity Connection SRSV:

- Installing SSL Certificate: When you install Unity Connection SRSV, a local certificate is automatically created and installed to secure communication between Unity Connection SRSV and Unity Connection. This means that all the network traffic (including usernames, passwords, other text data, and voicemails) between Unity Connection SRSV and Unity Connection is automatically encrypted.

- Using Shared Secrets: Unity Connection SRSV uses shared secrets to authenticate Unity Connection access. For more information on shared secrets, see the “Unity Connection SRSV Passwords and Shared Secrets” section of the “Passwords, PINs, and Authentication Rule Management” chapter of the Security Guide for Cisco Unity Connection, Release 11.x at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/security/b_11xcucsecx.html.

Task List for Securing Communication between Unity Connection SRSV Administration and Unity Connection SRSV

Perform the following tasks to create and install an SSL server certificate to secure communication between Unity Connection SRSV Administration and Unity Connection SRSV:

1. If you are using Microsoft Certificate Services to issue certificates: Install Microsoft Certificate Services. For information on installing Microsoft Certificate Services on a server running Windows Server 2003, see the Installing Microsoft Certificate Services (Windows Server 2003 Only), on page 6. For information on installing Microsoft Certificate Services on a server running a later version of Windows Server, see the Microsoft documentation.

   If you are using another application to issue certificates, install the application. See the manufacturer documentation for installation instructions and skip to Task 2

   If you are using an external certification authority to issue certificates, skip to Task 2

Note If you have already installed Microsoft Certificate Services or another application that can create certificate signing requests, skip to Task 2

2. Create a certificate signing request. Then download the certificate signing request to the server on which you installed Microsoft Certificate Services or another application that issues certificates, or download the request to a server that you can use to send the certificate signing request to an external certificate authority (CA). Do the Creating and Downloading a Certificate Signing Request on Unity Connection SRSV, on page 4.

3. If you are using Microsoft Certificate Services to export the root certificate and to issue the server certificate: Do the procedure in the Exporting the Root Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only), on page 7.

Note If you are using another application to issue the certificate, see the documentation of the application for information on issuing certificates. If you are using an external CA to issue the certificate, send the certificate signing request to the external CA. When the external CA returns the certificate, continue with Task Task List for Securing Communication between Unity Connection SRSV Administration and Unity Connection SRSV

Only PEM-formatted (also known as Base-64 encoded DER) certificates can be uploaded to Unity Connection SRSV. The certificate must have a .pem filename extension. If the certificate is not in this format, you can convert to PEM format using freely available utilities like OpenSSL.

4. Upload the root certificate and the server certificate to the Unity Connection SRSV server. Do the Uploading Root and Server Certificates to Unity Connection SRSV, on page 5.

5. Prevent users from receiving a security alert whenever they access Unity Connection SRSV using the Unity Connection SRSV Administration or Cisco Unity Connection Administration. Do the following tasks on all the computers from which users can access Unity Connection SRSV:

   - Import the server certificate that you uploaded to the Unity Connection SRSV server in Task Task List for Securing Communication between Unity Connection SRSV Administration and Unity Connection SRSV into the certificate store. The procedure to import certificates differs from browser to browser. For more information Task List for Securing Communication between Unity Connection SRSV Administration and Unity Connection SRSVon importing certificates, see the documentation for the browser.

   - Import the server certificate that you uploaded to the Unity Connection SRSV server in Task Task List for Securing Communication between Unity Connection SRSV Administration and Unity Connection SRSV into the Java store. The procedure to import certificates differs from browser to browser. For more information on importing certificates, see the documentation for the browser.

Creating and Downloading a Certificate Signing Request on Unity Connection SRSV

Step 1 In Cisco Unified Operating System Administration, expand Security and select **Certificate Management**.

Step 2 On the Certificate List page, select **Generate CSR**.

Step 3 On the Generate Certificate Signing Request page, in the **Certificate Name** list, select **tomcat** and then select **Generate CSR**.

Step 4 When the Status area displays a message that the CSR was successfully generated, select **Close**.

Step 5 On the Certificate List page, select **Download CSR**.

Step 6 On the Download Certificate Signing Request page, in the **Certificate Name** list, select **tomcat** and then select **Download CSR**.

Step 7 In the File Download dialog box, select **Save**.

Step 8 In the Save As dialog box, in the **Save As Type** list, select **All Files**

Step 9 Save the file**tomcat.csr** to a location on the server on which you installed Microsoft Certificate Services or on a server that you can use to send the CSR to an external certification authority.

Step 10 On the Download Certificate Signing Request page, select**Close**.

Uploading Root and Server Certificates to Unity Connection SRSV

Step 1 In Cisco Unified Operating System Administration, expand Security and select **Certificate Management**.

Note If you select **Find** to display a list of the certificates currently installed on the server, you see an existing, automatically generated, self-signed certificate for Tomcat. That certificate is unrelated to the Tomcat certificates that you upload in this procedure.

Step 2 Upload the root certificate:

a) On the Certificate List page, select **Upload Certificate**.
b) On the Upload Certificate page, in the Certificate Name list, select **tomcat-trust** but leave the Root Certificate field blank.
c) Select **Browse and navigate to** the location of the root CA certificate.

If you used Microsoft Certificate Services to issue the certificate, this is the location of the root certificate that you exported in the Exporting the Root Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only), on page 7.

If you used an external certification authority to issue the certificate, this is the location of the root CA certificate that you received from the external certification authority.

d) Select the name of the file and select **Open**.
e) On the Upload Certificate page, select **Upload File**.
f) When the Status area reports that the upload succeeded, select **Close**.

Step 3 Upload the server certificate:

a) On the Certificate List page, select **Upload Certificate**.
b) On the Upload Certificate page, in the Certificate Name list, select **tomcat**.
c) In the Root Certificate field, enter the filename of the root certificate that you uploaded in Step 2.
d) Select **Browse** and navigate to the location of the server certificate.

If you used Microsoft Certificate Services to issue the certificate, this is the location of the server certificate that you issued in the Exporting the Root Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only), on page 7.

If you used an external certification authority to issue the certificate, this is the location of the server certificate that you received from the external certification authority.

e) Select the name of the file and select **Open**.
f) On the Upload Certificate page, select **Upload File**.
g) When the Status area reports that the upload succeeded, select **Close**.

Step 4 Restart the Tomcat service (the service cannot be restarted from Cisco Unified Serviceability):

a) Sign in to the Cisco Unity Connection SRSV server using an SSH application.
b) Run the following CLI command to restart the Tomcat service:

```
utils service restart Cisco Tomcat
```

Restarting Connection Branch Sync Service on Unity Connection

Step 1 In Cisco Unity Connection Serviceability, expand Tools menu and select **Service Management**.

Step 2 In the Optional Services section, for the Connection Branch Sync service, select **Stop**.

Step 3 When the Status area displays a message that the Unity Connection IMAP Server service is successfully stopped, select **Start** for the service.

Installing Microsoft Certificate Services (Windows Server 2003 Only)

If you want to use a third-party certificate authority to issue SSL certificates, or if Microsoft Certificate Services is already installed, skip this section.

Do the procedure in this section if you want to use Microsoft Certificate Services to issue your own certificate and if you want to install the application on a server running Windows Server 2003.

If you want to install a root certification authority (the generic term for Microsoft Certificate Services) on a Windows Server 2008 server, refer to the Windows Server 2008 online help.

Step 1 On any server in which DNS name (FQDN) or IP address can be resolved by all client computers that access Unity Connection SRSV voicemails, sign in to Windows using an account that is a member of the local Administrators group.

Step 2 On the Windows Start menu, select **Settings** > **Control Panel** and select **Add or Remove Programs**.

Step 3 In the left pane of the Add or Remove Programs control panel, select **Add/Remove Windows Components**.

Step 4 In the Windows Components dialog box, check the **Certificate Services** check box.

Step 5 When the warning appears about not being able to rename the computer or to change domain membership, select **Yes**.

Step 6 Select **Next**.

Step 7 On the CA Type page, select **Stand-alone Root CA** and select **Next**. (A stand-alone certification authority (CA) is a CA that does not require Active Directory.)

Step 8 On the CA Identifying Information page, in the Common Name for This CA field, enter a name for the certification authority.

Step 9 Select the default value in the Distinguished Name Suffix field.

Step 10 For Validity Period, select the default value of **5 Years** and select **Next**.

Step 11 On the Certificate Database Settings page, select **Next** to accept the default values.

If a message appears indicating that Internet Information Services is running on the computer and must be stopped before proceeding, select **Yes** to stop the services.

Step 12 If you are prompted to insert the Windows Server 2003 disc into the drive, insert the disc.

Step 13 In the Completing the Windows Components Wizard dialog box, select **Finish**.

Step 14 Close the Add or Remove Programs dialog box.

Exporting the Root Certificate and Issuing the Server Certificate (Microsoft Certificate Services Only)

Step 1 On the server on which you installed Microsoft Certificate Services, sign in to Windows using an account that is a member of the Domain Admins group.

Step 2 On the Windows Start menu, select **Programs** > **Administrative Tools** and select **Certificate Authority** .

Step 3 In the left pane, expand **Certification Authority (Local)** > select the certificate authority that you created while installing Microsoft Certificate Services in the Installing Microsoft Certificate Services (Windows Server 2003 Only), on page 6.

Step 4 Export the root certificate:

a) Right-click the name of the certification authority and select **Properties**.
b) On the General tab, select **View Certificate**.
c) Click the **Details** tab and select **Copy to File**.
d) On the Welcome to the Certificate Export Wizard page, select **Next**.
e) On the Export File Format page, select **Next** to accept the default value of **DER Encoded Binary X.509 (.CER)**.
f) On the File to Export page, enter a path and filename for the .cer file that you can access from the Unity Connection server.

Note Write down the path and filename. You need it in a later procedure.

g) Follow the onscreen prompts until the wizard has finished the export.
h) Select **OK** to close the Certificate dialog box and select **OK** again to close the Properties dialog box.

Step 5 Issue the server certificate:

a) Right-click the name of the certification authority and select **All Tasks > Submit New Request**.
b) Browse to the location of the certificate signing request file that you created in the Creating and Downloading a Certificate Signing Request on Unity Connection SRSV, on page 4, and double-click the file.
c) In the left pane of Certification Authority, select **Pending Requests**.
d) Right-click the pending request that you submitted in b and select **All Tasks > Issue**.
e) In the left pane of Certification Authority, select **Issued Certificates**.
f) Right-click the new certificate and select **All Tasks > Export Binary Data**.
g) In the Export Binary Data dialog box, in the Columns that Contain Binary Data list, select **Binary Certificate**.
h) In the Export Binary Data dialog box, select **Save Binary Data to a File** and select **OK**.
i) In the Save Binary Data dialog box, enter a path and filename. Select a network location that you can access from the Unity Connection SRSV server and select OK.

Note Write down the path and filename. You need it in a later procedure.

Step 6 Close Certification Authority.

Unity Connection SRSV Passwords and Shared Secrets

All the requests initiated from the central Unity Connection server to the Unity Connection SRSV server use administrator credentials of Unity Connection SRSV for communication whereas the requests from Unity Connection SRSV to Unity Connection use secret tokens for authentication.

The central Unity Connection server uses the administrator username and password of Unity Connection SRSV to authenticate access to the server. The username and password of the Unity Connection SRSV get stored in the Unity Connection database as you create a new branch on the central Unity Connection server.

During each provisioning cycle with Unity Connection SRSV, the central Unity Connection server generates a secret token and shares the token with Unity Connection SRSV. After the provisioning is completed from the Unity Connection SRSV site, it notifies Unity Connection using the same token. Then this token is removed from both Unity Connection and Unity Connection SRSV servers as soon as the provisioning cycle is completed. This concept of runtime token keys is known as shared secrets.

Changing Unity Connection SRSV User PIN

You can change the PIN of a Unity Connection SRSV user either from Cisco Unity Connection Administration or from the telephone user interface (TUI). After changing the PIN of the selected user, you need to provision the associated branch to update the user information in the Unity Connection SRSV database.

Note You cannot change the PIN of an SRSV user through Cisco Unity Connection SRSV Administration interface.