



CHAPTER 17

Securing Connections in Cisco Unity Connection Survivable Remote Site Voicemail 9.1(1)

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

See the following sections:

- [Using Self-Signed Certificate Based Access, page 17-1](#)
- [Securing Connections between Central Connection server and Connection SRSV, page 17-2](#)
- [Securing Connections between Connection SRSV Administration and Connection SRSV, page 17-2](#)
- [Installing Microsoft Certificate Services \(Windows Server 2003 Only\), page 17-5](#)
- [Exporting the Root Certificate and Issuing the Server Certificate \(Microsoft Certificate Services Only\), page 17-6](#)

Using Self-Signed Certificate Based Access

You can use the self-signed certificate based access for communication between central Connection server and Connection SRSV. By default, central Connection server and Connection SRSV does not accept self-signed certificates. To accept self-signed certificates on the central Connection server and Connection SRSV, you need to perform the following steps on command prompt using administrator credentials:

Step 1 Run the following command:

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

Step 2 Run the following command to confirm that the value of “System.SRSV.AcceptSrvSelfSignedCertificates” 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.AcceptSrvSelfSignedCertificates to 1, you need to restart the Connection Branch Sync Service and Tomcat Service to reflect the changes and allow the self-signed certificate access.

To Restart the Tomcat service please follow following steps:

-
- Step 1** Sign in to the Connection server by using an SSH application.
- Step 2** Run the following CLI command to restart the Tomcat service:

```
utils service restart Cisco Tomcat
```

Securing Connections between Central Connection server and Connection SRSV

Connection SRSV uses both Secure Sockets Layer (SSL) certificate and shared secrets to secure communication between the central Connection and the branch.

1. Installing SSL Certificate

When you install Cisco Unity Connection SRSV, a local certificate is automatically created and installed to secure communication between Connection SRSV and Connection. This means that all network traffic (including usernames, passwords, other text data, and voice messages) between Connection SRSV and Connection is automatically encrypted. For more information on installing SSL certificate, refer to the "Using SSL to Secure Client/Server Connections in Cisco Unity Connection 9.x" chapter of the *Security Guide for Cisco Unity Connection Release 9.x* at

http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/security/guide/9xcucsecx.html.

2. Using Shared Secrets

Connection SRSV uses shared secrets to authenticate Connection access. For more information on shared secrets, refer to the "Cisco Unity Connection SRSV Passwords and Shared Secrets" section of the "Passwords, PINs, and Authentication Rule Management in Cisco Unity Connection 9.x" chapter of the *Security Guide for Cisco Unity Connection Release 9.x* at

http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/security/guide/9xcucsecx.html.

Securing Connections between Connection SRSV Administration and Connection SRSV

Do the following tasks to create and install an SSL server certificate to secure Connection SRSV Administration access to 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)" section on page 17-5. For information on installing Microsoft Certificate Services on a server running a later version of Windows Server, refer to Microsoft documentation.

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

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

**Note**

If you already have 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 CA. Do the [“To Create and Download a Certificate Signing Request” procedure on page 17-3](#).
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 \(Microsoft Certificate Services Only\)” section on page 17-6](#).

If you are using another application to issue the certificate, see the documentation for 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 4.

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

4. Upload the root certificate and the server certificate to the Connection SRSV server. Do the [“To Upload the Root and Server Certificates to the Cisco Unity Connection SRSV Server” procedure on page 17-4](#).
5. To prevent users from seeing a security alert whenever they access Connection SRSV by using the Connection SRSV Administration or Connection, do the following tasks on all computers from which users will access Connection SRSV:
 - Import the server certificate that you uploaded to the Connection SRSV server in Task 4. into the certificate store. The procedure differs based on the browser. For more information, see the documentation for the browser.
 - Import the server certificate that you uploaded to the Connection SRSV server in Task 4. into the Java store. The procedure differs based on the operating system running on the client computer. For more information, see the operating system documentation and the Java Runtime Environment documentation.

To Create and Download a Certificate Signing Request

- Step 1** On the Cisco Unity Connection SRSV server, sign in to Cisco Unified Operating System Administration.
- Step 2** On the Security menu, select **Certificate Management**.
- Step 3** On the Certificate List page, select **Generate CSR**.
- Step 4** On the Generate Certificate Signing Request page, in the **Certificate Name** list, select **tomcat**.
- Step 5** Select **Generate CSR**.
- Step 6** When the Status area displays a message that the CSR was successfully generated, select **Close**.
- Step 7** On the Certificate List page, select **Download CSR**.
- Step 8** On the Download Certificate Signing Request page, in the **Certificate Name** list, select **tomcat**.
- Step 9** Select **Download CSR**.
- Step 10** In the File Download dialog box, select **Save**.

- Step 11** In the Save As dialog box, in the **Save As Type** list, select **All Files**.
- Step 12** 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 13** On the Download Certificate Signing Request page, select **Close**.

To Upload the Root and Server Certificates to the Cisco Unity Connection SRSV Server

- Step 1** On the Cisco Unity Connection SRSV server on which you created the certificate signing request, sign in to Cisco Unified Operating System Administration.
- Step 2** On the Security menu, select **Certificate Management**.



Note If you select **Find** and display a list of the certificates currently installed on the server, you will 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 3** Upload the root certificate:
- On the Certificate List page, select **Upload Certificate**.
 - On the Upload Certificate page, in the Certificate Name list, select **tomcat-trust**.
 - Leave the Root Certificate field blank.
 - Select **Browse**, and browse 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 [“To Export the Root Certificate and to Issue the Server Certificate” procedure on page 17-6](#).
 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.
 - Select the name of the file.
 - Select **Open**.
 - On the Upload Certificate page, select **Upload File**.
 - When the Status area reports that the upload succeeded, select **Close**.
- Step 4** Upload the server certificate:
- On the Certificate List page, select **Upload Certificate**.
 - On the Upload Certificate page, in the Certificate Name list, select **tomcat**.
 - In the Root Certificate field, enter the filename of the root certificate that you uploaded in [Step 3](#).
 - Select **Browse**, and browse 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 [“To Export the Root Certificate and to Issue the Server Certificate” procedure on page 17-6](#).
 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.
 - Select the name of the file.

- f. Select **Open**.
- g. On the Upload Certificate page, select **Upload File**.
- h. When the Status area reports that the upload succeeded, select **Close**.

Step 5 Restart the Tomcat service (the service cannot be restarted from Cisco Unified Serviceability):

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

```
utils service restart Cisco Tomcat
```

To Restart the Connection Branch Sync Service

- Step 1** Sign in to Cisco Unity Connection Serviceability.
 - Step 2** On the Tools menu, select **Service Management**.
 - Step 3** In the Optional Services section, for the Connection Branch Sync Service, select **Stop**.
 - Step 4** When the Status area displays a message that the Connection IMAP Server service was 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.

To Install the Microsoft Certificate Services Component

- Step 1** On any server whose DNS name (FQDN) or IP address can be resolved by all client computers that will access Connection SRSV voice messages, sign in to Windows by using an account that is a member of the local Administrators group.
- Step 2** On the Windows Start menu, select **Settings > Control Panel > 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. Do not change any other items.
- 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** Accept the default value in the Distinguished Name Suffix field.
 - Step 10** For Validity Period, accept the default value of **5 Years**.
 - Step 11** Select **Next**.
 - Step 12** 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 13** If you are prompted to insert the Windows Server 2003 disc into the drive, do so.
 - Step 14** In the Completing the Windows Components Wizard dialog box, select **Finish**.
 - Step 15** Close the Add or Remove Programs dialog box.
-

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

Do the following procedure only when you are using Microsoft Certificate Services to issue the certificate.

To Export the Root Certificate and to Issue the Server Certificate

- Step 1** On the server on which you installed Microsoft Certificate Services, sign in to Windows by using an account that is a member of the Domain Admins group.
- Step 2** On the Windows Start menu, select **Programs > Administrative Tools > Certification Authority**.
- Step 3** In the left pane, expand **Certification Authority (Local) > <Certification authority name>**, where <Certification authority name> is the name that you gave to the certification authority when you installed Microsoft Certificate Services in the [“To Install the Microsoft Certificate Services Component” procedure on page 17-5](#).
- 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. Select the **Details** tab.
 - d. Select **Copy to File**.
 - e. On the Welcome to the Certificate Export Wizard page, select **Next**.
 - f. On the Export File Format page, select **Next** to accept the default value of **DER Encoded Binary X.509 (.CER)**.
 - g. On the File to Export page, enter a path and filename for the .cer file. Select a network location that you can access from the Connection server.

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

- h. Follow the onscreen prompts until the wizard has finished the export.
- i. 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 [“To Create and Download a Certificate Signing Request”](#) procedure on page 17-3, 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. Select **Save Binary Data to a File**.
- i. Select **OK**.
- j. In the Save Binary Data dialog box, enter a path and filename. Select a network location that you can access from the Connection SRSV server.
Write down the path and filename. You will need it in a later procedure.
- k. Select **OK**.

Step 6 Close Certification Authority.
