SIP Federation Security Certificate Configuration with Cisco Adaptive Security Appliance

This section explains SIP Federation Security Certificate Configuration with Cisco Adaptive Security Appliance.

- Security Certificate Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance, on page 1
- Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge (External Interface) with Microsoft CA, on page 5
- Security Certificate Configuration on Lync Edge Server for TLS Federation, on page 14

Security Certificate Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance

This section explains the Security Certificate Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance.

Generate Key Pair and Trustpoints on the Cisco Adaptive Security Appliance

You need to generate the key pair for this certification (for example **imp_proxy_key)**, and configure a trustpoint to identify the self-signed certificate from Cisco Adaptive Security Appliance to IM and Presence Service (for example **imp_proxy**). You need to specify the enrollment type as "self" to indicate you are generating a self-signed certificate on Cisco Adaptive Security Appliance, and specify the certificate subject name as the IP address of the inside interface.

Before you begin

Ensure you carried out the configuration tasks described in the following chapters:

- IM and Presence Service Configuration for SIP Federation
- Cisco Adaptive Security Appliance configuration for SIP Federation

Procedure

Step 1 On the Cisco Adaptive Security Appliance enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

Step 2 Enter this command to generate the key pair for this certification:

```
crypto key generate rsa label imp_proxy_key modulus 1024
```

Step 3 Enter the following sequence of commands to create a trustpoint for IM and Presence Service:

```
crypto ca trustpoint trustpoint_name (for example, imp_proxy)
(config-ca-trustpoint)# enrollment self
(config-ca-trustpoint)# fqdn none
(config-ca-trustpoint)# subject-name cn=ASA_inside_interface_ip_address
(config-ca-trustpoint)# keypair imp_proxy_key
```

Troubleshooting Tip

Enter the command **show crypto key mypubkey rsa** to check that the key pair is generated.

What to do next

Generate Self-Signed Certificate on the Cisco Adaptive Security Appliance, on page 2

Generate Self-Signed Certificate on the Cisco Adaptive Security Appliance

Before you begin

- Complete the steps in Generate Key Pair and Trustpoints on the Cisco Adaptive Security Appliance, on page 1.
- You need a text editor that has UNIX support to complete this procedure. We recommend Microsoft Wordpad version 5.1, or Microsoft Notepad version 5.1 service pack 2.

Procedure

Step 1 Enter this command to generate the self-signed certificate:

```
(config-ca-trustpoint)# crypto ca enroll trustpoint_name (for example, imp_proxy)
```

Step 2 Enter **no** when you are prompted to include the device serial number in the subject name.

Step 3 Enter **yes** when you are prompted to generate the self-signed certificate.

Step 4 Enter this command to prepare the certificate to export to the IM and Presence Service:

```
crypto ca export imp_proxy identity-certificate
```

The PEM encoded identity certificate displays on screen, for example:

```
-----BEGIN
CERTIFICATE-----MIIBnDCCAQWgAwIBAgIBMTANBgkqhkiG9w0BAQQFADAUMRIwEAYDVQQDEwlDVVAt…….. -----END
CERTIFICATE-----
```

Step 5 Copy and paste the entire contents of the Cisco Adaptive Security Appliance certificate into Wordpad or Notepad with a .pem extension.

Step 6 Save the .pem file to your local machine.

What to do next

Import Self-Signed Certificate onto the IM and Presence Service, on page 3

Import Self-Signed Certificate onto the IM and Presence Service

Before you begin

Complete the steps in Generate Self-Signed Certificate on the Cisco Adaptive Security Appliance, on page 2

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate**.

Step 3 For the Certificate Purpose, choose **cup-trust**.

Note Leave the Root Name field blank.

Step 4 Click **Browse**, and locate the Cisco Adaptive Security Appliance .pem certificate file (that you created in the previous procedure) on your local computer.

Step 5 Click **Upload File** to upload the certificate to the IM and Presence Service node.

Troubleshooting Tips

Perform a find on the certificate list, `<asa ip address>.pem` and an `<asa ip address>.der` are in the certificate list.

What to do next

Generate a New Certificate on the IM and Presence Service, on page 4

Generate a New Certificate on the IM and Presence Service

Note Cisco ASA firewall certificates must have the Server Authentication and Client Authentication attributes set for inside, outside. This can be verified by checking the certificate Enhanced Key Usage (EKU) parameter or for an Object Identifier (OID) value of:

1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2

Before you begin

Complete the steps in Import Self-Signed Certificate onto the IM and Presence Service, on page 3

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security** > **Certificate Management**.

Step 2 Click **Generate New**.

Step 3 From the Certificate Purpose drop-down list, choose **cup**.

Step 4 Click **Generate**.

What to do next

Import an IM and Presence Service Certificate into the Cisco Adaptive Security Appliance, on page 4

Import an IM and Presence Service Certificate into the Cisco Adaptive Security Appliance

In order to import the IM and Presence Service certificate onto the Cisco Adaptive Security Appliance you need to create a trustpoint to identify the imported certificate from the IM and Presence Service (for example **cert_from_imp**), and specify the enrollment type as “terminal” to indicate that the certificate received from the IM and Presence Service will be pasted into the terminal.

Note It is essential that the IM and Presence Service and the Cisco Unified Communications Manager nodes, and the Cisco Adaptive Security Appliance are synchronized off the same NTP source.

Before you begin

- Complete the steps in Generate a New Certificate on the IM and Presence Service, on page 4.
- You need a text editor that has UNIX support to complete this procedure. We recommend Microsoft Wordpad version 5.1, or Microsoft Notepad version 5.1 service pack 2.

Procedure

Step 1 Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

Step 2 Enter this sequence of commands to create a trustpoint for the imported IM and Presence Service certificate:

```
crypto ca trustpoint cert_from_imp enrollment terminal
```

Step 3 Enter this command to import the certificate from IM and Presence Service:

```
crypto ca authenticate cert_from_imp
```

Step 4 Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security** > **Certificate Management** on the IM and Presence Service.

Step 5 Click **Find**.

Step 6 Locate the IM and Presence Service certificate that you created in the previous procedure.

Step 7 Click **Download**.

Step 8 Open the imp.pem file using one of the recommended text editors.

Step 9 Cut and paste the contents of the imp.pem into the Cisco Adaptive Security Appliance terminal.

Step 10 Enter `quit`.

Step 11 Enter `yes` when you are prompted to accept the certificate.

Step 12 Run the command `show crypto ca certificate` to view the certificate.

What to do next:

Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge (External Interface) with Microsoft CA, on page 5

Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge (External Interface) with Microsoft CA

These procedures are an example, and demonstrate how to configure certificates using the Microsoft CA.

Note An example of this procedure using the VeriSign CA is provided in the appendix of this guide.

CA Trustpoints

When generating a trustpoint, you must specify an enrollment method to be used with the trustpoint. You can use Simple Certificate Enrollment Process (SCEP) as the enrollment method (assuming you are using a Microsoft CA), where you use the **enrollment url** command to define the URL to be used for SCEP enrollment with the trustpoint you declared. The URL defined should be the URL of your CA.

You can also use manual enrollment as the enrollment method, where you use the **enrollment terminal** command to paste the certificate received from the CA into the terminal. Both enrollment method procedures are described in this section. Refer to the *CiscoSecurity Appliance Command Line Configuration Guide* for further details about the enrollment method.

In order to use SCEP, you need to download the Microsoft SCEP add-on from the following URL:

http://www.microsoft.com/Downloads/details.aspx?familyid=9F306763-D036-41D8-8860-1636411B2D01&displaylang=en

The SCEP add-on must be installed on the Microsoft CA that you are configuring the certificates on.

Download the SCEP add-on as follows:

- Download and run **scepsetup.exe**.
- Select **local system account**.
- Deselect **SCEP challenge phrase to enroll**.
- Enter the details of the CA.

When you click **Finish**, retrieve the SCEP URL. You use this URL during trustpoint enrollment on the Cisco Adaptive Security Appliance.

Configure a Certificate on the Cisco Adaptive Security Appliance Using SCEP

Procedure

Step 1 Enter this command to generate a key pair for the CA:

```
crypto key generate rsa label public_key_for_ca modulus 1024
```

Step 2 Enter this command to generate a trustpoint to identify the CA.

```
crypto ca trustpoint trustpoint_name
```

Step 3 Use the **client-types** command to specify the client connection types for the trustpoint that can be used to validate the certificates associated with a user connection. Enter this command to specify a **client-types ssl** configuration which indicates that SSL client connections can be validated using this trustpoint:

```
(config-ca-trustpoint)# client-types ssl
```

Step 4 Enter this command to configure the FQDN of the public IM and Presence Service address:

```
fqdn fqdn_public_imp_address
```

Note You may be issued a warning regarding VPN authentication here.

Step 5 Enter this command to configure a keypair for the trustpoint:

keypair *public_key_for_ca*

Step 6 Enter this command to configure the enrollment method for the trustpoint:

enrollment url http://*ca_ip_address***/certsrv/mscep/mscep.dll**

Step 7 Enter this command to obtain the CA certificate for the trustpoint you configured:

crypto ca authenticate *trustpoint_name*

```
INFO: Certificate has the following attributes: Fingerprint: cc966ba6 90dfe235 6fe632fc
2e521e48
```

Step 8 Enter **yes** when you are prompted to accept the certificate from the CA.

```
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

Step 9 Run the **crypto ca enroll** command.

crypto ca enroll *trustpoint_name*

The following warning output displays:

```
%WARNING: The certificate enrollment is configured with an fqdn that differs from the system
fqdn. If this certificate will be used for VPN authentication this may cause connection
problems.
```

Step 10 Enter **yes** when you are prompted to continue with the enrollment.

```
Would you like to continue with this enrollment? [yes/no]: yes

% Start certificate enrollment..
```

Step 11 Enter a password when you are prompted to create a challenge password.

```
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate. For security reasons your password will
not be saved in the configuration. Please make a note of it.

Password: <password>

********** Re-enter password: **********
```

Step 12 Enter **no** when you are prompted to include the device serial number in the subject name.

Step 13 Enter **yes** when you are prompted to request the certificate from the CA.

```
Request certificate from CA? [yes/no]: yes

% Certificate request sent to Certificate Authority
```

Step 14 Go to the CA and issue the pending certificate (if the certificate was not issued automatically).

What to do next

Certificate Configuration for the External Access Edge Interface, on page 9

Configure a Certificate on the Cisco Adaptive Security Appliance Using Manual Enrollment

Enrolling a trustpoint by uploading a CA certificate:

Procedure

Step 1 Enter this command to generate a key pair for the CA:

```
crypto key generate rsa label public_key_for_ca modulus 1024
```

Step 2 Enter this sequence of commands to generate a trustpoint to identify the CA:

```
crypto ca trustpoint trustpoint_name fqdn fqdn_public_imp_address client-types ssl keypair public_key_for_ca
```

Note
- The FQDN value must be the FQDN of the public IM and Presence Service address.
- The keypair value must be the keypair created for the CA.

Step 3 Enter this command to configure the enrollment method for the trustpoint:

```
enrollment terminal
```

Step 4 Enter this command to authenticate the certificate:

```
crypto ca authenticate trustpoint_name
```

Step 5 Acquire the root certificate of the CA:

a) Go to your CA webpage, for example, `http(s)://ca_ip_address/certsrv`.
b) Click **Download a CA certificate, certificate chain, or CRL**.
c) Choose **Base 64**.
d) Download the CA certificate.
e) Save the certificate as a .cer file, for example `CARoot.cer`.

Step 6 Open the root certificate (.cer file) in a text editor.

Step 7 Copy and paste the certificate contents into the Cisco Adaptive Security Appliance terminal.

Step 8 Enter **yes** when you are prompted to accept the certificate.

Generating a CSR for Cisco Adaptive Security Appliance Public Certificate.

Step 9 Enter this command to send an enrollment request to the CA:

```
crypto ca enroll trustpoint_name
```

Step 10 Enter **no** when you are asked if you want to include the device serial number in the subject name.

Step 11 Enter **yes** when you are asked to Display Certificate Request to terminal.

Step 12 Copy and paste this base-64 certificate into a text editor (to use in a later step).

Step 13 Enter **no** when you are asked to redisplay the enrollment request.

Step 14 Paste the base-64 certificate (that you copied in Step 4) into the certificate request page of your CA:

a) Go to your CA webpage, for example, `http(s)://ca_ip_address/certsrv`.

b) Click **Request a certificate**.
c) Click **Advanced Certificate request**.
d) Click **Submit a certificate request by using a base-64-encoded CMC orPKCS#10 file...**
e) Paste the base-64 certificate (that you copied in Step 4).
f) Submit the request and issue the certificate from the CA.
g) Download the certificate and save as a *.cer file.
h) Open the certificate in a text editor, copy and paste the contents into the terminal. End with the word **quit** on a separate line.

Step 15 Enter this command to import the certificate that you receive from the CA:

```
crypto ca import trustpoint_name certificate
```

Step 16 Enter `yes` when you are asked if you want to continue with the enrollment.

What to do next -

Certificate Configuration for the External Access Edge Interface, on page 9

Certificate Configuration for the External Access Edge Interface

This procedure describes how to configure the certificate on the Access Edge server with a standalone CA.

Download CA Certification Chain

Procedure

Step 1 On the Access Edge Server, choose **Start** > **Run**.
Step 2 Enter `http://<name of your Issuing CA Server>/certsrv`, and click **OK**.
Step 3 Click **Download a CA certificate, certificate chain, or CRL** from the Select a task menu.
Step 4 Click **Download CA certificate chain** from Download a CA Certificate, Certificate Chain, or CRL menu.
Step 5 Click **Save** in the File Download dialog box.
Step 6 Save the file on a hard disk drive on your server. This file has an extension of .p7b. If you open this .p7b file, the chain displays the following two certificates:
a) name of Standalone root CA certificate
b) name of Standalone subordinate CA certificate (if any)

What to do next

Install a CA Certification Chain, on page 10

Install a CA Certification Chain

Before you begin

Complete the steps inDownload CA Certification Chain, on page 9

Procedure

Step 1 Choose **Start** > **Run**.

Step 2 Enter `mmc`, and click **OK**.

Step 3 From the File menu, choose **Add/Remove Snap-in**.

Step 4 Click **Add** in the Add/Remove Snap-in dialog box.

Step 5 In the list of Available Standalone Snap-ins, choose **Certificates**.

Step 6 Click **Add**.

Step 7 Choose **Computer account**.

Step 8 Click **Next**.

Step 9 In the Select Computer dialog box, perform the following tasks:

a) Ensure that **<Local Computer> (the computer this console is running on)** is selected.

b) Click **Finish**.

Step 10 Click **Close**.

Step 11 Click **OK**.

Step 12 In the left pane of the Certificates console, expand **Certificates:** Local Computer.

Step 13 Expand Trusted Root Certification Authorities.

Step 14 Right-click **Certificates**, and point to All Tasks.

Step 15 Click **Import**.

Step 16 In the Import wizard, click **Next**.

Step 17 Click **Browse** and go to where you saved the certificate chain.

Step 18 Choose the file, and click **Open**.

Step 19 Click **Next**.

Step 20 Leave the default value **Place all certificates in the store** and ensure that Trusted Root Certification Authorities appears under the Certificate store.

Step 21 Click **Next**.

Step 22 Click **Finish**.

What to do next

Request Certificate from CA Server, on page 11

Request Certificate from CA Server

Before you begin

Complete the steps in Install a CA Certification Chain, on page 10

Procedure

Step 1 Log in to the Access Edge server and open a web browser.

Step 2 Open the following URL: **http://***certificate_authority_server_IP_address***/certsrv**

Step 3 Click **Request a Certificate**.

Step 4 Click **Advanced Certificate Request**.

Step 5 Click **Create and submit a request to this CA**.

Step 6 In the Type of Certificate Needed list, click **Other**.

Step 7 Enter the FQDN of the Access Edge external interface for the Subject Common Name,

Step 8 in the Object Identifier (OID) field, enter the following value:

1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2

Note A comma separates the two 1s in the middle of the OID.

Step 9 Perform one of the following procedures:

a) If you are using Windows Certificate Authority 2003, in Key Options check the **Store certificate in the local computer certificate store** check box.

b) If you are using Windows Certificate Authority 2008, refer to the workaround described in this sections Troubleshooting Tips.

Step 10 Enter a friendly name.

Step 11 Click **Submit**.

What to do next

Download Certificate from CA Server, on page 11

Download Certificate from CA Server

Before you begin

Complete the steps in Request Certificate from CA Server, on page 11

Procedure

Step 1 Launch the CA console by choosing **Start** > **Administrative Tools** > **Certificate Authority**.

Step 2 In the left pane, click on **Pending Requests**.

Step 3 In the right pane, right-click on the certificate request that you submitted.

Step 4 Choose **All Tasks** > **Issue**.

Step 5 Open `http://local_server/certsrv` on the Access Edge server that CA is running on.

Step 6 Click **View the Status of a Pending Certificate Request** then click your certificate request.

Step 7 Click **Install this certificate**.

What to do next

Upload a Certificate onto Access Edge, on page 12

Upload a Certificate onto Access Edge

This procedure describes how to upload the certificate on the Access Edge server using the Certificate Wizard. You can also import the certificates manually on the Access Edge server by choosing **Microsoft Office Communications Server 2007** > **Properties** > **Edge Interfaces**.

Before you begin

Complete the steps in Download Certificate from CA Server, on page 11

Procedure

Step 1 Choose **Start** > **Administrative Tools** > **Computer Management** on the Access Edge server.

Step 2 In the left pane, right-click on **Microsoft Office Communications Server 2007**.

Step 3 Click **Certificates**.

Step 4 Click **Next**.

Step 5 Click the **Assign an existing certificate** task option.

Step 6 Click **Next**.

Step 7 Choose the certificate that you wish to use for the External Access Edge Interface, and click **Next**.

Step 8 Click **Next**.

Step 9 Check the **Edge Server Public Interface** check box, and click **Next**.

Step 10 Click **Next**.

Step 11 Click **Finish**.

What to do next -

TLS Proxy Configuration on the Cisco Adaptive Security Appliance

Create Custom Certificate for Access Edge Using Enterprise Certificate Authority

Refer to these instructions if you are using a Microsoft Enterprise CA to issue a client/server role certificate to the external interface of Access Edge or to the public interface of the Cisco Adaptive Security Appliance.

Before you begin

These steps require that the Certificate Authority (CA) is an Enterprise CA and is installed on the Enterprise Edition of either Windows Server 2003 or 2008.

For additional details about these steps, refer to the Microsoft instructions:
http://technet.microsoft.com/en-us/library/bb694035.aspx

Procedure

	Command or Action	Purpose
Step 1	Perform the steps as mentioned above.	

Create and Issue a Custom Certificate Template

Procedure

Step 1 Follow Steps 1- 6 from the Microsoft site: Creating and Issuing the Site Server Signing Certificate Template on the Certification Authority.

http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver1

Tip For Step 5, use a more appropriate name for this specific template, such as Mutual Authentication Certificate.

Step 2 Follow these steps in place of Steps 7-12 from the Microsoft site:

a) Choose the **Extensions** tab. Make sure that under **Application Policies** that both **Client Authentication** and **Server Authentication** are present and that no other Policies are present. If these policies are not available, then you must add them before proceeding.

- In the **Edit Application Policies Extension** dialog box, click **Add**.
- In the **Add Application Policy** dialog box, choose **Client Authentication**, press Shift and choose **Server Authentication**, and then click **Add**.
- In the **Edit Application Policies Extension** dialog box, choose any other policy that may be present and then click **Remove**.

In the **Properties of New Template** dialog box, you should now see listed as the description of Application Policies: Client Authentication, Server Authentication.

b) Choose the **Issuance Requirement** tab. If you do not want the Certificate to be automatically issued, then choose **CA certificate manager approval**. Otherwise, leave this option blank.
c) Choose the **Security** tab and ensure that all required users and groups have both read and enroll permission.
d) Choose the **Request Handling** tab and click the **CSP** button.
e) On the **CSP Selection** dialog box choose **Requests must use one of the following CSP's**.
f) From the list of CSP's choose **Microsoft Basic Cryptographic Provider v1.0 and Microsoft Enhanced Cryptographic Provider v1.0**, and click **OK**.

Step 3 Continue with Steps 13-15 from the Microsoft site: Creating and Issuing the Site Server Signing Certificate Template on the Certification Authority.

http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver1

What to do next

Request Site Server Signing Certificate, on page 14

Request Site Server Signing Certificate

Procedure

Step 1 Follow Steps 1-6 from the Microsoft site: Site Server Signing Certificate for the Server That Will Run the Configuration Manager 2007 Site Server.

http://technet.microsoft.com/en-us/library/bb694035.aspx#BKMK_siteserver2

Tip For Step 5, select the name of the certificate template you created previously, such as Mutual Authentication Certificate and enter the external FQDN of the access edge in the **Name** field.

Step 2 Follow these steps in place of Steps 7-8 from the Microsoft site:

a) If the certificate request is automatically issued then you are presented with an option to install the signed certificate. Select **Install this Certificate**.

b) If the certificate request is not automatically issued then you must wait for the administrator to issue the certificate. Once issued:

- On the member server, load Internet Explorer and connect to the Web enrollment service with the address `http://<server>/certsrv` where `<server>` is the name or IP address of the Enterprise CA.
- On the Welcome page, choose **View the status of a pending certificate request**.

c) Choose the issued certificate and click **Install this Certificate**.

Security Certificate Configuration on Lync Edge Server for TLS Federation

The following guide from Microsoft's TechNet Library (http://technet.microsoft.com/en-us/library/gg398409.aspx) explains how to configure certificates on Access Edge for TLS federation with Microsoft Lync. The IM and Presence Service requires Mutual TLS authentication for federated connections, therefore you must configure Microsoft Lync certificates to support both Server and Client Authentication. You can use this guide to configure Lync Server to federate directly with the IM and Presence Service over TLS.

For information about how to configure static routes on Lync server for direct federation, see Configure a Static Route from Lync to IM and Presence.