Main page: Cisco Unified Presence, Release 7.x

Contents

◊ 6.3.2 Related Topics

Previous Topic

- How to Configure Security Certificates for Cisco Unified Presence to Microsoft OCS Federation (with Cisco Adaptive Security Appliance)

The procedures described in this section are an example, and demonstrates 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
- Configuring the Certificate on Cisco Adaptive Security Appliance using SCEP Enrollment
- Configuring the Certificate on Cisco Adaptive Security Appliance using Manual Enrollment
- How to Configure the Certificate for External Access Edge Interface
- How to Create a Custom Certificate for Access Edge Using an Enterprise Certificate Authority

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 indicate that you will paste the certificate received from the CA into the terminal. Both enrollment method procedures are described in this section. Refer to the *Cisco Security 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. The SCEP add-on must be installed on the Microsoft CA that you are configuring the certificates on.
http://www.microsoft.com/Downloads/details.aspx?familyid=9F306763-D036-41D8-8860-1636411B2D01&displaylang=

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 will use this URL during trustpoint enrollment on Cisco Adaptive Security Appliance.

Related Topics

- Common Cisco Adaptive Security Appliance Problems and Recommended Actions
- Getting More Information

Configuring the Certificate on Cisco Adaptive Security Appliance using SCEP Enrollment

Procedure

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

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

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

```
crypto ca trustpoint <trustpoint_name>
```

3. Use the "client-types" sub-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
```

4. Enter this command to configure the FQDN of the public Cisco Unified Presence address:

```
fqdn <fqdn_public_cup_address>
```

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

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

```
keypair public_key_for_ca
```

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

```
enrollment url http://<ip address of CA>/certsrv/mscep/mscep.dll
```

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
```

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.
```

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

```
crypto ca enroll <trustpoint_name>
```

10. 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.
```

11. 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..
```

12. 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: **********
Re-enter password: **********
```

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

14. 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
```

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

Related Topics

- Common Cisco Adaptive Security Appliance Problems and Recommended Actions
- Getting More Information

What To Do Next

How to Configure the Certificate for External Access Edge Interface

Configuring the Certificate on Cisco Adaptive Security Appliance using Manual Enrollment

Procedure

1. Enter this sequence of commands to generate a trustpoint to identify the CA:

```
crypto ca trustpoint <name of trustpoint>
fqdn <fqdn_public_cup_address>
client-types ssl
keypair public_key_for_ca
```

Notes:

- The FQDN value must be the FQDN of the public Cisco Unified Presence address.
- The keypair value must be the keypair created for the CA.

2. Enter this command to configure the enrollment method for the trustpoint:

```
enrollment terminal
```

3. Enter this command to authenticate the certificate:

```
crypto ca authenticate <trustpoint_name>
```

4. Acquire the root certificate of the CA:

- Go to your CA webpage, for example, http(s)://<CA_IP_Addr>/certsrv.
- Select Download a CA certificate, certificate chain, or CRL.
- Select Base 64.
- Download the CA certificate.
- Save the certificate as a .cer file, for example CARoot.cer.

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

6. Copy and paste this certificate into the Cisco Adaptive Security Appliance terminal.

7. Enter yes when you are prompted to accept the certificate.

8. Enter this command to send an enrollment request to the CA:

```
crypto ca enroll <trustpoint_name>
```

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

10. Enter yes when you are asked to Display Certificate Request to terminal.

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

12. Enter no when you are asked to redisplay the enrollment request.

13. Enter this command to import the certificate that you receive from the CA:

```
crypto ca <trustpoint_name> import certificate
```

14. Enter yes when you are asked if you want to continue with the enrollment.

15. Paste the base-64 certificate (that you copied in step 11) into the certificate request page of your CA:

- Go to your CA webpage, for example, http(s)://<CA_IP_Addr>/certsrv.
- Select **Request a certificate**.
- Select **Advanced Certificate request**.
- Select **Submit a certificate request by using a base-64-encoded CMC orPKCS#10 file...**
- Paste the base-64 certificate (that you copied in step 11).
- Submit the request and issue the certificate from the CA.
- Download the certificate and save as a *.cer file.
- Open the certificate in a text editor and paste the contents into the terminal. End with the word 'quit' on a separate line.

Related Topics

- Common Cisco Adaptive Security Appliance Problems and Recommended Actions
- Getting More Information

What To Do Next

How to Configure the Certificate for External Access Edge Interface

How to Configure the Certificate for External Access Edge Interface

Downloading the CA Certification Chain

Procedure

1. Click **Start > Run**.
2. Enter **http://<name of your Issuing CA Server>/certsrv**, and click **OK**.
3. Click **Download a CA certificate, certificate chain, or CRL** from the Select a task menu.
4. Click **Download CA certificate chain** from Download a CA Certificate, Certificate Chain, or CRL menu.
5. Click **Save** in the File Download dialog box.

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:
    - ♦ name of Standalone root CA certificate
    - ♦ name of Standalone subordinate CA certificate (if any)

Related Topics

- Common Cisco Adaptive Security Appliance Problems and Recommended Actions
- Getting More Information

What To Do Next

Installing the CA Certification Chain

Installing the CA Certification Chain

Before You Begin

Download the CA certificate chain.

Procedure

1. Click **Start > Run**.
2. Enter **mmc**, and click **OK**.
3. Select **Add/Remove Snap-in** from the File menu.
4. Click **Add** in the Add/Remove Snap-in dialog box.
5. Select **Certificates** in the list of Available Standalone Snap-ins.
6. Click **Add**.
7. Select **Computer account.**
8. Click **Next**.
9. In the Select Computer dialog box, perform the following tasks:
    1. Ensure that **<Local Computer>** (the computer this console is running on) is selected
    2. Click **Finish**.
10. Click **Close**.
11. Click **OK**.
12. In the left pane of the Certificates console, expand **Certificates:** ***Local Computer*** .
13. Expand Trusted Root Certification Authorities.
14. Right-click **Certificates**, and point to All Tasks.
15. Click **Import**.
16. In the Import Wizard, click **Next**.
17. Click **Browse** and go to where you saved the certificate chain.
18. Select the file, and click **Open**.
19. Click **Next**.
20. Leave the default value **Place all certificates in the store** and ensure that Trusted Root Certification Authorities appears under the Certificate store.
21. Click **Next**.
22. Click **Finish**.

Related Topics

- Getting More Information

What To Do Next

Requesting a Certificate from the CA Server

Requesting a Certificate from the CA Server

Before You Begin

Install the CA certificate chain.

Procedure

1. Log in to the Access Edge server and open a web browser.
2. Open the following URL: **http://<ca_server_IP_address>/certsrv**
3. Click **Request a Certificate**.
4. Click **Advanced Certificate Request**.
5. Click **Create and submit a request to this CA**.
6. Click **Other** in the Type of Certificate Needed list.
7. Enter the FQDN of the Access Edge external interface for the Subject Common Name,
8. Enter the following OID in the OID field:
   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.
9. Perform one of the following procedures:
   1. If you are using Windows Certificate Authority 2003, check **Store certificate in the local computer certificate store** in Key Options.
   2. If you are using Windows Certificate Authority 2008, refer to the workaround described in the Troubleshooting Tips of this section. Enter a friendly name.
10. Enter a friendly name.
11. Click **Submit**.

Related Topics

- Getting More Information

What To Do Next

Downloading the Certificate from the CA Server

Downloading the Certificate from the CA Server

Previous Topic

- Requesting a Certificate from the CA Server

Before You Begin

Request a certificate from the CA server.

Procedure

1. Launch the CA console by selecting **Start -> Administrative Tools -> Certificate Authority**.
2. Click on **Pending Requests** in the left pane.
3. Right-click on the certificate request that you submitted in the right pane.
4. Click **All Tasks > Issue**.
5. Open **http://<local_server>/certsrv** on the Access Edge server that CA is running on.
6. Click on your certificate request from **View the Status of a Pending Certificate Request**.
7. Click **Install this certificate**.

Related Topics

- Getting More Information

What To Do Next

Uploading the Certificate onto Access Edge

Uploading the 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 selecting **Microsoft Office Communications Server 2007 > Properties > Edge Interfaces.**

Before You Begin

Download the certificate from the CA server.

Procedure

1. Select **Start > Administrative Tools > Computer Management** on the Access Edge server.
2. Right-click on **Microsoft Office Communications Server 2007** in the left pane.
3. Click **Certificates**.
4. Click **Next**.
5. Click the **Assign an existing certificate** task option.
6. Click **Next**.
7. Select the certificate that you wish to use for the External Access Edge Interface, and click **Next**.
8. Click **Next**.
9. Click the **Edge Server Public Interface** checkbox, and click **Next**.
10. Click **Next**.
11. Click **Finish**.

Related Topics

- Getting More Information

What To Do Next

Configuring the TLS Proxy on Cisco Adaptive Security Appliance

How to Create a Custom Certificate for Access Edge Using an Enterprise Certificate Authority

Refer to these instructions if you are using a Microsoft Enterprise Certificate Authority 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 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

- Creating and Issuing a Custom Certificate Template
- Requesting the Site Server Signing Certificate

Creating and Issuing a Custom Certificate Template

Procedure

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

2. Follow these steps in place of Steps 7-12 from the Microsoft site:
    1. Select 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, select **Add**.
        - ◊ In the **Add Application Policy** dialog box, select Client Authentication, press Shift and select **Server Authentication**, and then select **Add**.
        - ◊ In the **Edit Application Policies Extension** dialog box, select any other policy that may be present and then select **Remove**.
    2. Select the **Issuance Requirement** tab. If you do not want the Certificate to be automatically issued, then select **CA certificate manager approval**. Otherwise, leave this option blank.
    3. Select the **Security** tab and ensure that all required users and groups have both read and enroll permission.
    4. Select the **Request Handling** tab and select the CSP button.
    5. On the **CSP Selection** dialog box select **Requests must use one of the following CSP?s**.
    6. From the list of CSP?s select **Microsoft Basic Cryptographic Provider v1.0 and Microsoft Enhanced Cryptographic Provider v1.0**, and select **OK**.
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

Related Topics

- Getting More Information

What To Do Next

Requesting the Site Server Signing Certificate

Requesting the Site Server Signing Certificate

Procedure

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. 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.
2. Follow these steps in place of Steps 7-8 from the Microsoft site:
    1. If the certificate request is automatically issued then you will be presented with an option to install the signed certificate. Select **Install this Certificate**.
    2. If the certificate request is not automatically issued then you will need to 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, select **View the status of a pending certificate request**.
    3. Select the issued certificate and select **Install this Certificate**.

Related Topics

- Getting More Information