Configuring Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge Using VeriSign

June 18, 2013

How to Configure the Security Certificates on Cisco Adaptive Security Appliance

Deleting the Old Certificates and Trustpoints

This procedure describes how to delete the old intermediate and signed certificate, and the trustpoint for the root certificate on Cisco Adaptive Security Appliance.

Before You Begin

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

- Configuring Cisco Unified Presence for SIP Federation, page 4-1
- Configuring Cisco Adaptive Security Appliance for SIP Federation, page 6-1

Procedure

Step 1 Enter config mode, type:

```
>Enable
>password
>config t
```

Step 2 Enter this command to display the trustpoints:

```
show crypto ca trustpoints
```

Step 3 Enter this command to delete the trustpoint and associated certificates:

```
no crypto ca trustpoint <name of trustpoint>
```

The following warning output displays:

```
WARNING: Removing an enrolled trustpoint will destroy all
certificates received from the related Certificate Authority.
```

Step 4 Enter **yes** when you are prompted to delete the trustpoint.

What To Do Next

Generating a New Trustpoint for VeriSign, page B-2

Generating a New Trustpoint for VeriSign

Procedure

Step 1 Enter config mode, type:

```
>Enable
>password
>config t
```

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

```
crypto key generate rsa label keys_for_verisign
```

Step 3 Enter the following sequence of commands to create a trustpoint for Cisco Unified Presence:

```
crypto ca trustpoint <name of trustpoint>
(config-ca-trustpoint)# enrollment terminal
(config-ca-trustpoint)# subject-name cn=<fqdn>,
OU=<organisational_unit>,O=<organisation_name>,C=<country>,St=<state>,L=<locality>
(config-ca-trustpoint)# keypair keys_for_verisign
(config-ca-trustpoint)# fqdn none
(config-ca-trustpoint)# exit
```

Note If you are submitting a renewal certificate signing request (CSR) file to VeriSign, the subject-name value must contain the following information:

- Country (two letter country code only)
- State (no abbreviations)
- Locality (no abbreviations)
- Organization Name
- Organizational Unit
- Common Name (FQDN) - This value must be the FQDN of the public Cisco Unified Presence.

Troubleshooting Tips

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

What To Do Next

Importing the Intermediate Certificate, page B-6

Importing the Root Certificate

Before You Begin

Complete the steps in Generating a New Trustpoint for VeriSign, page B-2.

Procedure

Step 1 Enter config mode, type:

```
>Enable
>password
>config t
```

Step 2 Enter this command to import the certificate onto Cisco Adaptive Security Appliance:

```
crypto ca authenticate  <name of trustpoint>
```

Step 3 Enter the CA certificate, for example:

```
-----BEGIN CERTIFICATE-----
MIIDAzCCAmwCEQC5L2DMiJ+hekYJuFtwbIqvMA0GCSqGSIb3DQEBBQUAMIH...
-----END CERTIFICATE-----
quit
```

Note Finish with the word "quit" on a separate line.

Step 4 Enter **yes** when you are prompted to accept the certificate.

What To Do Next

Generating the Certificate Signing Request, page B-4

Generating the Certificate Signing Request

Before You Begin

Complete the steps in Importing the Root Certificate, page B-3.

Procedure

Step 1 Enter config mode, type:

```
>Enable
>password
>config t
```

Step 2 Enter this command to send an enrollment request to the CA:

```
crypto ca enroll <name of trustpoint>
```

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

```
% Start certificate enrollment..
% The subject name in the certificate will be: <fqdn>,
OU=<organisational_unit>,O=<organisation_name>,C=<country>,St=<state>,L=<locality>
```

Step 4 Enter **no** when you are prompted to include the device serial number in the subject name.

Step 5 Enter **yes** when you are prompted to display the certificate request in the terminal.

The certificate request displays.

What To Do Next

Submitting the Certificate Signing Request to VeriSign, page B-4

Submitting the Certificate Signing Request to VeriSign

When you submit the Certificate Signing Request, VeriSign will provide you with the following certificate files:

- verisign-signed-cert.cer (signed certificate)
- trial-inter-root.cer (subordinate intermediate root certificate)
- verisign-root-ca.cer (root CA certificate)

Save the certificate files in separate notepad files once you have downloaded them.

Before You Begin

- Complete the steps in Generating the Certificate Signing Request, page B-4.
- You will need the challenge password that you defined when generating the Certificate Signing Request.

Procedure

Step 1 Go to the VeriSign website.

Step 2 Follow the procedure to enter a Certificate Signing Request.

Step 3 When prompted, submit the challenge password for the Certificate Signing Request.

Step 4 Paste the Certificate Signing Request into the window provided.

Note You need to paste from **-----BEGIN CERTIFICATE-----** to **-----END CERTIFICATE-----** inclusive.

What To Do Next

Deleting the Certificate Used for the Certificate Signing Request, page B-5

Deleting the Certificate Used for the Certificate Signing Request

You must delete the temporary root certificate used to generate the Certificate Signing Request.

Before You Begin

Complete the steps in Submitting the Certificate Signing Request to VeriSign, page B-4.

Procedure

Step 1 Enter config mode, type:

```
>Enable
>password
>config t
```

Step 2 Enter this command to display the certificates:

```
show running-config crypto ca
look for crypto ca certificate chain <name of trustpoint>
```

Step 3 Enter this command to delete the certificate:

```
(config)# crypto ca certificate chain <name of trustpoint>
(config-cert-chain)#  no certificate ca 00b92f60cc889fa17a4609b85b70$
```

The following warning output displays:

```
WARNING: The CA certificate will be disassociated from this trustpoint and
will be removed if it is not associated with any other trustpoint.  Any
other certificates issued by this CA and associated with this trustpoint
will also be removed.
```

Step 4 Enter **yes** when you are prompted to delete the trustpoint.

What To Do Next

Importing the Intermediate Certificate, page B-6

Importing the Intermediate Certificate

Before You Begin

Complete the steps in Deleting the Certificate Used for the Certificate Signing Request, page B-5.

Procedure

Step 1 Enter config mode, type:

```
>Enable
>password
>config t
```

Step 2 Enter this command to import the certificate onto Cisco Adaptive Security Appliance:

```
crypto ca authenticate <name of trustpoint>
```

Step 3 Enter the CA certificate, for example:

```
-----BEGIN CERTIFICATE-----
MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0BAQU....
-----END CERTIFICATE-----
quit
```

Note Finish with the word "quit" on a separate line.

Step 4 Enter **yes** when you are prompted to accept the certificate.

What To Do Next

Creating a Trustpoint for the Root Certificate, page B-6

Creating a Trustpoint for the Root Certificate

Before You Begin

Complete the steps in Importing the Intermediate Certificate, page B-6.

Step 1 Enter config mode, type:

```
>Enable
>password
>config t
```

Step 2 Enter this command to generate the trustpoint:

```
crypto ca trustpoint verisign_root
```

Step 3 Enter the following sequence of commands:

```
(config-ca-trustpoint)# revocation-check none
(config-ca-trustpoint)# keypair keys_for_verisign
(config-ca-trustpoint)# enrollment terminal
(config-ca-trustpoint)# exit
```

Importing the Root Certificate

Before You Begin

Complete the steps in Creating a Trustpoint for the Root Certificate, page B-6.

Procedure

Step 1 Enter config mode, type:

```
>Enable
>password
>config t
```

Step 2 Enter this command to import the certificate onto Cisco Adaptive Security Appliance:

```
crypto ca authenticate  verisign_root
```

Step 3 Enter the CA certificate, for example:

```
-----BEGIN CERTIFICATE-----
MIICmDCCAgECECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQECBQAw....
-----END CERTIFICATE-----
quit
```

Note Finish with the word "quit" on a separate line.

Step 4 Enter **yes** when you are prompted to accept the certificate.

What To Do Next

Importing the Signed Certificate, page B-7

Importing the Signed Certificate

Before You Begin

Complete the steps in Importing the Root Certificate, page B-7.

Procedure

Step 1 Enter config mode, type:

```
>Enable
>password
>config t
```

Step 2 Enter this command to import the certificate onto Cisco Adaptive Security Appliance:

```
crypto ca import verisignca certificate
```

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 3 Enter **yes** when you are prompted to continue with the certificate enrollment.

Step 4 Enter the CA certificate, for example:

```
-----BEGIN CERTIFICATE-----
MIIFYTCCBEmgAwIBAgIQXtEPGWzZ0b9gejHejq+HazANBgkqhkiG9w0B....
-----END CERTIFICATE-----
quit
```

Note Finish with the word "quit" on a separate line.

Step 5 Enter **yes** when you are prompted to accept the certificate.

What To Do Next

Importing the VeriSign Certificates onto Microsoft Access Edge, page B-8

Importing the VeriSign Certificates onto Microsoft Access Edge

This procedure describes how to import the VeriSign root and intermediate certificates onto the Microsoft Access Edge server.

Before You Begin

Save the certificates that were provided by VeriSign to the Access Edge server, for example, in C:\.

Procedure

Step 1 On the Access Edge server, enter **mmc** from the run command.

Step 2 Select **File-> Add/Remove Snap-in**.

Step 3 Click **Add**.

Step 4 Click **Certificates**.

Step 5 Click **Add**.

Step 6 Select **Computer account**.

Step 7 Click **Next**.

Step 8 Select **Local computer**.

Step 9 Click **Finish**.

Step 10 Click **OK** to close the Add/Remove Snap-In window.

Step 11 In the main console, expand the Certificates tree.

Step 12 Open the **Trusted Root Certificates** branch.

Step 13 Right-click on **Certificates.**

Step 14 Select **All Tasks > Import**.

Step 15 Click **Next** on the certificate wizard.

Step 16 Browse for a VeriSign certificate in the C:\ directory.

Step 17 Click **Place all certificates in the following store**.

Step 18 Select **Trusted Root Certification Authorities** as the certificate store.

Step 19 Repeat steps 13 to 18 to import the additional VeriSign certificates.