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

This section provides information on the Security Certificate Exchange Between the Cisco Adaptive Security Appliance and Microsoft Access Edge Using VeriSign.

Security Certificate Configuration on Cisco Adaptive Security Appliance

This section explains the Security Certificate Configuration on Cisco Adaptive Security Appliance.

Delete 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:

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

Procedure

Step 1 Enter configuration mode:

```
> Enable
> <password>
```

```
> configure terminal
```

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 trustpoint_name
```

The following warning output displays:

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

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

What to do next

Generate New Trustpoint for VeriSign, on page 2

Generate New Trustpoint for VeriSign

Procedure

Step 1 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 keys_for_verisign
```

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

```
(config)# crypto ca trustpoint trustpoint_name
(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 IM and Presence Serivce.

Troubleshooting Tips

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

What to do next

Import Intermediate Certificate, on page 6

Import Root Certificate

Before you begin

Complete the steps in Generate New Trustpoint for VeriSign, on page 2.

Procedure

Step 1 Enter configuration mode:

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

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

```
crypto ca authenticate trustpoint_name
```

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

Generate Certificate Signing Request, on page 4

Generate Certificate Signing Request

Before you begin

Complete the steps in Import Root Certificate, on page 3.

Procedure

Step 1 Enter configuration mode:

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

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

```
(config)# crypto ca enroll trustpoint_name
```

The following warning output displays:

```
%WARNING: The certificate enrollment is configured with an fqdnthat 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

Submit Certificate Signing Request to VeriSign, on page 4

Submit Certificate Signing Request to VeriSign

When you submit the Certificate Signing Request, VeriSign provides 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 Generate Certificate Signing Request, on page 4.
- You must have 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 must paste from **-----BEGIN CERTIFICATE-----** to **-----END CERTIFICATE-----** inclusive.

What to do next

Delete Certificate Used for Certificate Signing Request, on page 5

Delete Certificate Used for Certificate Signing Request

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

Before you begin

Complete the steps in Submit Certificate Signing Request to VeriSign, on page 4.

Procedure

Step 1 Enter configuration mode:

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

Step 2 Enter this command to display the certificates:

```
(config)# show running-config crypto calook for crypto ca certificate chain trustpoint_name
```

Step 3 Enter this command to delete the certificate:

```
(config)# crypto ca certificate chain trustpoint_name
(config-cert-chain)# no certificate ca 00b92f60cc889fa17a4609b85b70$
```

The following warning output displays:

```
WARNING: The CA certificate will be disassociated from this trustpoint andwill 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

Import Intermediate Certificate, on page 6

Import Intermediate Certificate

Before you begin

Complete the steps in Delete Certificate Used for Certificate Signing Request, on page 5.

Procedure

Step 1 Enter configuration mode:

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

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

```
crypto ca authenticate trustpoint_name
```

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

Create a Trustpoint for Root Certificate, on page 7

Create a Trustpoint for Root Certificate

Before you begin

Complete the steps in Import Intermediate Certificate, on page 6.

Procedure

Step 1 Enter configuration mode:

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

Step 2 Enter this command to generate the trustpoint:

```
(config)# crypto ca trustpoint verisign_root
(config-ca-trustpoint)#
```

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
```

Import a Root Certificate

Before you begin

Complete the steps in Create a Trustpoint for Root Certificate, on page 7.

Procedure

Step 1 Enter configuration mode:

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

Step 2 Enter this command to import the certificate onto the 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

Import Signed Certificate, on page 8

Import Signed Certificate

Before you begin

Complete the steps in Import a Root Certificate, on page 7.

Procedure

Step 1 Enter configuration mode:

> **Enable**

> *<password>*

> **configure terminal**

Step 2 Enter this command to import the certificate onto the 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

Import VeriSign Certificates onto Microsoft Access Edge, on page 9

Import 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 Choose **File** > **Add/Remove Snap-in**.
Step 3 Click **Add**.
Step 4 Click **Certificates**.
Step 5 Click **Add**.
Step 6 Choose **Computer account**.
Step 7 Click **Next**.
Step 8 Choose **Local computer**.
Step 9 Click **Finish**.
Step 10 To close the **Add/Remove Snap-In** window., click **OK**.
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 Choose **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 As the certificate store, choose **Trusted Root Certification Authorities**.
Step 19 Repeat steps 13 to 18 to import the additional VeriSign certificates.