Main page: Cisco Unified Presence, Release 7.x

Contents

- 1 Previous Topic
- 2 Generating the Key Pair and Trustpoints on Cisco Adaptive Security Appliance
  - 2.1 Before You Begin
  - 2.2 Procedure
  - 2.3 Related Topics
  - 2.4 Troubleshooting Tip
  - 2.5 What To Do Next
- 3 Generating a Self-Signed Certificate on Cisco Adaptive Security Appliance
  - 3.1 Before You Begin
  - 3.2 Procedure
  - 3.3 Related Topics
  - 3.4 What To Do Next
  - 3.5 Importing the Self Signed Certificate onto Cisco Unified Presence
    - 3.5.1 Before You Begin
    - 3.5.2 Procedure
    - 3.5.3 Troubleshooting Tips
    - 3.5.4 Related Topics
    - 3.5.5 What To Do Next
  - 3.6 Generating a New Certificate on Cisco Unified Presence
    - 3.6.1 Before You Begin
    - 3.6.2 Procedure
    - 3.6.3 Related Topics
    - 3.6.4 What To Do Next
  - 3.7 Importing the Cisco Unified Presence Certificate onto Cisco Adaptive Security Appliance
    - 3.7.1 Before You Begin
    - 3.7.2 Procedure
    - 3.7.3 Troubleshooting Tips
    - 3.7.4 Related Topics
    - 3.7.5 What To Do Next

Previous Topic

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

- Generating the Key Pair and Trustpoints on Cisco Adaptive Security Appliance
- Generating a Self-Signed Certificate on Cisco Adaptive Security Appliance
- Importing the Self Signed Certificate onto Cisco Unified Presence
- Generating a New Certificate on Cisco Unified Presence
- Importing the Cisco Unified Presence Certificate onto Cisco Adaptive Security Appliance

Generating the Key Pair and Trustpoints on Cisco Adaptive Security Appliance

You need to generate the key pair for this certification (for example **cup_proxy_key**), and configure a trustpoint to identify the self-signed certificate from Cisco Adaptive Security Appliance to Cisco Unified Presence (for example **cup_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:

- Configuring Cisco Unified Presence for Federation
- Configuring Cisco Adaptive Security Appliance for this Integration

Procedure

1. Enter config mode, type:

```
>Enable

>password

>config t
```

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

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

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

```
crypto ca trustpoint <name of trustpoint e.g.cup_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 cup_proxy_key
```

Related Topics

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

Troubleshooting Tip

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

What To Do Next

Generating a Self-Signed Certificate on Cisco Adaptive Security Appliance

Generating a Self-Signed Certificate on Cisco Adaptive Security Appliance

Before You Begin

- Complete the steps in Generating the Key Pair and Trustpoints on Cisco Adaptive Security Appliance.
- 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

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

   (config-ca-trustpoint)# crypto ca enroll <*name of trustpoint e.g.cup_proxy*>

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

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

4. Enter this command to prepare the certificate to export to Cisco Unified Presence:

   crypto ca export cup_proxy identity-certificate

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

   -----BEGIN CERTIFICATE-----

   MIIBnDCCAQWgAwIBAgIBMTANBgkqhkiG9w0BAQQFADAUMRIwEAYDVQQDEwlDVVAt.....

   -----END CERTIFICATE-----

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

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

Related Topics

- Getting More Information

What To Do Next

Importing the Self Signed Certificate onto Cisco Unified Presence

Importing the Self Signed Certificate onto Cisco Unified Presence

Before You Begin

Generate a self-signed certificate on the Cisco Adaptive Security Appliance.

Procedure

1. Select **Cisco Unified Operating System Administration > Security > Certificate Management** on Cisco Unified Presence.
2. Click **Upload Certificate**.
3. Select **sipproxy-trust** for Certificate Name.
   Note: Leave the Root Name field blank.
4. Click **Browse**, and locate the Cisco Adaptive Security Appliance .pem certificate file (that you created in the previous procedure) on your local computer.
5. Click **Upload File** to upload the certificate to the Cisco Unified Presence server.

Troubleshooting Tips

Perform a find on the certificate list, you will see an <*asa ip address*>.pem and an <*asa ip address*>.der in the certificate list.

Related Topics

- Getting More Information

What To Do Next

Generating a New Certificate on Cisco Unified Presence

Generating a New Certificate on Cisco Unified Presence

Before You Begin

Import the self-signed certificate onto Cisco Unified Presence.

Procedure

1. Select **Cisco Unified Operating System Administration > Security > Certificate Management** on Cisco Unified Presence.
2. Click **Generate New**.
3. Select **sipproxy** for the certificate name.

Related Topics

- Getting More Information

What To Do Next

Importing the Cisco Unified Presence Certificate onto Cisco Adaptive Security Appliance

Importing the Cisco Unified Presence Certificate onto Cisco Adaptive Security Appliance

In order to import the Cisco Unified Presence certificate onto Cisco Adaptive Security Appliance, you need to create a trustpoint to identify the imported certificate from Cisco Unified Presence (e.g. **cert_from_cup**), and specify the enrollment type as "terminal" to indicate that you will paste the certificate received from Cisco Unified Presence into the terminal.

Before You Begin

- Generate a new certificate on Cisco Unified Presence.
- 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

1. Enter config mode, type:

```
>Enable

>password

>config t
```

2. Enter this sequence of commands to create a trustpoint for the imported Cisco Unified Presence certificate:

```
crypto ca trustpoint cert_from_cup

enrollment terminal
```

3. Enter this command to import the certificate from Cisco Unified Presence:

```
crypto ca authenticate cert_from_cup
```

4. Select **Cisco Unified Operating System Administration > Security > Certificate Management** on Cisco Unified Presence.

5. Click **Find**.

6. Locate the sipproxy certificate that you created in the previous procedure.

7. Click **Download**.

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

9. Cut and paste the contents of the sipproxy.pem into the Cisco Adaptive Security Appliance prompt window.

10. Enter **quit**.

11. Enter **y** when you are prompted to accept the certificate.

Troubleshooting Tips

Run the command **show crypto ca certificate** to view the certificate.

Related Topics

- Getting More Information

What To Do Next

How to Configure Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge (External Interface) Using a Microsoft CA