Firepower Threat Defense Certificate-Based Authentication

- Requirements and Prerequisites for FTD Certificate-Based Authentication, on page 1
- Firepower Threat Defense VPN Certificate Guidelines and Limitations, on page 2
- Managing Firepower Threat Defense VPN Certificates, on page 2
- Installing a Certificate Using Self-Signed Enrollment , on page 3
- Installing a Certificate Using SCEP Enrollment, on page 4
- Installing a Certificate Using Manual Enrollment, on page 5
- Installing a Certificate by Importing a PKCS12 File, on page 6
- Troubleshooting Firepower Threat Defense VPN Certificates, on page 7

Requirements and Prerequisites for FTD Certificate-Based Authentication

Model Support

FTD

Supported Domains

Any

User Roles

Admin

Network Admin

Firepower Threat Defense VPN Certificate Guidelines and Limitations

- When a certificate enrollment object is associated with and then installed on a device, the process of certificate enrollment starts immediately. The process is automatic for self-signed and SCEP enrollment types, meaning it does not require any additional administrator action. Manual certificate enrollment and importing a PKCS12 file requires extra administrator action.
- When the certificate enrollment is complete, a trustpoint exists on the device with the same name as the certificate enrollment object. Use this trustpoint in the configuration of your VPN Authentication Method.
- Firepower Threat Defense currently supports RSA keys only, not ECDSA, even though the choice appears in the user interface.
- Since Firepower Threat Defense VPNs are not supported in a clustered environment, PKI is also not supported in a clustered environment.
- Firepower Threat Defense devices support certificate enrollment using Microsoft Certificate Authority(CA) Service, and CA Services provided on Cisco Adaptive Security Appliances(ASA) and Cisco IOS Router.
- Firepower Threat Defense devices cannot be configured as a certificate authority (CA).

Guidelines for Certificate Management Across Domains and Devices

- The Firepower Threat Defense devices support, and have been verified, certificate enrollment using, Microsoft CA Service, and CA Services provided on Cisco Adaptive Security Appliances and Cisco IOS Routes.
- Certificate enrollment can be done in a child or parent domain.
- When enrollment is done from a parent domain, the certificate enrollment object also needs to be in the same domain. If the trustpoint on a device is overridden in the child domain, the overridden value will be deployed on the device.
- When the certificate enrollment is done on a device in a leaf domain, the enrollment will not be visible to the parent domain another child domain.
- When a leaf domain is deleted, certificate enrollments on the contained devices have to be removed.
- Once a device has certificates enrolled in one domain, it will not be allowed to be enrolled in any other domain. However, the certificates can be viewed in the the other domain.
- When a device is moved from one domain to another domain, or from no domain into a domain, certificate enrollments on that device have to be removed and reconfigured in the new domain. You will receive an alert to delete the enrollments on these devices.

Managing Firepower Threat Defense VPN Certificates

See PKI Infrastructure and Digital Certificates for an introduction to Digital Certificates.

See Certificate Enrollment Objects for a description of the objects used to enroll and obtain certificates on managed devices.

Procedure

Step 1 Select **Devices** > **Certificates**.

You can see the following columns for each device listed on this screen:

- **Name**—Lists the devices that already have trustpoints associated with them. Expand the device to see the list of associated trustpoints.
- **Enrollment Type**—Displays the type of enrollment used for a trustpoint.
- **Status**—Provides the status of the **CA Certificate** and **Identity Certificate**. You can view the certificate contents, when `Available`, by clicking the magnifying glass.

  If the enrollment fails, click status to view the failure message.
- The additional columns provide the status of the **CA Certificate** and **Identity Certificate**. In each column, the certificate contents, when `Available`, can be viewed by clicking the magnifying glass.

  The values of these columns depend on the enrollment type and change during the process of enrollment. The CA Certificate can be `Available`, `Not Available`, and `Not Applicable`. The Identity Certificate status can be `Available`, `Pending`, and `Available and Pending` during a refresh.
- Refresh (circling arrows) a certificate on a managed device. Refreshing a certificate would synchronize the Firepower Threat Defense device certificate status to the Firepower Management Center.
- Delete (trash can) a configured certificate.

Step 2 Choose **(+) Add** > **Add New Certificate** to associate and install an enrollment object on a device. Continue based on the type of enrollment.

Note When a certificate enrollment object is associated with and then installed on a device, the process of certificate enrollment starts immediately. The process is automatic for self-signed and SCEP enrollment types, meaning it does not require any additional administrator action. Manual certificate enrollment and importing a PKCS12 file requires extra administrator action.

Related Topics

Installing a Certificate Using Self-Signed Enrollment , on page 3

Installing a Certificate Using SCEP Enrollment, on page 4

Installing a Certificate Using Manual Enrollment, on page 5

Installing a Certificate by Importing a PKCS12 File, on page 6

Installing a Certificate Using Self-Signed Enrollment

Procedure

Step 1 On the **Devices** > **Certificates** screen, choose **Add** > **Add New Certificate** to open the **Add New Certificate** dialog.

Step 2 Choose a device from the **Device** drop down list.

Step 3 Associate a certificate enrollment object with this device in one of the following ways:

- Choose a Certificate Enrollment Object of the appropriate type from the drop-down list.
- Click **(+)**, to add a new Certificate Enrollment Object, see Adding Certificate Enrollment Objects.

Step 4 Press **Install**, to start the Self Signed, automatic, enrollment process.

For self signed enrollment type trustpoints, the **CA Certificate** status will always be `NotApplicable` since the managed device is acting as its own CA and does not need a CA certificate to generate its own Identity Certificate.

The **Identity Certificate** will go from InProgress to Available as the device creates its own self signed identity certificate.

Step 5 Click the magnifying glass to view the self-signed Identity Certificate created for this device.

What to do next

When the certificate enrollment is complete, a trustpoint exists on the device with the same name as the certificate enrollment object. Use this trustpoint in the configuration of your VPN Authentication Method.

Installing a Certificate Using SCEP Enrollment

Before you begin

Note Using SCEP enrollment establishes a direct connection between the managed device and the CA server. So be sure your device is connected to the CA server before beginning the enrollment process.

Procedure

Step 1 Press **Install**, to start the automatic enrollment process.

Step 2 On the **Devices** > **Certificates** screen, choose **Add** > **Add New Certificate** to open the **Add New Certificate** dialog.

Step 3 Choose a device from the **Device** drop down list.

Step 4 Associate a certificate enrollment object with this device in one of the following ways:

- Choose a Certificate Enrollment Object of the appropriate type from the drop-down list.
- Click **(+)**, to add a new Certificate Enrollment Object, see Adding Certificate Enrollment Objects.

Step 5 Press **Install**, to start the automatic enrollment process.

For SCEP enrollment type trustpoints, the **CA Certificate** status will transition from InProgress to Available as the CA Certificate is obtained from the CA server and installed on the device.

The **Identity Certificate** will go from `InProgress` to `Available` as the device obtains its identity certificate using SCEP from the specified CA.

Note The SCEP certificate enrollment could possibly fail because of some error messages. For example:

```
Error:
crypto ca authenticate scep1 nointeractive:[error]:ERROR:receiving Certificate
Authority certificate: status = FAIL, cert length = 0
Possible
```

Some recommendations to overcome this situaton:

- Make sure that the connectivity to the SCEP Server from the FTD - Route is added to the SCEP Server.
- If the SCEP Server is referred with hostname/FQDN, configure DNS Server using FlexConfig object.
- Ensure that the SCEP Server and the FTD device are in time-sync by configuring the same NTP Server.

Step 6 Click the magnifying glass to view the Identity Certificate created and installed on this device.

What to do next

When the certificate enrollment is complete, a trustpoint exists on the device with the same name as the certificate enrollment object. Use this trustpoint in the configuration of your VPN Authentication Method.

Installing a Certificate Using Manual Enrollment

Procedure

Step 1 Press **Install** to start the enrollment process.

Step 2 On the **Devices** > **Certificates** screen, choose **Add > Add New Certificate** to open the **Add New Certificate** dialog.

Step 3 Choose a device from the **Device** drop down list.

Step 4 Associate a certificate enrollment object with this device in one of the following ways:

- Choose a Certificate Enrollment Object of the appropriate type from the drop-down list.
- Click **(+)**, to add a new Certificate Enrollment Object, see Adding Certificate Enrollment Objects.

Step 5 Press **Import**, to initiate the manual enrollment process.

The **CA Certificate** status will go from `InProgress` to `Available` as the Firepower Management Center installs the CA certificate (provided in the enrollment object) on the managed device, authenticates the CA Server, and creates a trustpoint on the managed device.

The **Identity Certificate** status could throw a warning message that CSR generation and identity certificate import is pending.

Step 6 Execute the appropriate activity with your PKI CA Server to obtain an identity certificate.

a) Click **Identity Certificate** warning to view and copy the CSR.

b) Execute the appropriate activity with your PKI CA Server to obtain an identity certificate using this CSR.

This activity is completely independent of the Firepower Management Center or the managed device. When complete, you will have an Identity Certificate for the managed device. You can copy it or place it in a file.

c) To finish the manual process, install the obtained identity certificate onto the managed device.

Return to the Firepower Management Center dialog to paste the Identity Certificate into its field. Or, select **Browse** to choose the identity certificate file.

Step 7 Select **Import** to import the Identity Certificate.

The Identity Certificate status will be `Available` when the import complete.

Step 8 Click the magnifying glass to view the **Identity Certificate** for this device.

What to do next

When the certificate enrollment is complete, a trustpoint exists on the device with the same name as the certificate enrollment object. Use this trustpoint in the configuration of your VPN Authentication Method.

Installing a Certificate by Importing a PKCS12 File

Procedure

Step 1 Go to **Devices > Certificates** screen, then click **+ Add > Import PKCS12 File** to open the **Import PKCS12 File** dialog.

Step 2 Choose a pre-configured managed device from the **Device** drop down list.

Step 3 Specify a **Certificate Enrollment** type of **PKCS12**.

Step 4 Select **Browse** to find and choose your PKCS#12 Certificate file.

Step 5 Enter the **Passphrase** for decryption.

Step 6 Press **Add**.

For file import, the CA Certificate and Identity Certificate status will go from `In Progress` to `Available` as it installs the PKCS12 file on the device.

Step 7 Once `Available`, click the magnifying glass to view the Identity Certificate for this device.

What to do next

The certificate (trustpoint) on the managed device is named the same as the PKCS#12 file. Use this certificate in your VPN authentication configuration.

Troubleshooting Firepower Threat Defense VPN Certificates

See Firepower Threat Defense VPN Certificate Guidelines and Limitations, on page 2 to determine if variations in your certificate enrollment environment may be causing a problem. Then consider the following:

- Ensure there is a route to the CA Server from the device.

  If the CA Server's host name is given in the Enrollment Object, use Flex Config to configure DNS appropriately to reach the server. Alternatively, use the IP Address of the CA Server.

- If you are using a Microsoft 2012 CA Server, the default IPsec Template is not accepted by the managed device and must be changed.

  To configure a working template, follow these steps as you use MS CA documentation as a reference.

  1. Duplicate the IPsec (Offline Request) template.
  2. In **Extensions > Application policies**, select *IP security end system*, instead of the *IP security IKE intermediate*.
  3. Set the permissions and the template name.
  4. Add the new template and change the registry settings to reflect the new template name.