

Certificates

- Secure Firewall Threat Defense VPN certificate guidelines and limitations, on page 1
- Manage Firewall Threat Defense certificates, on page 2
- Install a certificate using self-signed enrollment, on page 6
- Install a certificate using EST enrollment, on page 6
- Install a certificate using SCEP enrollment, on page 7
- Install a certificate using manual enrollment, on page 8
- Install a certificate using a PKCS12 file, on page 9
- Install a certificate using ACME enrollment, on page 10
- Troubleshoot Threat Defense certificates, on page 11

Secure Firewall Threat Defense VPN certificate guidelines and limitations

Certificate enrollment guidelines

When a PKI enrollment object is associated with and then installed on a device, the certificate enrollment process starts immediately. The process is automatic for self-signed and SCEP enrollment types; it does not require any additional administrator's action. Manual certificate enrollment requires administrator's action.

- When a PKI enrollment object is associated with and then installed on a device, the certificate enrollment process starts immediately. The process is automatic for self-signed and SCEP enrollment types; it does not require any additional administrator's action. Manual certificate enrollment requires administrator's action.
- When importing identity certificates into Firewall Threat Defense devices, the expiration date of the certificate must not exceed February 6, 2106. Ensure that all certificates used within devices have expiration dates earlier to February 6, 2106 to avoid issues during certificate import or renewal.
- 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.
- Firewall 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.
- Firewall Threat Defense devices cannot be configured as a certificate authority (CA).

Guidelines for certificates and multitenancy

Firewall Threat Defense devices support certificate enrollment using Microsoft CA Service, as well as CA services provided by Cisco Adaptive Security Appliances and Cisco IOS Routers.

Supported certificate enrollment services:

Certificate enrollment domains

- Certificate enrollment can be done in a **child domain** or a **parent domain**.
- When enrollment is done from a **parent domain**, the certificate enrollment object must also 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.

Enrollment visibility and behavior in leaf domains

- When certificate enrollment is done on a device in a **leaf domain**, the enrollment will be visible to the parent domain or another child domain.
- Adding additional certificates in a leaf domain is possible.

Certificate enrollment restrictions and permissions

- Once a device has certificates enrolled in one domain, it will be allowed to be enrolled in any other domain. The certificates can be added in the other domain.

Device movement between domains

- When you move a device from one domain to another, the certificates also get moved accordingly. You will receive an alert to delete the enrollments on these devices.

Manage Firewall Threat Defense certificates

This task enables you to manage certificates on devices including viewing certificate status, enrolling new certificates, and performing certificate operations such as export and re-enrollment.

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 Choose **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.
- **Domain**—Displays the certificates that are enrolled in a specific domain.

- **Enrollment Type**—Displays the type of enrollment used for a trustpoint.
- **Identity Certificate Expiry**—Displays the expiration date and certificate-health status of the identity certificate. If the certificate has expired, this column indicates how long ago it expired.
- **CA Certificate Expiry**—Displays the expiration date of the certificate authority (CA) certificate associated with the 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.

  When you view the CA certificate information, you can view the hierarchy of all the certifying authorities, which issued your CA certificate. If the enrollment fails, click status to view the failure message.
- Click **Enable weak-crypto** on the right to enable weak cipher usage in certificates. When you click the toggle button, you get a warning to confirm before enabling weak ciphers. Click **Yes** to enable weak ciphers.



Note When a certificate enrollment fails due to weak cipher usage, you get a prompt to enable the weak cipher. You can choose to enable weak cipher when you need to use weak encryption.

- The additional column lists icons to perform the following tasks:
  - **Export Certificate**—Click to export and download a copy of the certificate. You can choose to export the PKCS12 (Complete Certificate Chain) or the PEM (Identity Certificate Only) format.

    You must provide a pass phrase to export a PKCS12 certificate format to import the file later.
  - **Re-enroll certificate**—Re-enroll an existing certificate.
  - **Refresh certificate status**—Refresh a certificate to synchronize the device certificate status to the Cloud-Delivered Firewall Management Center.
  - **Delete certificate**—Delete all the associated certificates for a trustpoint.

Step 2 Click **Add** to associate and install an enrollment object on a device.

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 requires extra administrator action.



Note The certificate enrollment on a device does not block the user interface and the enrollment process gets executed in the background, enabling the user to perform certificate enrollment on other devices in parallel. The progress of these parallel operations can be monitored on the same user interface. The respective icons display the certificate enrollment status.

Related Topics

Install a certificate using self-signed enrollment, on page 6
Install a certificate using SCEP enrollment, on page 7
Install a certificate using manual enrollment, on page 8
Install a certificate using a PKCS12 file, on page 9

Automatically update CA bundles

You can set the management center to automatically update the CA certificates through CLI commands. By default, the CA certificates are automatically updated when you install or upgrade to version 7.0.5.

Note In an IPv6-only deployment, the automatic update of CA certificates may fail, because, some of the Cisco servers do not support IPv6. In such cases, force update the CA certificates using the **configure cert-update run-now force** command.

Procedure

Step 1 Log into the FMC CLI using SSH, or, if virtual, open the VM console.

Step 2 You can verify whether the CA certificates in the local system are the latest or not:

configure cert-update test

This command compares the CA bundle on the local system with the latest CA bundle (from the Cisco server). If the CA bundle is up to date, no connection check is executed and the test result is displayed as the one below:

Example:

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

If the CA bundle is out of date, the connection check is executed on the downloaded CA bundle and the test result is displayed.

Example:

When the connection check fails:

```
> configure cert-update test
Test failed, not able to fully connect.
```

Example:

When the connection check succeeds, or the CA bundle is already up to date:

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

Step 3 (Optional) To instantly update the CA bundles:

configure cert-update run-now

Example:

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

When you execute this command, the CA certificates (from the Cisco server) are verified for SSL connectivity. If the SSL connectivity check fails for even one of the Cisco servers, the process is terminated.

Example:

```
> configure cert-update run-now
Certs failed some connection checks.
```

To proceed with the update despite connection failures, use the **force** keyword.

Example:

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

Step 4 If you do not want the CA bundles to be automatically updated, disable the configuration:

configure cert-update auto-update disable

Example:

```
> configure cert-update auto-update disable
Autoupdate is disabled
```

Step 5 To re-enable the automatic update of CA bundles:

configure cert-update auto-update enable

Example:

```
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

When you enable the automatic update on the CA certificates, the update process is executed daily at a system-defined time.

Step 6 (Optional) View the status of automatic update of CA certificates:

show cert-update

Example:

```
> show cert-update
Autoupdate is enabled and set for every day at 09:34 UTC
CA bundle was last modified 'Thu Sep 15 16:12:35 2022'
```

Install a certificate using self-signed enrollment

Install a self-signed certificate to establish secure VPN connections by creating an identity certificate directly on the managed device.

Procedure

Step 1 Choose **Devices** > **Certificates**.

Step 2 Click **Add** to open the **Add New Certificate** dialog box.

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

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

- Select a Certificate Enrollment Object of the type Self-Signed from the drop-down list.
- Click + to add a new Certificate Enrollment Object. For more information, refer to Add certificate enrollment objects.

Step 5 Click **Add** to start the Self Signed, automatic, enrollment process.

For self signed enrollment type trustpoints, the **CA Certificate** status is always displayed. The managed device self-signs its identity certificate and does not require a CA certificate. Self-signed enrollment does not enable the device to act as a CA or provide CA services.

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

Step 6 Click the magnifying glass to view the self-signed Identity Certificate created for this device.

What to do next

When 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 Site to Site and Remote Access VPN Authentication Method.

Install a certificate using EST enrollment

Use EST enrollment to automatically obtain and install identity certificates on devices from a Certificate Authority (CA).

Before you begin

Note Using EST 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.

Note EST's ability to auto-enroll a device when its certificate expires is not supported.

Follow these steps to install a certificate using EST enrollment:

Procedure

Step 1 Choose **Devices** > **Certificates**.

Step 2 Click **Add** to open the **Add New Certificate** dialog box.

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

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

- Select the EST certificate enrollment object from the **Cert Enrollment** drop-down list.
- Click **+** to add a new Certificate Enrollment Object. For more information, refer to Add certificate enrollment objects.

Step 5 Click **Add** to enroll the certificate on the device.

The **Identity Certificate** will go from `InProgress` to `Available` as the device obtains its identity certificate using EST from the specified CA. Sometimes, a manual refresh might be required to obtain the identity certificate.

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

Install a certificate using SCEP enrollment

Install a certificate using SCEP enrollment to enable secure authentication for VPN connections and other security features on your device.

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.

Follow these steps to install a certificate using SCEP enrollment:

Procedure

Step 1 Choose **Devices** > **Certificates**.

Step 2 Click **Add** to open the **Add New Certificate** dialog box.

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

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

- Select a Certificate Enrollment Object of the type SCEP from the drop-down list.
- Click + to add a new Certificate Enrollment Object. For more information, refer to Add certificate enrollment objects.

Step 5 Click **Add** 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. Sometimes, a manual refresh might be required to obtain the identity certificate.

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

What to do next

When 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 Site to Site and Remote Access VPN Authentication Method.

Install a certificate using manual enrollment

Manual enrollment allows you to obtain and install an identity certificate on a managed device by generating a certificate signing request (CSR) and working with your PKI CA server to obtain the corresponding identity certificate.

Procedure

Step 1 Choose **Devices** > **Certificates**.

Step 2 Click **Add** to open the **Add New Certificate** dialog box.

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

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

- Select a Certificate Enrollment Object of the type **Manual** from the drop-down list.
- Click + to add a new Certificate Enrollment Object. For more information, refer to Add certificate enrollment objects.

Step 5 Click **Add** to start the enrollment process.

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 Cloud-Delivered Firewall Management Center or the managed device. When complete, you will have an Identity Certificate for the managed device. You can place it in a file.

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

Return to the Cloud-Delivered Firewall Management Center dialog and select **Browse Identity Certificate** to choose the identity certificate file.



Note Ensure not to choose a binary certificate (PKCS12, DER, and alike) file because Firewall Threat Defense does not support them.

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 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 Site to Site and Remote Access VPN Authentication Method.

Install a certificate using a PKCS12 file

Install a certificate using a PKCS12 file to enable secure authentication and encrypted communications on managed devices.

Procedure

Step 1 Choose **Devices** > **Certificates**.

Step 2 Click **Add** to open the **Add New Certificate** dialog box.

Step 3 Choose a pre-configured managed device from the **Device** drop down list.

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

- Select a Certificate Enrollment Object of the PKCS type from the drop-down list.
- Click + to add a new Certificate Enrollment Object. For more information, refer to Add certificate enrollment objects.

Step 5 Click **Add**.

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

Note When you upload the PKCS12 file for the first time, the file is stored in Cloud-Delivered Firewall Management Center as part of the CertEnrollment object. For any failed enrollments due to a wrong passphrase or failed deployment, retry enrolling the PKCS12 certificate without uploading the file again. Also, whenever you modify the certificate enrollment object to permit overrides, you must update the **Passphrase** for the certificate for a sucessful enrollment. A PKCS12 file size should not be larger than 24K.

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 certificate enrollment object. Use this certificate in your VPN authentication configuration.

Install a certificate using ACME enrollment

Install certificates automatically using the ACME (Automatic Certificate Management Environment) protocol to eliminate manual certificate installation. To renew certificates automatically, enable **Auto Enrollment** in the ACME certificate enrollment object.

Before you begin

ACME enrollment is supported on Firewall Threat Defense version 10.0.0 and later.

Procedure

Step 1 Choose **Devices** > **Certificates**.

Step 2 Click **Add** to open the **Add New Certificate** dialog box.

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

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

- Select a Certificate Enrollment Object of the type ACME from the drop-down list.
- Click **+** to add a new Certificate Enrollment Object. For more information, refer to Add certificate enrollment objects.

Step 5 Click **Add** to start the automatic enrollment process.

For ACME enrollment type trustpoints, the **Identity Certificate** status shows `InProgress` until enrollment is successful. The **CA Certificate** status is **Not Applicable** for ACME enrollment. To establish the certificate chain, separately enroll the required CA certificate by using a **Manual CA-only** certificate enrollment object.

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

What to do next

When enrollment is complete, a trustpoint is configured on the device with the same name as the certificate enrollment object. Use this trustpoint in the configuration of your remote access VPN authentication.

Troubleshoot Threat Defense certificates

See Secure Firewall Threat Defense VPN certificate guidelines and limitations, on page 1 to determine if variations in your certificate enrollment environment may be causing a problem.

Certificate expiration monitoring
CA server connectivity

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.

Microsoft 2012 CA server template configuration

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.

Default keyring certificate regeneration

On the Cloud-Delivered Firewall Management Center, you might receive this health alert related to the Firewall Threat Defense device:

```
Code - F0853; Description - default Keyring's certificate is invalid, reason: expired
```

Solution: In such cases, use the following command to regenerate the default certificate in CLISH CLI:

```
> system support regenerate-security-keyring default
```

CA certificate configuration errors

A red cross appears in the CA certificate status with this error:

Error: `Fail to configure CA certificate`

Solution: See Troubleshoot Certificate Error on FMC.

Certificate verification in .pfx files

To check the list of the certificates in a .pfx file, use tools such as `certutil` or `openssl`. You can see the whole chain with ID certificate, SubCA certificate, and CA certificate (if any).

- `certutil -dump cert.pfx`

- `openssl pkcs12 -info -in cert.pfx`

Identity certificate import errors

Error: `Identity certificate import required`

Solution: See Troubleshoot Certificate Error "Identity certificate import required" on FMC.

Self-signed certificates hostname behavior in Threat Defense high-availability environments

In a Threat Defense HA configuration, the secondary unit adopts the primary unit's hostname. When you break the HA pair, you must perform these actions:

- Manually update the hostname on the secondary unit to its unique identifier
- Perform a certificate re-enrollment to ensure that the certificate accurately reflects the unit's identity.