Use ACME Certificates for Remote Access VPN Policies in Cisco Secure Firewall Management Center

Revised: December 5, 2025

Use an ACME Certificate for a Remote Access VPN Policy in Secure Firewall Management Center

Is this Guide for You?

This guide is for network administrators who manage SSL and TLS certificates for Threat Defense devices managed by a Management Center. It provides detailed steps for using an Automated Certificate Management Environment (ACME) certificate from Lets Encrypt to authenticate a Threat Defense device as a remote access VPN gateway.

You can obtain ACME certificates from other ACME servers as well; however, in this guide, we use Let's Encrypt as the ACME server.

Sample Scenario

Alex is a network administrator of an enterprise that uses a Management Center to manage multiple Threat Defense devices. He secures remote access VPN on Threat Defense devices using ACME certificates from Let’s Encrypt, a Certificate Authority.

Overview of ACME Enrollments

ACME protocol is an open and standardized protocol designed to automate the issuance, renewal, and management of SSL and TLS certificates. By automating interactions between a certificate authority (CA) and a client, ACME eliminates the manual and complex processes for managing certificates.

Firewall Management Center communicates with an ACME-enabled CA server using the authentication protocol through an authentication interface. For each device, you must have a manual CA certificate for authentication and communication with the ACME server. The ACME server validates domain ownership through port 80 of the Firewall Threat Defense device's authentication interface. After domain validation, the ACME server issues an SSL or TLS certificate to the device.

In an HA pair, the standby device inherits the ACME certificate and all related configurations from the active device’s ACME certificate enrollment object.

Benefits of using ACME Enrollments

- Automation: Automates the lifecycle of SSL and TLS certificates that includes tasks such as:
  - Requesting certificates
  - Managing domain validations
  - Renewing certificates

    You can also update the domain information of an ACME certificate by editing the ACME enrolment object.
  - Revoking certificates
- Security: Ensures security through various mechanisms such as:
  - Using HTTPS for secure communication between the client and the CA server.

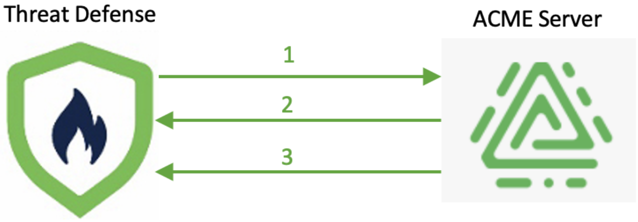
- Using key pairs for authentication requests.
- Reducing the risk of service outages and site vulnerabilities caused by expired certificates.
- Validating domain ownership.

- Cost-effectiveness: Allows use of free certificate services, such as Let's Encrypt, to reduce SSL and TLS certification expenses.
- Scalability: Manages numerous certificates efficiently across multiple domains and subdomains, providing a scalable SSL and TLS certificate management solution.

How ACME Certificates Work

This figure shows the stages of ACME certificate enrollment.

Figure 1: Stages of ACME Certificate Enrollment



This table explains the process of ACME certificate enrollment for a Firewall Threat Defense device.

Stage	Description
1	Firewall Threat Defense device requests an ACME certificate for a specific domain or a list of domains through the source interface.
2	ACME server validates the domain ownership through TCP port 80 of the Firewall Threat Defense device's authentication interface. For domain validation, the Firewall Threat Defense device uses an HTTP-based challenge mechanism (HTTP-01). **Note** Firewall Threat Defense briefly opens port 80 during the enrollment challenge-response process to provide only the ACME challenge data; the port closes as soon as the enrollment succeeds or fails.
3	After domain validation, the ACME server issues an SSL or TLS certificate to the Firewall Threat Defense device.

Note The stages are repeated for each FQDN in the certificate enrollment request.

System Requirements

Table 1 lists the platforms and versions for this use case.

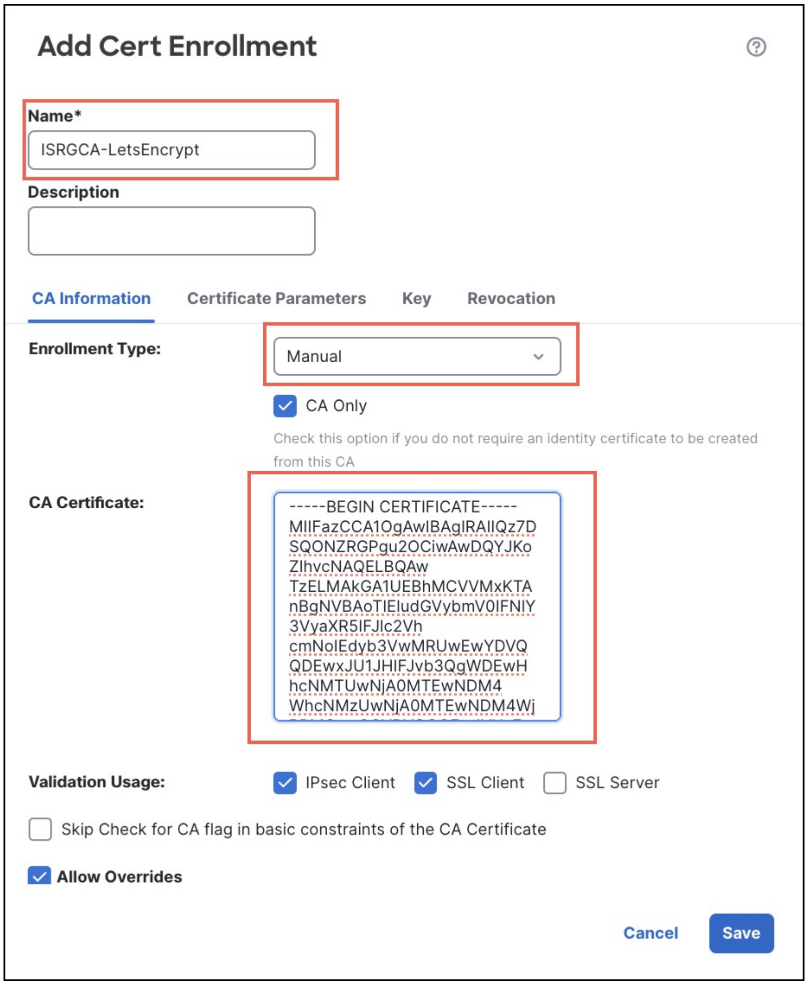
Product	Version	Version Used in This Document
Cisco Secure Firewall Management Center	10.0 or later	10.0
Cisco Secure Firewall Threat Defense	10.0 or later	10.0
ACME Server	-	Let’s Encrypt

Prerequisites for Using ACME Certificates

General Prerequisites

- Ensure that the Firewall Threat Defense device is Version 10.0 or later.
- Configure DNS in the Firewall Threat Defense platform settings to resolve the domain name of the ACME server.
- Ensure your domain maps to a public IP address. Configure the device interface with this IP address, and set it as the authentication interface in the ACME certificate enrollment.
- Enroll an ACME CA certificate, a manual CA-only certificate that authenticates the ACME server, on the device.
    - When you use Let’s Encrypt as the ACME server, you must get the Internet Security Research Group (ISRG) root certificate from https://letsencrypt.org/certificates/ and attach it as a manual CA-only certificate on the device.

      For example, use the root certificate from https://letsencrypt.org/certs/isrgrootx1.pem.txt to configure the manual CA certificate for the ACME server.



Add Cert Enrollment

Name* ISRGCA-LetsEncrypt

Description

Enrollment Type: Manual

☑ CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
-----BEGIN CERTIFICATE-----
MIIFazCCA1OgAwIBAgIRAIIQz7D
SQONZRGPgu2OCiwAwDQYJKo
ZIhvcNAQELBQAw
TzELMAkGA1UEBhMCVVMxKTA
nBgNVBAoTIEludGVybmV0IFNIY
3VyaXR5IFJlc2Vh
cmNoIEdyb3VwMRUwEwYDVQ
QDEwxJU1JHIFJvb3QgWDEwH
hcNMTUwNjA0MTEwNDM4
WhcNMzUwNjA0MTEwNDM4Wj
```

Validation Usage: ☑ IPsec Client ☑ SSL Client □ SSL Server

□ Skip Check for CA flag in basic constraints of the CA Certificate

☑ Allow Overrides

- If you configure object overrides for any device, ensure that you enroll an ACME CA certificate on that device too.

- Configure the same NTP server for the ACME server and the Firewall Threat Defense device.

Prerequisites for ACME Server

- Ensure that you have access to the Let's Encrypt ACME server.
- Ensure that the ACME server is reachable from the Firewall Threat Defense device.
- Ensure that the ACME server can validate the domain name and the alternate FQDNs.
- Ensure that the ACME server is reachable from the source interface of the device, if the authentication interface is different from the source interface.

Prerequisite for VPN Load Balancing

Ensure you include the director and member FQDNs in the **Alternate FQDN** field when you configure an ACME enrollment object for a VPN load balancing group. Note that ACME certificates do not support wildcard certificates.

Guidelines and Limitations for Using ACME Certificates

Guideline

To renew an ACME certificate on the device before its lifetime, re-enroll the certificate and deploy the configuration in the device.

Limitations

- ACME certificates do not support:
  - Site-to-site VPN
  - Management interface in the converged mode
  - DNS authentication (DNS-01); only HTTP-01 is supported
  - Domain override
  - Wildcard certificates: These certificate secure a single domain and multiple subdomains using a wildcard character (*) in the domain name field.
  - Clustering
- ACME certificates support only 2048, 3072, and 4096 key sizes for RSA keys and 256, 384 and 521 for ECDSA keys.
- ACME enrolment is not compatible with control plane ACLs.

  When using Let's Encrypt with control plane ACLs:

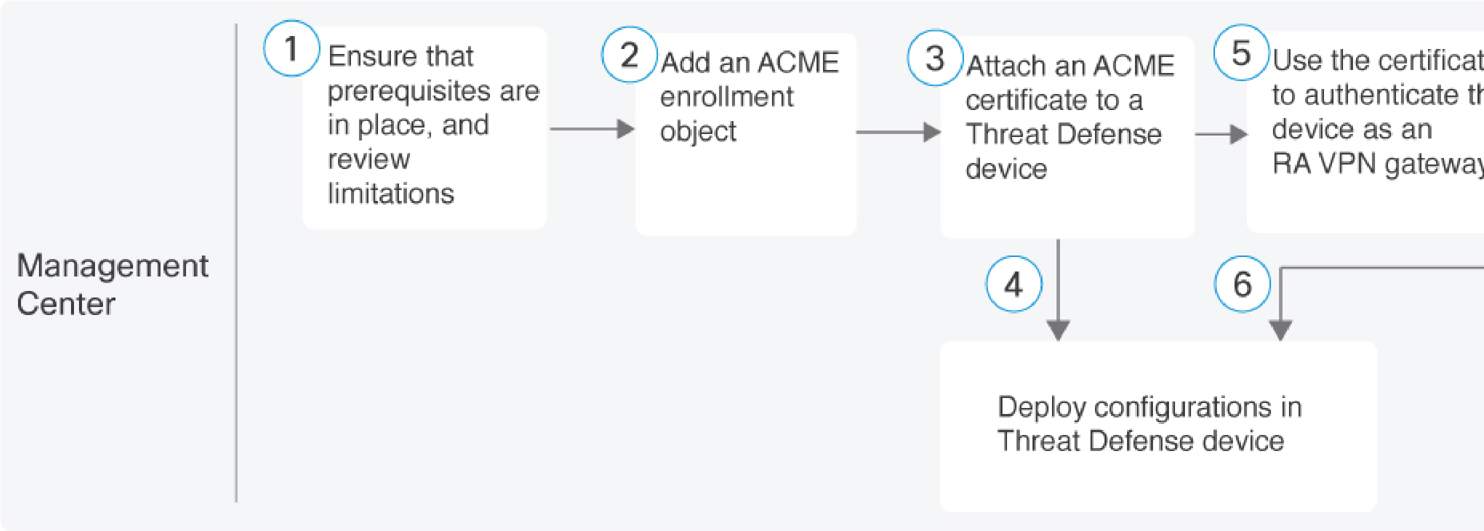
  1. Disable the ACL before the ACME enrollment to allow port 80 access.
  2. Enroll the ACME certificate.
  3. Verify the enrollment.
  4. Re-enable the ACL.

  When using ACME servers other than Let's Encrypt with control plane ACLs, include the server's FQDN in the ACL.

Workflow of ACME Enrollment in Firewall Management Center

Workflow

These are the stages of enrolling an ACME certificate in Firewall Management Center:


Management Center
1
Ensure that prerequisites are in place, and review limitations
2
Add an ACME enrollment object
3
Attach an ACME certificate to a Threat Defense device
5
Use the certificat to authenticate th device as an RA VPN gateway
4
6
Deploy configurations in Threat Defense device

1. Ensure that Prerequisites for Using ACME Certificates, on page 4 are in place, and review Guidelines and Limitations for Using ACME Certificates, on page 6.
2. Add an ACME Certificate Enrollment Object, on page 7.
3. Attach an ACME Certificate to a Firewall Threat Defense Device, on page 11.
4. Deploy configurations in the device.
5. Use the certificate as an identity certificate to authenticate the device as an RA VPN gateway. For more information, see Configure a New Remote Access VPN Policy with an ACME Certificate, on page 13.
6. Deploy configurations in the device.

Add an ACME Certificate Enrollment Object

Before you begin

Ensure that you review Prerequisites for Using ACME Certificates, on page 4 and Guidelines and Limitations for Using ACME Certificates, on page 6.

Procedure

Step 1 Choose **Objects** > **PKI** > **Cert Enrollment**.

Step 2 Click **Add Cert Enrollment**.

Step 3 In the **Name** field, enter the name for the ACME certificate enrollment.

When the enrollment is complete, the trustpoint name on the managed devices will be the given name.

Step 4 (Optional) In the **Description** field, enter a description for the enrollment.

Step 5 In the **CA Information** tab:

a) From the **Enrollment Type** drop-down list, choose **ACME**.

b) In the **Enrollment URL** field, use the default URL https://acme-v02.api.letsencrypt.org/directory, which is Let’s Encrypt's ACME CA server's URL.

   In the **Authentication Protocol** field, **HTTP-01** is the predefined protocol used to validate domain ownership.

c) From the **Authentication Interface** drop-down list, choose a security zone or an interface group that has the interface through which the ACME server communicates with the device to verify domain ownership.

   Click **+** to add a security zone or an interface group. The default interface is the management interface.

d) From the **Source Interface** drop-down list, choose an a security zone or an interface group that has the interface through which the device interacts with the ACME server to request and receive the enrolled ACME certificate.

   Click **+** to add a security zone or an interface group. The default interface is the management interface. The source and the authentication interfaces can be the same.

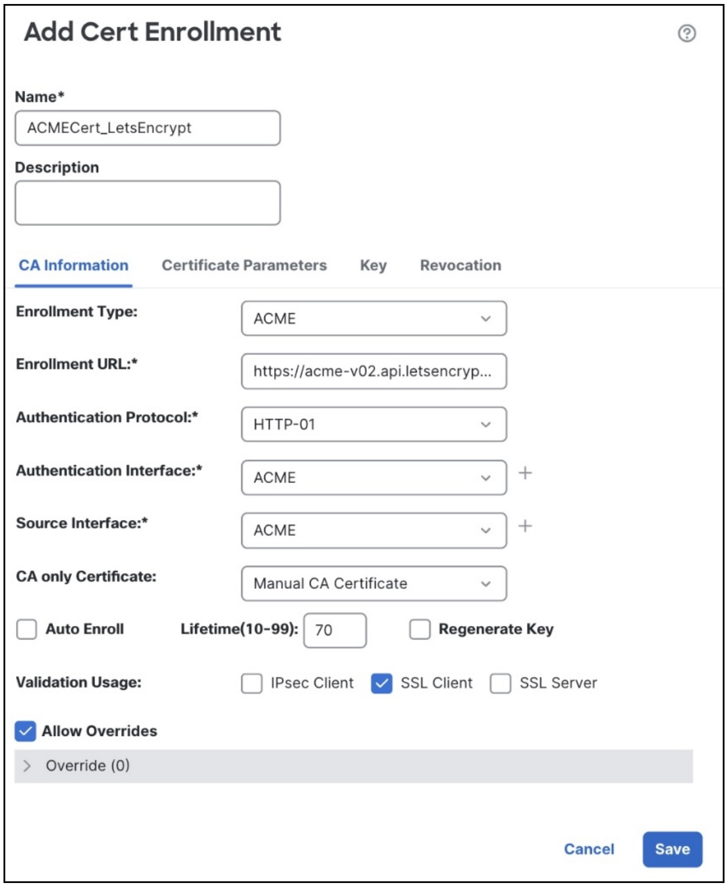
e) From the **CA only Certificate** drop-down list, choose a manual CA-only certificate that authenticates the ACME server.

f) Check the **Auto Enroll** check box to enable automatic enrollment of the ACME certificates based on the configured lifetime.

g) In the **Lifetime** field, enter the percentage of the ACME certificate lifetime after which certificate re-enrollment is automatically initiated. The default value is 70.

   For example, if the certificate's lifetime is 100 days and this field is set to 80, auto-renewal will be triggered on day 81.

h) Check the **Regenerate Key** check box to regenerate a new key for each ACME enrollment. If you uncheck this check box, the previous key is used for enrollment.



Add Cert Enrollment

Name*: ACMECert_LetsEncrypt

Description:

Enrollment Type:	ACME
Enrollment URL:*	https://acme-v02.api.letsencryp...
Authentication Protocol:*	HTTP-01
Authentication Interface:*	ACME
Source Interface:*	ACME
CA only Certificate:	Manual CA Certificate

□ Auto Enroll   Lifetime(10-99): 70   □ Regenerate Key

Validation Usage: □ IPsec Client ☑ SSL Client □ SSL Server

☑ Allow Overrides

Override (0)

Step 6 In the **Certificate Parameters** tab:

a) From the **Include FQDN** drop-down list, choose one of the following to define the certificate FQDN:

- **Use Device Hostname as FQDN** (Default)
- **Custom FQDN**: When you choose this option, enter the FQDN in the **Custom FQDN** field.

b) In the **Alternate FQDN** field, enter comma-separated values of additional FQDNs that will be part of the certificate's Subject Alternative Name (SAN) field.

In a digital certificate, this field allows a single certificate to secure multiple domain names, subdomains, or IP addresses.

Step 7 In the **Key** tab:

a) Click either **RSA** or **ECDSA** key type.

b) In the **Key Name** field:

- For an RSA key, only **modulus** is supported.
- For an ECDSA key, only **elliptic-curve name** is supported.

c) From the **Key Size** drop-down list, choose a key size.

- For an RSA key, use 2048, 3072, or 4096.

- For an ECDSA key, use 256, 384, or 521.

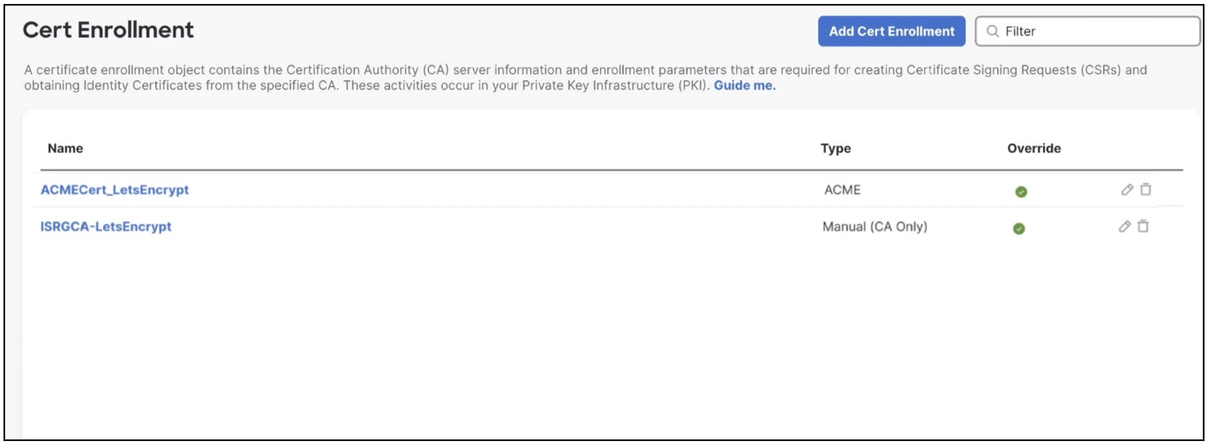
Step 8 (Optional) Configure the **Advanced Settings**, if required.

Step 9 Check the **Allow Overrides** check box to configure any object overrides for any device or domain.

By default, this option is enabled. If you plan to configure object overrides, you must enable this option before enrolling the certificate to the first device.

Step 10 Click **Save**.

You can view the ACME certificate enrollment object in the Certificate Enrollment page



A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI). Guide me.

Name	Type	Override
ACMECert_LetsEncrypt	ACME	●
ISRGCA-LetsEncrypt	Manual (CA Only)	●

What to do next

Edit an ACME Certificate Enrollment Object, on page 10 or Attach an ACME Certificate to a Firewall Threat Defense Device, on page 11

Edit an ACME Certificate Enrollment Object

Before you begin

Create an ACME certificate enrollment object. For more information, see Add an ACME Certificate Enrollment Object, on page 7

Procedure

Step 1 In the certificate enrollment object page, click the edit icon adjacent to the ACME certificate enrollment object that you want to edit.

Step 2 Click the **CA Information** tab.

Step 3 Update the **Auto-Enroll**, **Lifetime**, **Regenerate Key** fields as required.

You cannot edit any other fields in this tab.

Step 4 Click the **Certificate Parameters** tab

Step 5 Edit the **Alternate FQDN** field, if required.

You cannot edit any other fields in this tab.

Step 6 Click **Save**.

Step 7 Choose **Devices** > **Certificates**.

The message `Deployment pending, re-enroll to update the certificate` is displayed next to the ACME certificate.

Step 8 Re-enroll the ACME certificate to push the updated configurations to the device.

During re-enrollment, the existing alternate FQDNs are removed, and the new FQDNs are pushed to the device.

What to do next

Attach an ACME Certificate to a Firewall Threat Defense Device, on page 11

Attach an ACME Certificate to a Firewall Threat Defense Device

Before you begin

Add an ACME certificate enrollment object. For more information, see Add an ACME Certificate Enrollment Object, on page 7.

Procedure

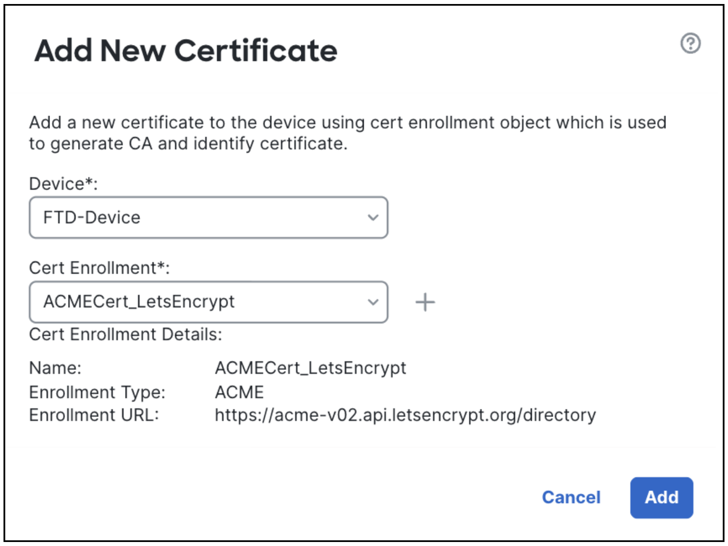
Step 1 Choose **Devices** > **Certificates**.

Step 2 Click **Add**.

Step 3 From the **Device** drop-down list, choose a Firewall Threat Defense device.

Step 4 From the **Cert Enrollment** drop-down list, choose an ACME certificate or click **+** to create an ACME certificate enrollment.

Review the certificate details.



Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: FTD-Device

Cert Enrollment*: ACMECert_LetsEncrypt

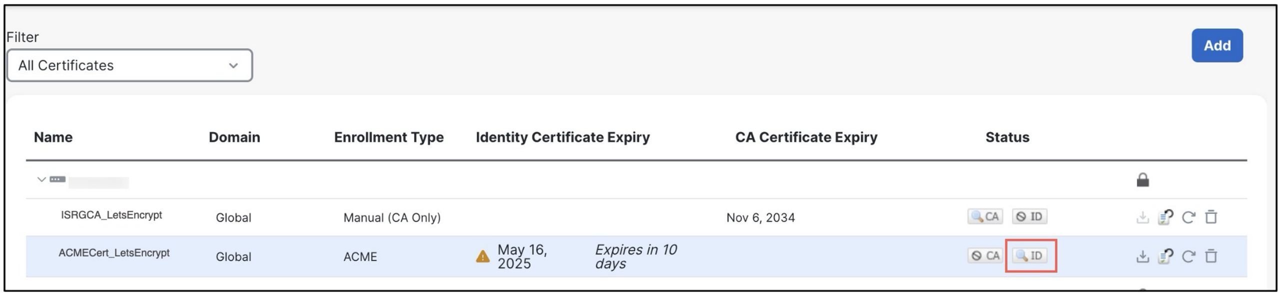
Cert Enrollment Details:

Name: ACMECert_LetsEncrypt
Enrollment Type: ACME
Enrollment URL: https://acme-v02.api.letsencrypt.org/directory

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

During this process, the **Status** in the **Certificates** page will be **In Progress** until the task is completed.

After the certificate is successfully attached to the device, the **ID** icon is displayed under **Status**.

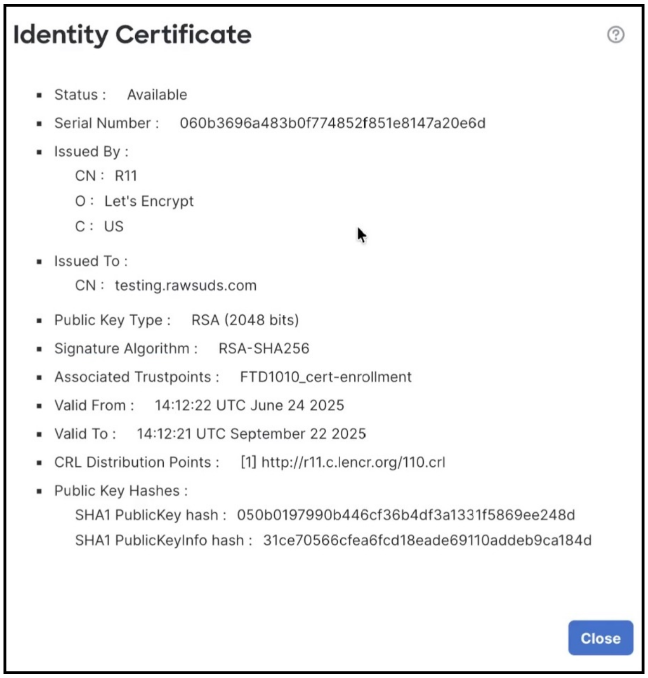


Filter

All Certificates

Name	Domain	Enrollment Type	Identity Certificate Expiry	CA Certificate Expiry	Status
[redacted]					
ISRGCA_LetsEncrypt	Global	Manual (CA Only)		Nov 6, 2034	CA ID
ACMECert_LetsEncrypt	Global	ACME	⚠ May 16, 2025 *Expires in 10 days*		CA ID

Click the **ID** icon to view the certificate details. Review these details, and click **Close**.



Identity Certificate

- Status : Available
- Serial Number : 060b3696a483b0f774852f851e8147a20e6d
- Issued By :
  CN : R11
  O : Let's Encrypt
  C : US
- Issued To :
  CN : testing.rawsuds.com
- Public Key Type : RSA (2048 bits)
- Signature Algorithm : RSA-SHA256
- Associated Trustpoints : FTD1010_cert-enrollment
- Valid From : 14:12:22 UTC June 24 2025
- Valid To : 14:12:21 UTC September 22 2025
- CRL Distribution Points : [1] http://r11.c.lencr.org/110.crl
- Public Key Hashes :
  SHA1 PublicKey hash : 050b0197990b446cf36b4df3a1331f5869ee248d
  SHA1 PublicKeyInfo hash : 31ce70566cfea6fcd18eade69110addeb9ca184d

What to do next

1. Deploy the configurations in the device.

   After a successful deployment, the device requests the ACME server for an ACME certificate. Upon domain validation, the ACME server issues an ACME certificate.

2. Use the ACME certificate to authenticate the device as an RA VPN gateway. For more information, see Configure a New Remote Access VPN Policy with an ACME Certificate, on page 13 or Update a Remote Access VPN Policy with an ACME Certificate, on page 14.

Configure a New Remote Access VPN Policy with an ACME Certificate

Before you begin

Ensure that you have attached an ACME certificate to a Firewall Threat Defense and deployed the configurations on the device. For more information, see Attach an ACME Certificate to a Firewall Threat Defense Device, on page 11.

Procedure

Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click **Add** to create a new remote access VPN policy.

Step 3 In the **Name** field, enter the name for the remote access VPN policy.

Step 4 In the **Description** field, enter a description for the policy.

Step 5 In **VPN Protocols**, select the protocols.

You can select **SSL** or **IPSec-IKEv2**, or both the VPN protocols. Firewall Threat Defense supports both the protocols to establish secure connections over a public network through VPN tunnels.

Step 6 In **Targeted Devices**, select the devices.

The devices that you select here function as your remote access VPN gateways for the VPN client users.

Step 7 Click **Next**.

Step 8 Configure the **Connection Profile** and **Group Policy** settings.

Step 9 Configure the **Authentication, Authorization & Accounting** settings.

Step 10 Configure the **Client Address Assignment** settings.

Step 11 Configure the **Group Policy** settings.

Step 12 Click **Next**.

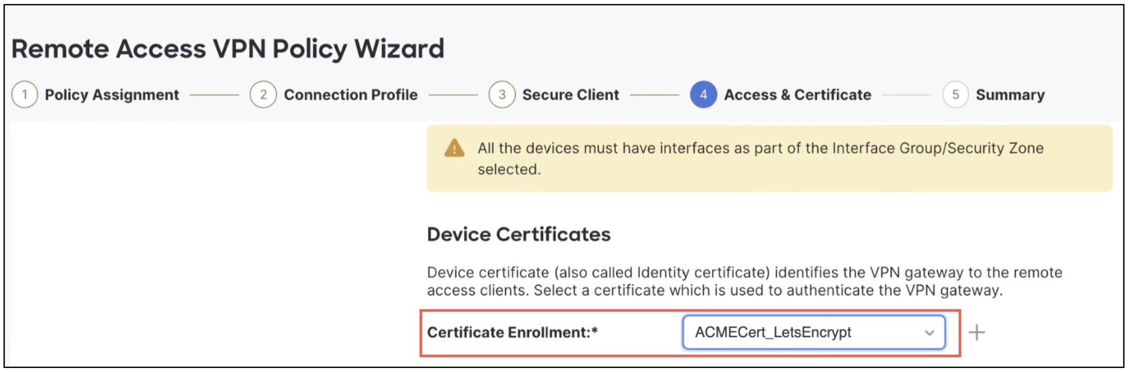
Step 13 Select the AnyConnect image that the VPN users will use to connect to the remote access VPN.

Step 14 Click **Next**.

Step 15 Configure **Network Interface for Incoming VPN Access**.

Step 16 Configure **Device Certificates**.

Device certificate (also called identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway. From the **Certificate Enrollment** drop-down list, choose the ACME certificate to authenticate the VPN gateway.



Remote Access VPN Policy Wizard

All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* ACMECert_LetsEncrypt

Step 17 Configure **Service Access Control**.

Step 18 Configure **Access Control for VPN Traffic** .

Step 19 Click **Next**.

Step 20 View the **Summary** of the remote access VPN policy configuration.

The **Remote Access Summary** page displays all the remote access VPN settings you have configured so far and provides links to the additional configurations that need to be performed before deploying the remote access VPN policy on the selected devices.

Click **Back** to make changes to the configuration, if required.

Step 21 Click **Finish** to complete the basic configuration for the remote access VPN policy.

Step 22 Deploy the configurations in the device.

What to do next

Validate ACME Certificate Enrollments, on page 15

Update a Remote Access VPN Policy with an ACME Certificate

To add the ACME certificate to a device in an existing remote access VPN policy:

Before you begin

1. Ensure that you have attached an ACME certificate to a Firewall Threat Defense and deployed the configurations on the device. For more information, see Attach an ACME Certificate to a Firewall Threat Defense Device, on page 11.

2. Ensure that you have configured a remote access policy.

Procedure

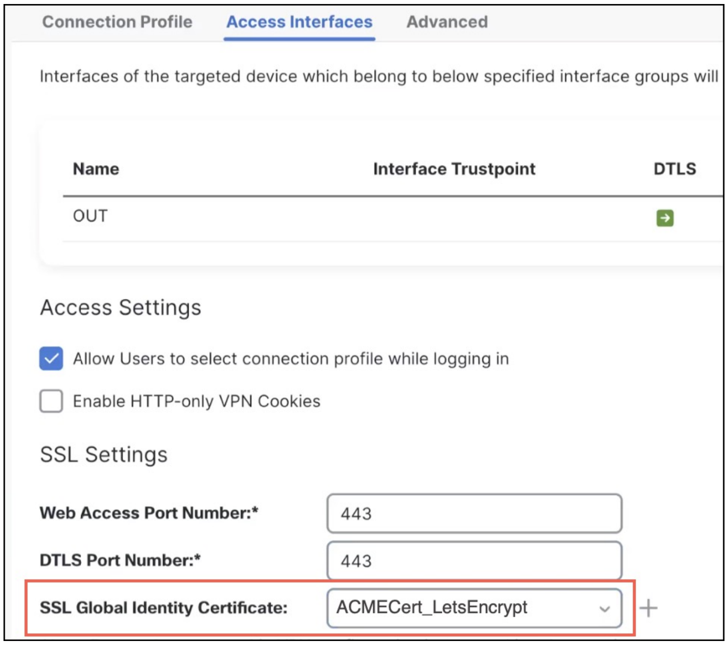
Step 1 Choose **Devices** > **VPN** > **Remote Access**.

Step 2 Click the edit icon adjacent to the remote access policy that you want to edit.

Step 3 Click **Access Interfaces**.

Step 4 In the **SSL Global identity Certificate** drop-down list, choose the ACME certificate.

Figure 2:



Connection Profile | Access Interfaces | Advanced

Interfaces of the targeted device which belong to below specified interface groups will

Name	Interface Trustpoint	DTLS
OUT		➔

Access Settings

☑ Allow Users to select connection profile while logging in

□ Enable HTTP-only VPN Cookies

SSL Settings

Web Access Port Number:* 443

DTLS Port Number:* 443

SSL Global Identity Certificate: ACMECert_LetsEncrypt

Step 5 Click **Save**.

Step 6 Deploy the configurations in the device.

During the deployment, the ACME certificate is linked to the device’s SSL trustpoint, ensuring that remote access VPN connections use the new certificate for secure SSL communication.

What to do next

Validate ACME Certificate Enrollments, on page 15

Validate ACME Certificate Enrollments

From the Firewall Threat Defense device CLI, run these commands:

- **show crypto ca certificates**

  Displays details about the certificates present in the Firewall Threat Defense device. You can verify if the ACME certificate is installed in the device.

```
firepower#show crypto ca certificates LE_ACME_cert_FTD1010
Certificate
  Status: Available
  Certificate Serial Number: 060b3696a483b0f774852f851e8147a20e6d
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: RSA-SHA256
  Issuer Name:
    CN=R11
    O=Let's Encrypt
    C=US
```

```
Subject Name:
  CN=test.rawsuds.com
CRL Distribution Points:
  [1]  http://r11.c.lencr.org/110.crl
Validity Date:
  start date: 14:12:22 UTC Jun 24 2025
  end   date: 14:12:21 UTC Sep 22 2025
  renew date: 14:12:21 UTC Aug 26 2025
Storage: immediate
Associated Trustpoints: FTD1010_cert-enrollment
Public Key Hashes:
 SHA1 PublicKey hash:     050b0197990b446cf36b4df3a1331f5869ee248d
 SHA1 PublicKeyInfo hash: 31ce70566cfea6fcd18eade69110addeb9ca184d
```

- **show crypto ca trustpoints**

  Displays details about the trustpoints present in the Firewall Threat Defense device.

  The **Device Certificate** field indicates if the certificate is installed in the device.

  The **Last Enrollment Result** field indicates the success of the last re-enrollment.

```
firepower# show crypto ca trustpoints
Trustpoint LE_ACME_cert_FTD1010:
    Not authenticated.
    Device certificate: Expires at 14:12:21 UTC Sep 22 2025
    ACME URL: https://acme-v02.api.letsencrypt.org:443/directory
    Current enrollment status:       Idle
    Last enrollment attempt:         15:10:57 UTC Jun 24 2025
    Last enrollment type:            Manual
    Last enrollment result:          SUCCESS
    Auto enrollment request count:   0
    Manual enrollment request count: 3


Trustpoint ISRG_root-cert:
    Subject Name:
        CN=ISRG Root X1
        O=Internet Security Research Group
        C=US
    Serial Number: 8210cfb0d240e3594463e0bb63828b00
    CA Certificate configured.
    Device certificate: Not present
```

Troubleshoot ACME Certificates

Use Debug Commands

Note Use debug commands only during low network traffic periods and for specific troubleshooting or TAC sessions, as they increase CPU usage.

- Use the **debug crypto ca <debug-level>** command to capture debug logs related to crypto CA operations.
- Use the **debug crypto ca acme <debug-level>** command to capture debug logs related to ACME enrollments.

Troubleshoot ACME Enrollment Errors

- **Symptom**: When you attach the ACME certificate to the device, the Status displays `Failed`.

  Resolution: Hover over the warning to see the recommended actions. For more information, see Prerequisites for Using ACME Certificates, on page 4.

- **Symptom**: When you attach the ACME certificate to the device, the Status displays `Failed`. When you hover over the ID symbol, `Failed to configure identity certificate` error appears.

  Possible Causes: The ACME CA certificate is not attached to the device.

  Resolution: Attach the ACME CA certificate to the device.

- **Symptom**: `Unable to connect to the server` or `Unable to connect to <ACME_server>` error message appears.

  Possible Causes:

  - The ACME server is not reachable.
  - The ACME server is reachable, but the ACME service is not running.
  - The ACME CA certificate is not attached to the device.

  Resolution:

  - Ensure that the ACME server is reachable from the Firewall Management Center.
  - Verify the state of the ACME service and restart it if it is not running.
  - Attach the ACME CA certificate to the device.

- **Symptom**: `Unable to validate the ACME server certificate` error message appears.

  Possible Cause: ACME CA certificate for the device is not enrolled in the Firewall Management Center

  Resolution: Attach an ACME CA certificate for the device in the Firewall Management Center.

- **Symptom**: `ACME processing timeout` error message appears.

  Possible Causes:

  - Firewall Management Center cannot resolve the requested FQDNs to the **Authentication Interface**.
  - URL of the ACME server is incorrect.
  - DNS is not configured in the device platform settings.
  - Domain names are inaccurate.

  Resolution:

  - Ensure that the Firewall Management Center can resolve the requested FQDNs to the **Authentication Interface**.
  - Verify the URL of the ACME server.
  - Run the `ping <interface> <acme-ca-fqdn>` command to verify DNS resolution, and verify if DNS is configured in the device platform settings.
  - Verify the FQDNs or alternate FQDNs. Re-enroll the certificate if you update the FQDNs.

Use Syslogs

To enable ACME enrollment syslogs, follow these steps:

1. Choose **Devices** > **Platform Settings**.
2. Create or edit a platform settings policy.
3. In the left pane, click **Syslog**.
4. Click the **Logging Setup** tab and check the **Enable Logging** check box.
5. In **Basic Logging Settings**, check the **Enable Logging** check box.
6. In **Logging to Secure Firewall Management Center**, select **All Logs** or **VPN Logs**.
7. Click the **Syslog Settings** tab.
8. Click the **Enable All Syslog Messages** tab.

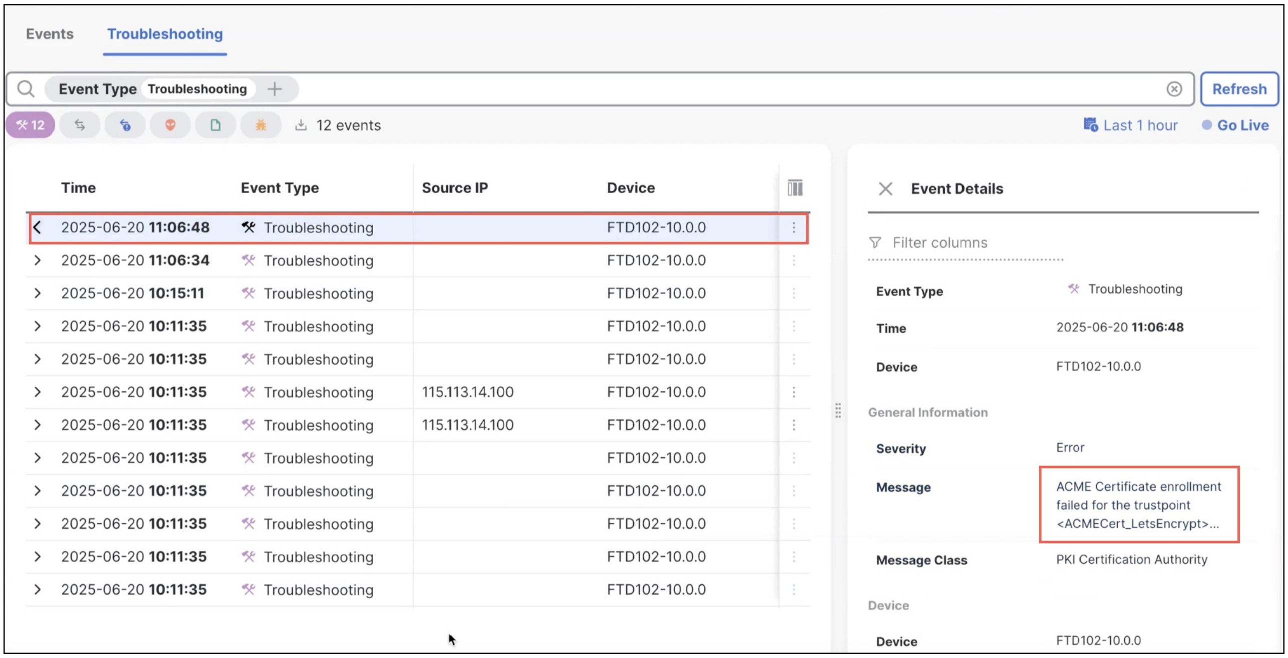
   The ACME enrollment syslogs are 717067, 717068, 717069, and 717070.

Use Troubleshooting Logs

Note Ensure that you configure the syslog settings in the device platform settings.

To monitor ACME enrollment logs:

1. Choose **Analysis** > **Unified Events**.
2. Click the **Troubleshooting** tab.
3. In the **Troubleshooting Events** table, you can do these actions:
   - View and analyze the troubleshooting events.
   - Click **Go Live** to monitor troubleshooting events in real time and correlate device logs with recent configuration changes.



Time	Event Type	Source IP	Device
2025-06-20 **11:06:48**	Troubleshooting		FTD102-10.0.0
2025-06-20 **11:06:34**	Troubleshooting		FTD102-10.0.0
2025-06-20 **10:15:11**	Troubleshooting		FTD102-10.0.0
2025-06-20 **10:11:35**	Troubleshooting		FTD102-10.0.0
2025-06-20 **10:11:35**	Troubleshooting		FTD102-10.0.0
2025-06-20 **10:11:35**	Troubleshooting	115.113.14.100	FTD102-10.0.0
2025-06-20 **10:11:35**	Troubleshooting	115.113.14.100	FTD102-10.0.0
2025-06-20 **10:11:35**	Troubleshooting		FTD102-10.0.0
2025-06-20 **10:11:35**	Troubleshooting		FTD102-10.0.0
2025-06-20 **10:11:35**	Troubleshooting		FTD102-10.0.0
2025-06-20 **10:11:35**	Troubleshooting		FTD102-10.0.0
2025-06-20 **10:11:35**	Troubleshooting		FTD102-10.0.0

Event Details

Filter columns

Event Type	Troubleshooting
Time	2025-06-20 **11:06:48**
Device	FTD102-10.0.0

General Information

Severity	Error
Message	ACME Certificate enrollment failed for the trustpoint <ACMECert_LetsEncrypt>...
Message Class	PKI Certification Authority

Device

Device	FTD102-10.0.0

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.