Install and Renew Certificates on ASA Managed by ASDM

Contents

Introduction

Prerequisites

Requirements

Components Used

Background Information

Trusted CA Security Considerations

Certificate Authentication Risks and Recommendations

Default Trustpoint Validation-Usage Behavior

Default Configuration Risks

Recommended Action

Example Configuration:

Authorization Risks and Recommendations

Recommended Action

Example Configuration

Additional Resources

Request and Install a new Identity Certificate with ASDM

Request and Install a New Identity Certificate with Certificate Signing Request (CSR)

Generate a CSR with ASDM

Create a Trustpoint with a Specific Name

(Optional) Create a New Key Pair

Choose the Key Pair Name

Configure the Certificate Subject and Fully Qualified Domain Name (FQDN)

Generate and Save the CSR

Install the Identity Certificate in PEM format with ASDM

Install CA Certificate that Signed the CSR

Install Identity Certificate

Bind the New Certificate to Interface with ASDM

Install an Identity Certificate Received in PKCS12 Format with ASDM

Install the Identity and CA Certificates from a PKCS12 File

Bind the New Certificate to Interface with ASDM

Certificate Renewal

Renew a Certificate Enrolled with Certificate Signing Request (CSR) with ASDM

Generate a CSR withASDM

Create a New Trustpoint with a Specific Name

(Optional) Create a New Key Pair

Select the Key Pair Name

Configure the Certificate Subject and Fully Qualified Domain Name (FQDN)

Generate and Save the CSR

Install the Identity Certificate in PEM Format with ASDM

Install CA Certificate that Signed the CSR

Install Identity Certificate

Bind the New Certificate to Interface with ASDM

Renew a Certificate Enrolled with PKCS12 File with ASDM

Install the Renewed Identity Certificate and CA Certificates from a PKCS12 File

Bind the New Certificate to Interface with ASDM

Verify

View Installed Certificates via ASDM

Troubleshoot

Frequently Asked Questions

Introduction

This document describes how to request, install, trust, and renew certain types of certificates on Cisco ASA Software managed with ASDM.

Prerequisites

Requirements

- Before you start to verify that the Adaptive Security Appliance (ASA) has the correct clock time, date, and time zone with certificate authentication, it is recommended to use a Network Time Protocol (NTP) server to synchronize the time on the ASA. Check Related Information for reference.
- To request a certificate that uses Certificate Signing Request (CSR), it is required to have access to a trusted internal or third-party Certificate Authority (CA). Examples of third-party CA vendors include, but are not limited to, Entrust, Geotrust, GoDaddy, Thawte, and VeriSign.

Components Used

The information in this document is based on these software and hardware versions:

- ASAv 9.18.1
- For PKCS12 creation, OpenSSL is used.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The type of certificates this document addresses are:

- Self-signed certificates
- Certificates signed by a 3rd party Certificate Authority or internal CA

The Secure Socket Layer (SSL), Transport Layer Security (TLS) and IKEv2 rfc7296 for EAP authentication protocols mandate that the SSL/TLS/IKEv2 server provides the client with a server certificate for the client to perform server authentication. It is recommended to use trusted third-party CAs to issue SSL certificates to the ASA for this purpose.

Cisco does not recommend use of a self-signed certificate because of the possibility that a user could inadvertently configure a browser to trust a certificate from a rogue server. There is also the inconvenience to users to have to respond to a security warning when it connects to the secure gateway.

Trusted CA Security Considerations

Certificate Authentication Risks and Recommendations

Default Trustpoint Validation-Usage Behavior

When a trusted CA certificate is installed, it can be used to authenticate different types of VPN connections using certificate authentication. It is controlled with**validation-usage**trustpoint command (**Configuration > Device Management > Certificate Management >CA Certificates >Add -> More Options... > Advanced >** select wanted Validation Usage).

The validation-usage types are:

- ipsec-client: Validates IPsec client connections.
- ssl-client: Validates SSL client connections.
- ssl-server: Validates SSL server certificates.

By default, the command allows validation for ipsec-client and ssl-client.

Default Configuration Risks

- Any CA certificate installed as trusted can be used by default to authenticate incoming client identity certificates for any tunnel group using certificate authentication.
- This default setting can be a security risk if you are not aware of it.

Recommended Action

Disable validation-usage for unintended trustpoints. If a CA certificate is not meant to authenticate VPN peers or users, disable validation-usage for that trustpoint.

Example Configuration:

<#root>

```
Navigate to:

Configuration > Device Management > Certificate Management > CA Certificates

.
a) Select a wanted trustpoint and click

Edit

.
b) Navigate to

Advanced

 and uncheck all

Validation Usage

 options.
```

```
trustpoint public-root-ca
 no validation-usage
```

Authorization Risks and Recommendations

By default, a trusted CA certificate can be used to authenticate VPN peer or user connecting to any tunnel-group. Proper authorization needs to be designed.

Recommended Action

Use certificate maps and tunnel-group maps to ensure only authorized certificates are used for specific tunnel groups. Set a default tunnel group map rule, that points to a no-access tunnel group to restrict unauthorized access.

Example Configuration

Certificate authentication is only allowed for:

- Machines with certificate issued by cn=example.com and having OU=machines in certificate subject.
- Users with certificate issued by cn=example.com and having OU=users in certificate subject.

Users with other certificates are assigned to no_access tunnel-group by default, thanks to**tunnel-group-map default-group no_access**command. The Certificate Map Rules have priority over group-url thanks to**tunnel-group-map enable rules**command. Knowing group-url does not help to bypass the Certificate Map Rules.

<#root>

```
! Configure group-policy preventing VPN access:



Navigate to:

Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add > General > More Opti


a) Uncheck

Inherit

next to

Simultaneous Logins

and set the value

0

.
b) Uncheck

 Inherit

next to

 Banner

and set a wanted massage, for example
```

NO ACCESS GROUP POLICY

.

```
group-policy no_access_gp internal
group-policy no_access_gp attributes
 banner value NO ACCESS GROUP POLICY
 vpn-simultaneous-logins 0
```

! Configure tunnel-groups for users and tunnel-group preventing VPN access:

Navigate to:

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

. Click

Add

and configure:
a) Authentication method as

Certificate

.
a)

Client Address Pools

.
b)

DNS Servers

.

c)

Group Policy

- for the

no_access

tunnel group use

no_access_gp

where simultaneous logins is set to 0.
d)

Group URLs

- only for the

mgmt-tunnel

and

users_access

tunnel groups. Navigate to:

Advanced > Group Alias/Group URL

, click

Add

in the

Group URLs

section and configure a group URL.

```
tunnel-group mgmt-tunnel type remote-access
tunnel-group mgmt-tunnel general-attributes
 address-pool vpn_pool
 default-group-policy mgmt-tunnel
tunnel-group mgmt-tunnel webvpn-attributes
 authentication certificate
 group-url https://ftd.example.com/mgmt enable
!
tunnel-group users_access type remote-access
tunnel-group users_access general-attributes
 default-group-policy user_access_gp
 address-pool vpn_pool
tunnel-group users_access webvpn-attributes
 authentication certificate
 group-url https://ftd.example.com/users enable
!
tunnel-group no_access type remote-access
tunnel-group no_access general-attributes
 default-group-policy no_access_gp
 address-pool vpn_pool
tunnel-group no_access webvpn-attributes
 authentication certificate
```

! Create certificate maps for users and use the certificate maps for tunnel-group mapping:

Navigate to:

Configuration > Remote Access VPN > Advanced > Certificate to AnyConnect and Clientless SSL VPN Connecti

.

a) Click

Add

to configure

Certificate to Connection Profile Maps

.

b) Select

New

and configure a certificate group map name, for example

mgmt_tunnel_map

or

users_access_map

.
c) Select a corresponding connection profile/tunnel group from the drop-down menu at

Mapped to Connection Profile

.
d) Click

Add

to configure

Mapping Criteria

.
e) Select:

Field: Subject

,

Component: Organizational Unit (OU)

,

Operator: Equals

,

Value:

machines or users.
d) Select:

Field: Issuer

,

Component: Common Name (CN)

,

Operator: Equals

,

Value:

example.com.

```
crypto ca certificate map mgmt_tunnel_map 10
 issuer-name attr cn eq example.com
 subject-name attr ou eq machines
crypto ca certificate map users_access_map 10
 issuer-name attr cn eq example.com
 subject-name attr ou eq users
!
webvpn
 (...)
 certificate-group-map mgmt_tunnel_map 10 mgmt-tunnel
 certificate-group-map users_access_map 10 users_access
```

! Enable tunnel-group maps and set the default tunnel-group preventing access if a user certificate did

Navigate to:

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connecti

.
a) Check

Use the configure rules to match a certificate to a Connection Profile

.
b) Check

Defult to Connection Profile

and select from the drop-down menu the

no-access

connection profile/tunnel group.

```
tunnel-group-map enable rules
tunnel-group-map default-group no_access
```

Additional Resources

For more detailed configuration instructions, refer to Cisco documentation:

- Validation Usage Configuration -Cisco Secure Firewall ASA Series Command Reference, T - Z Commands
- Certificate Map Configuration -Cisco Secure Firewall ASA Series Command Reference, T - Z Commands
- Tunnel-Group Map Configuration -Cisco Secure Firewall ASA Series Command Reference, T - Z Commands
- Tunnel-Group-Map Enable Configuration -Cisco Secure Firewall ASA Series Command Reference, T - Z Commands

Request and Install a new Identity Certificate with ASDM

A certificate can be requested from a Certificate Authority (CA) and installed on a ASA in two ways:

1. Use Certificate Signing Request (CSR). Generate a Key Pair, request an Identity Certificate from CA with a CSR, install the signed Identity Certificate obtained from the CA.
2. Use PKCS12 file obtained from a CA, or exported from a different device. The PKCS12 file contains Key Pair, Identity Certificate, CA certificate(s).

Request and Install a New Identity Certificate with Certificate Signing Request (CSR)

A CSR is created on the device that needs an Identity Certificate, use a Key Pair created on the device.

A CSR contains:

- certificate request information - requested subject and other attributes, public key from the Key Pair.
- signature algorithm information

- digital signature of certificate request information, signed with the private key from the Key Pair.

The CSR is passed to the Certificate Authority (CA) so that it signs it, in a PKCS#10 form.

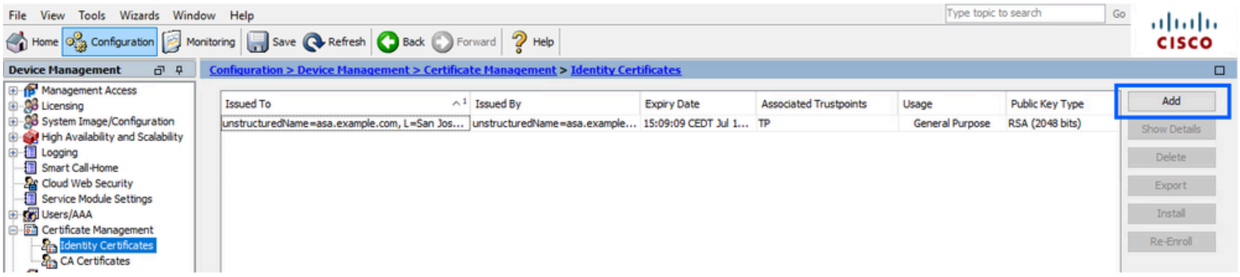
The signed certificate is returned from CA in a PEM form.

Note: CA can alter the FQDN and Subject Name parameters defined in the Trustpoint when it signs the CSR and creates a signed Identity Certificate.

Generate a CSR with ASDM

1. **Create a Trustpoint with a Specific Name**

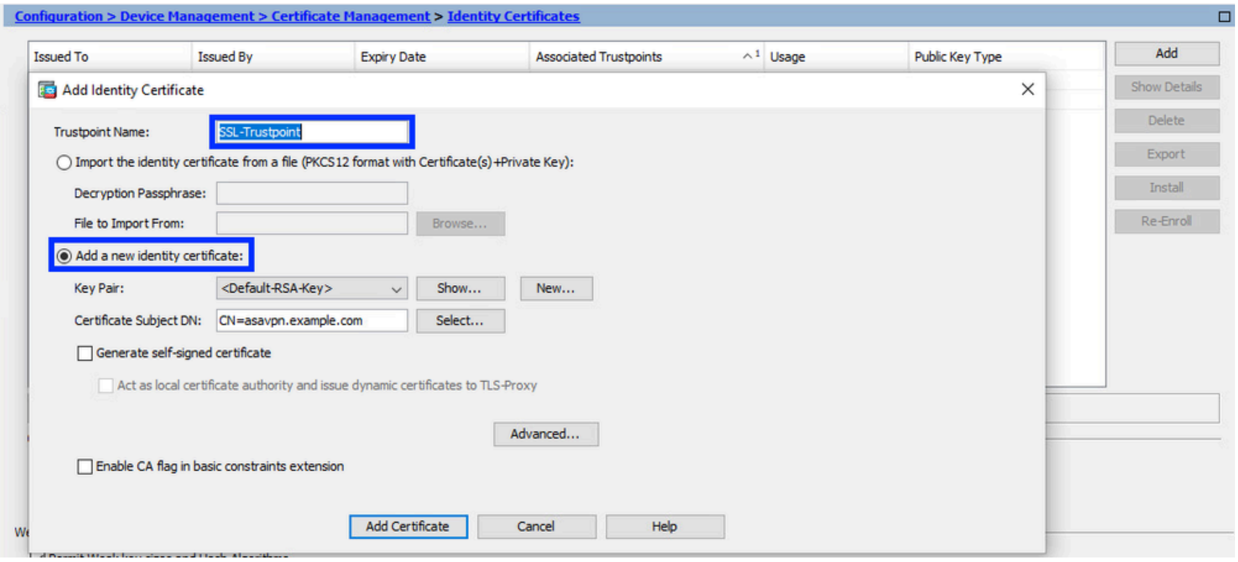
    a. Navigate to **Configuration > Device Management >Certificate Management > Identity Certificates**.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=asa.example.com, L=San Jos...	unstructuredName=asa.example...	15:09:09 CEDT Jul 1...	TP	General Purpose	RSA (2048 bits)

    b. Click **Add**.
    c. Define a trustpoint name.



Configuration > Device Management > Certificate Management > Identity Certificates

Trustpoint Name: SSL-Trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: <Default-RSA-Key>

Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

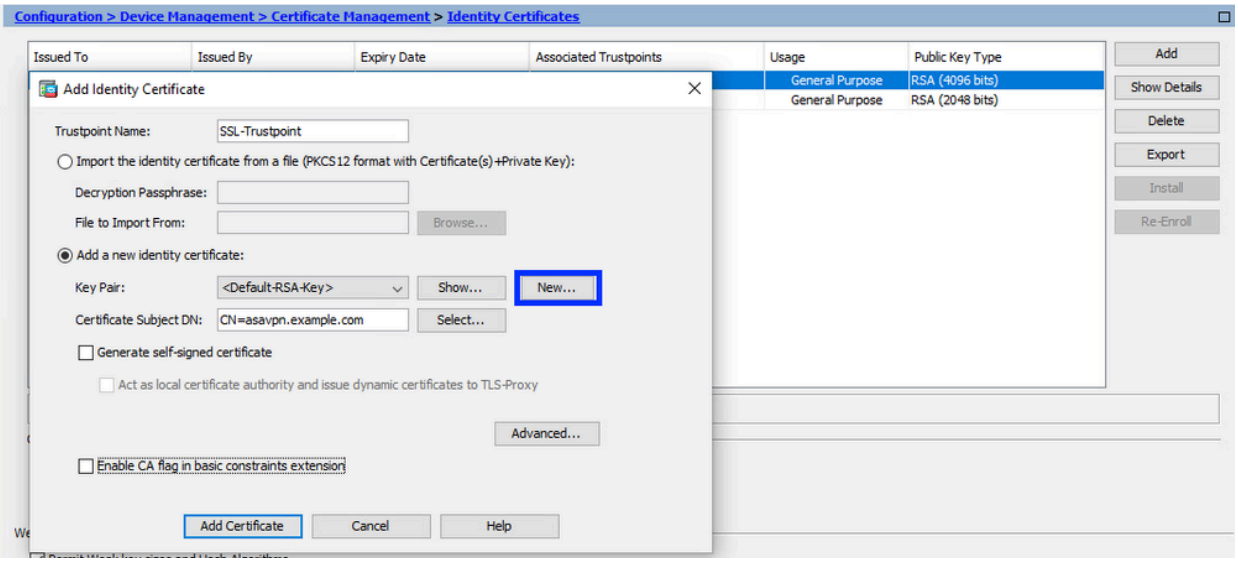
□ Enable CA flag in basic constraints extension

    d. Click the **Add a New Identity Certificate** radio button.

2. **(Optional) Create a New Key Pair**

Note: By default, the RSA key with the name of Default-RSA-Key and a size of 2048 is used. However, it is recommended to use a unique private/public Key Pair for each Identity Certificate.

a. Click **New** to generate a new Key Pair.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
				General Purpose	RSA (4096 bits)
				General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: <Default-RSA-Key>

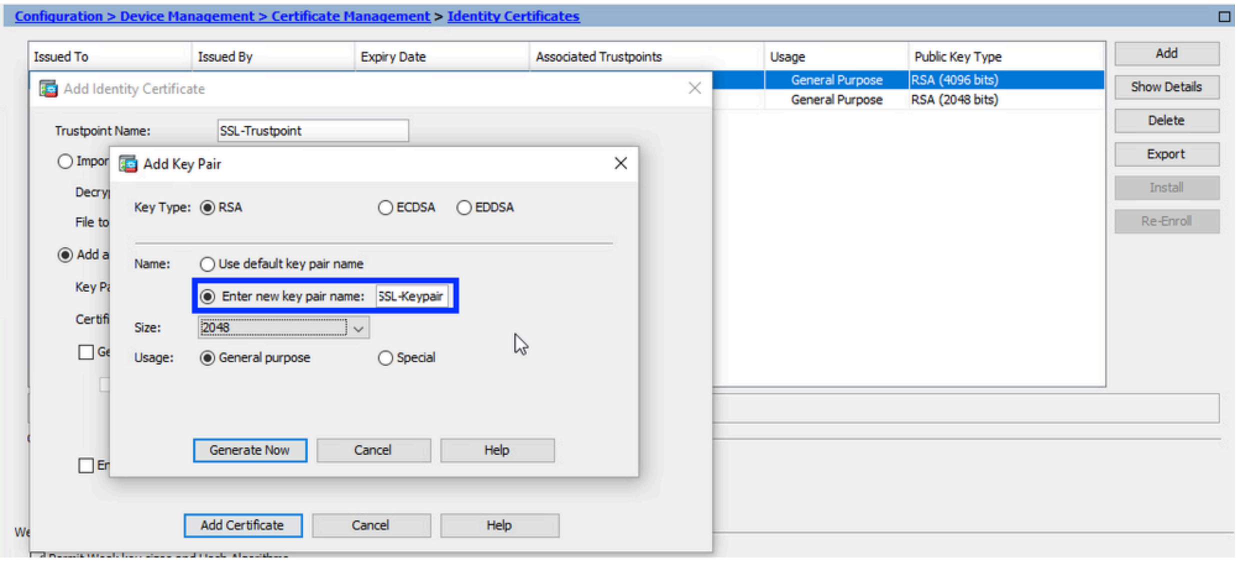
Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

b. Choose the option **Enter new Key Pair name** and enter a **name** for the new Key Pair.
c. Choose the **Key Type** - RSA or ECDSA.
d. Choose the **Key Size**; for RSA, choose General purpose for Usage.
e. Click **Generate Now**. The Key Pair is now created.



Add Key Pair

Key Type: ● RSA ○ ECDSA ○ EDDSA

Name: ○ Use default key pair name

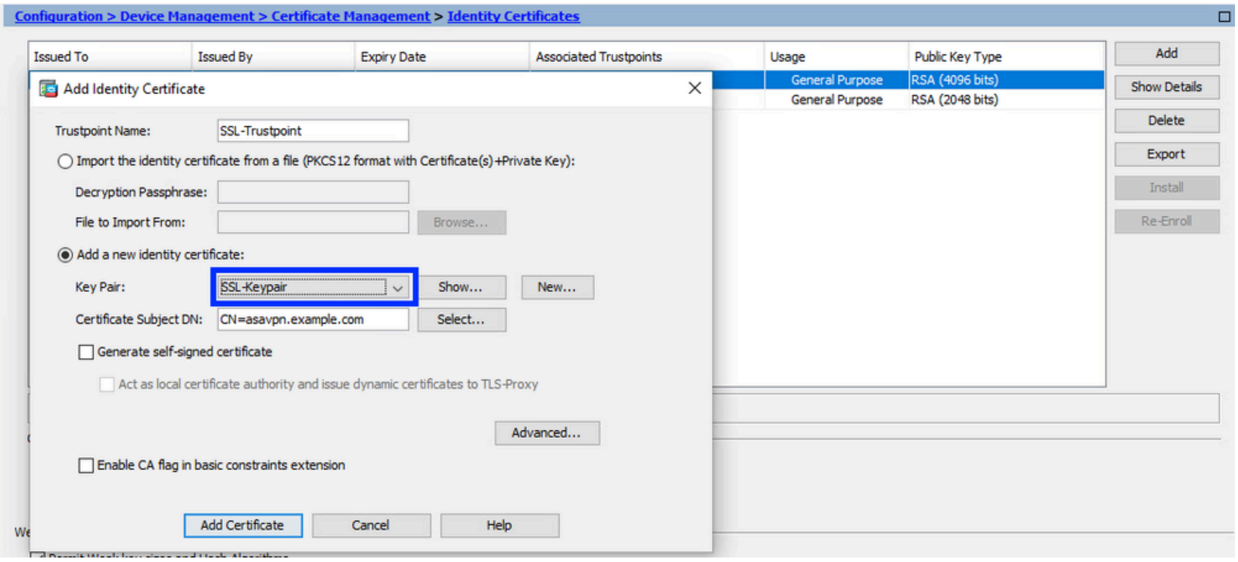
● Enter new key pair name: SSL-Keypair

Size: 2048

Usage: ● General purpose ○ Special

3. Choose the Key Pair Name

Choose the Key Pair to sign the CSR with, and to be binded with the new certificate.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
				General Purpose	RSA (4096 bits)
				General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-Keypair

Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

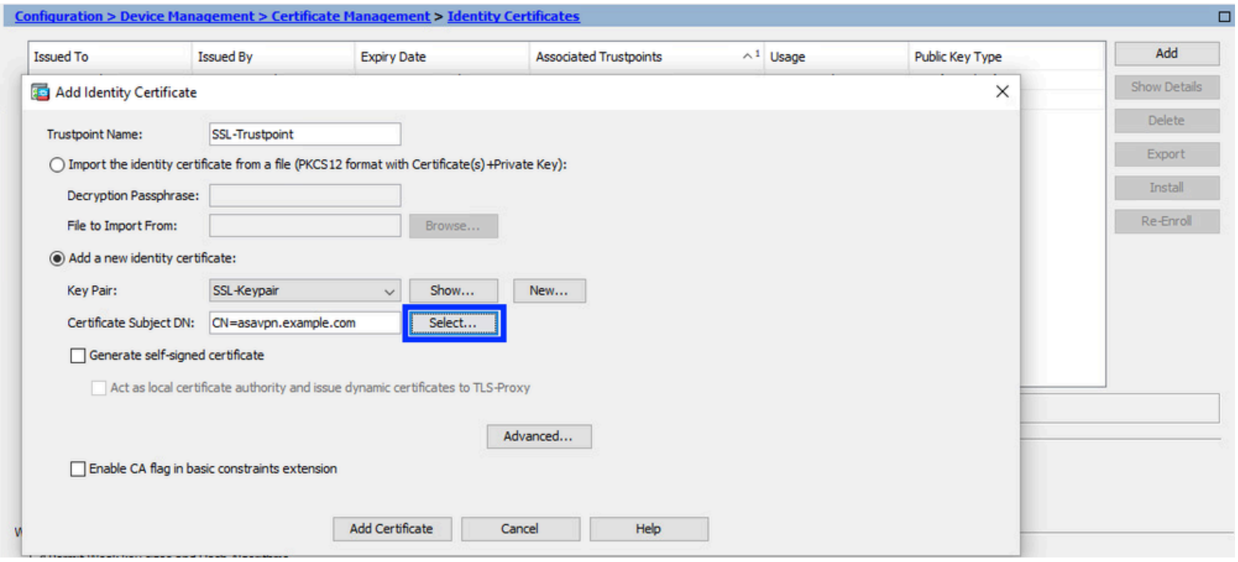
□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

4. **Configure the Certificate Subject and Fully Qualified Domain Name (FQDN)**

⚠ **Caution**: The FQDN parameter must match the FQDN or the IP address of the ASA interface that the Identity Certificate is used for. This parameter sets the requested Subject Alternative Name (SAN) extension for the Identity Certificate. The SAN extension is used by SSL/TLS/IKEv2 client to verify if the certificate matches the FQDN it connects to.

a. Click **Select**.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-Keypair

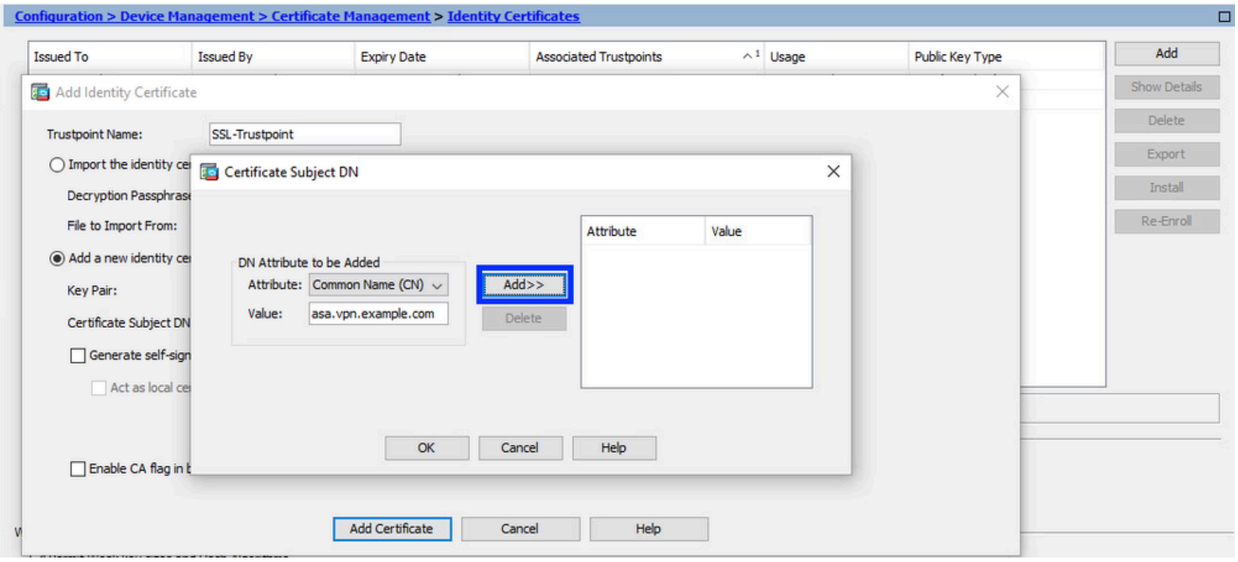
Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

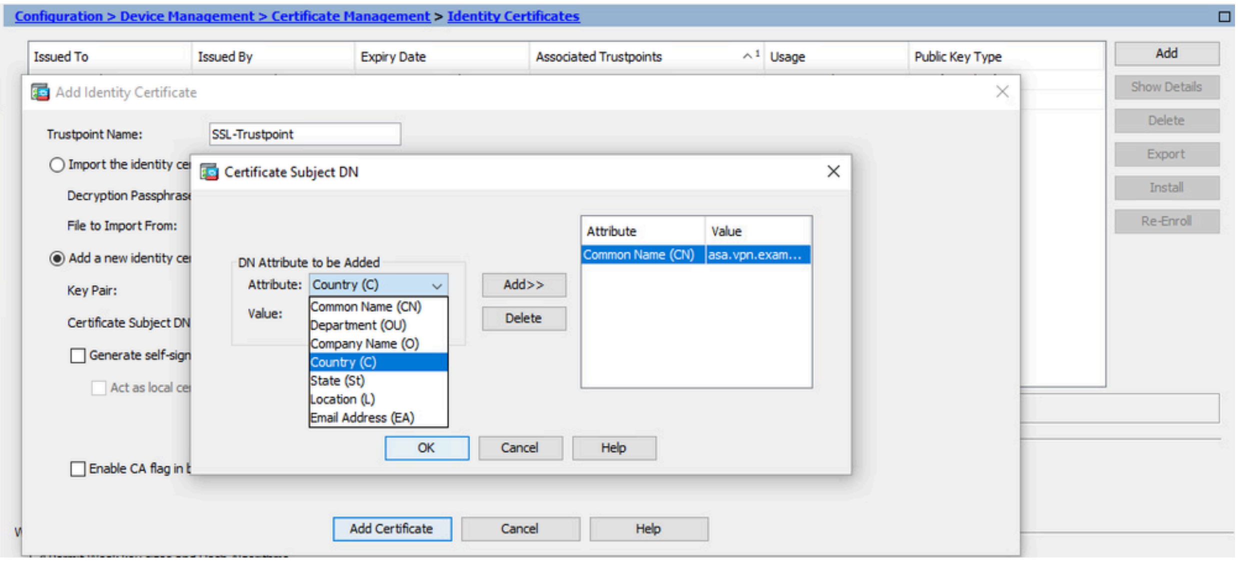
b. In the Certificate Subject DN window, configure certificate attributes - choose **attribute** from drop-down list, enter the **value**, click **Add**.



Trustpoint Name: SSL-Trustpoint

Attribute: Common Name (CN)

Value: asa.vpn.example.com



Trustpoint Name: SSL-Trustpoint

Attribute: Country (C)

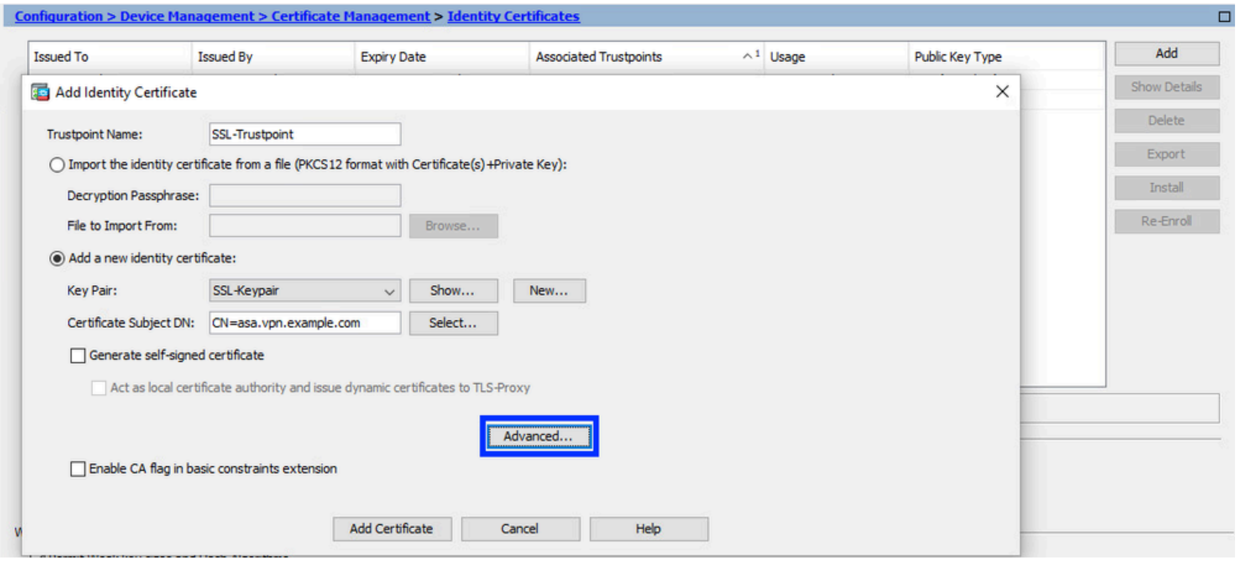
Attribute	Value
Common Name (CN)	asa.vpn.exam...

Attribute	Description
CN	The name through which the firewall can be accessed (usually the fully-qualified domain name, for example, vpn.example.com).
OU	The name of your department within the organization.
O	The legally registered name of your organization/company.
C	Country code (2 letter code without punctuation).
ST	The state in which your organization is located.
L	The city in which your organization is located.
EA	Email address

Note: None of the previous fields values can exceed a 64-character limit. Longer value could cause problems with the Identity Certificate installation. Also, It is not necessary to define all the DN attributes.

Click **OK** after all the attributes are added.

c. Configure the device FQDN - click **Advanced**.



Configuration > Device Management > Certificate Management > Identity Certificates

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-Keypair

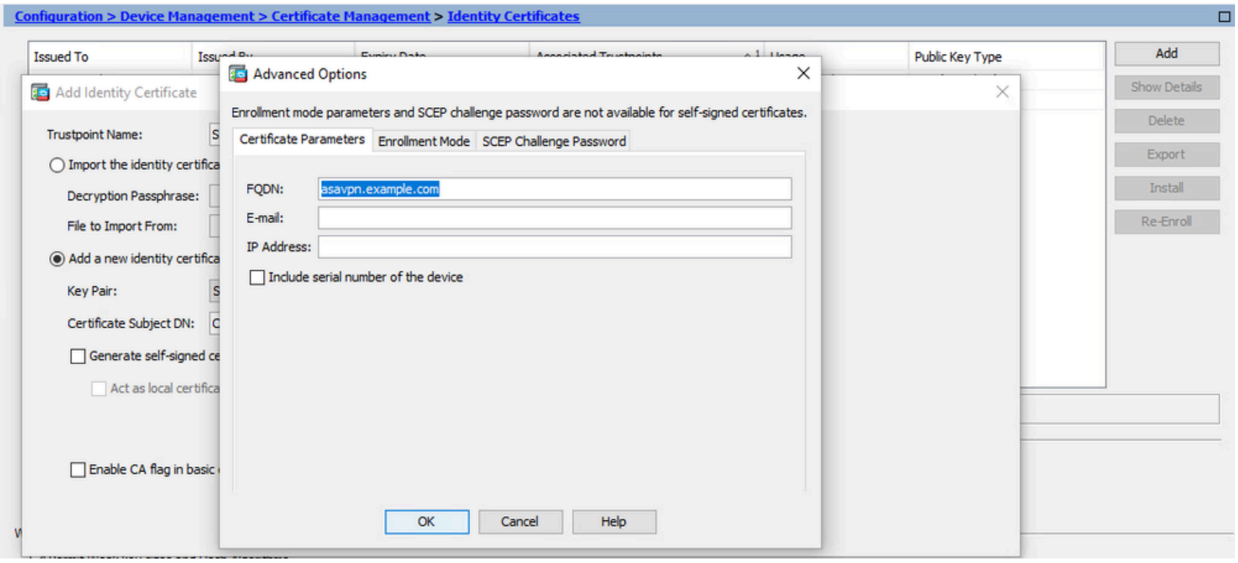
Certificate Subject DN: CN=asa.vpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

d. In the FQDN field, enter the **fully-qualified domain name** through which the device is accessible from the internet. Click **OK**.



Configuration > Device Management > Certificate Management > Identity Certificates

Advanced Options

Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.

FQDN: asavpn.example.com

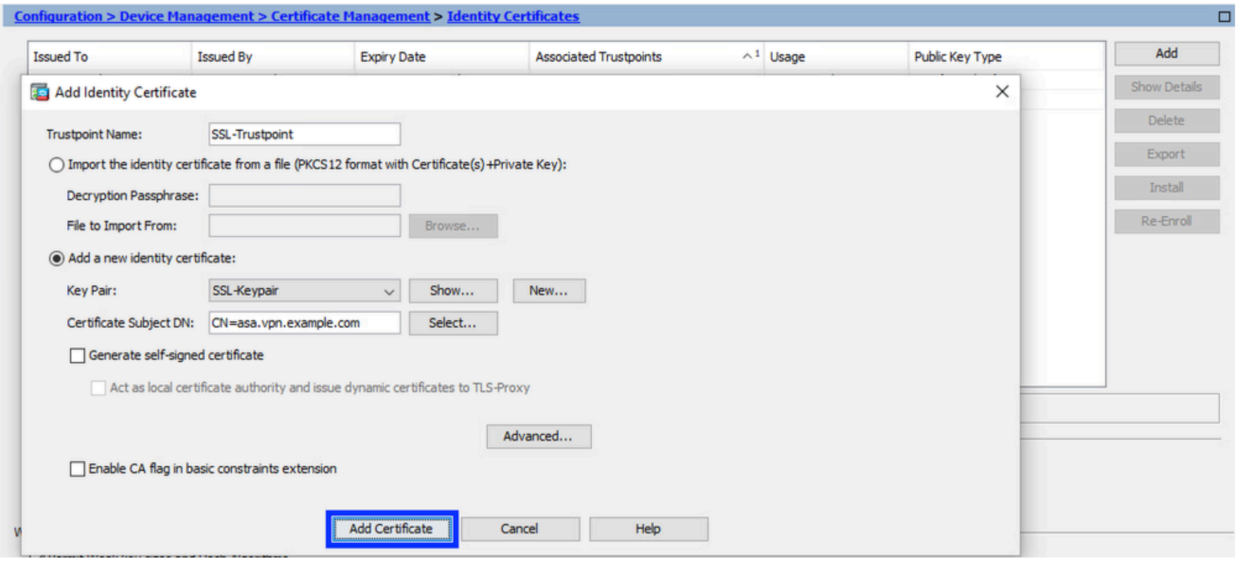
E-mail:

IP Address:

□ Include serial number of the device

5. Generate and Save the CSR

a. Click **Add Certificate**.



Configuration > Device Management > Certificate Management > Identity Certificates

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-Keypair

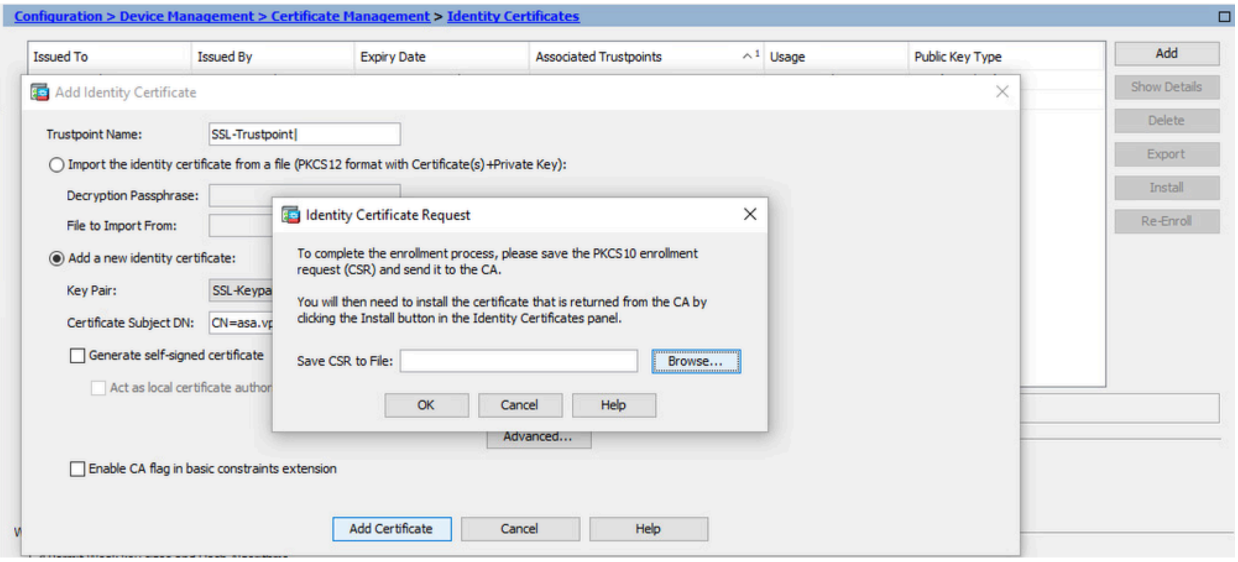
Certificate Subject DN: CN=asa.vpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

b. A prompt displays in order to **save** the CSR to a file on the local machine.



Configuration > Device Management > Certificate Management > Identity Certificates

Identity Certificate Request

To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.

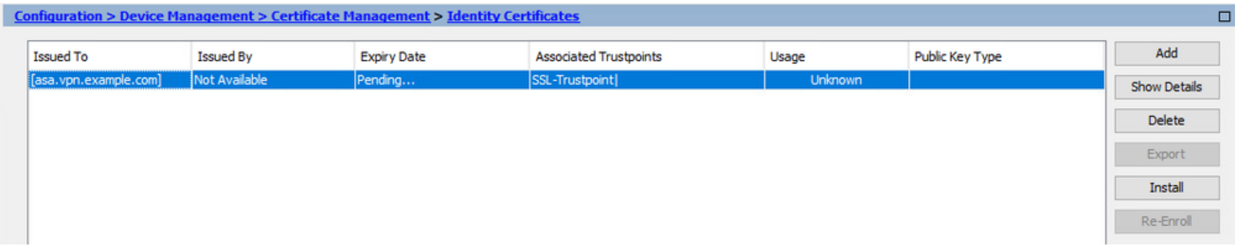
You will then need to install the certificate that is returned from the CA by clicking the Install button in the Identity Certificates panel.

Save CSR to File:

Click **Browse**, choose a **location** in which to save the CSR, and **save** the file with the .txt extension.

Note: When the file is saved with a .txt extension, the PKCS#10 request can be opened and viewed with a text editor (such as Notepad).

c. Now the new trustpoint is displayed in a Pending state.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
[asa.vpn.example.com]	Not Available	Pending...	SSL-Trustpoint	Unknown	

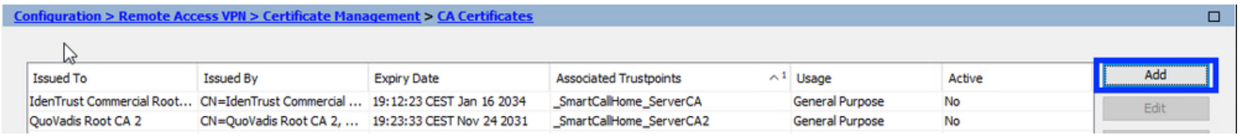
Install the Identity Certificate in PEM format with ASDM

The installation steps assume that the CA signed the CSR, and provided a PEM encoded (.pem,.cer, .crt)

Identity Certificate and CA certificate bundle.

1. **Install CA Certificate that Signed the CSR**

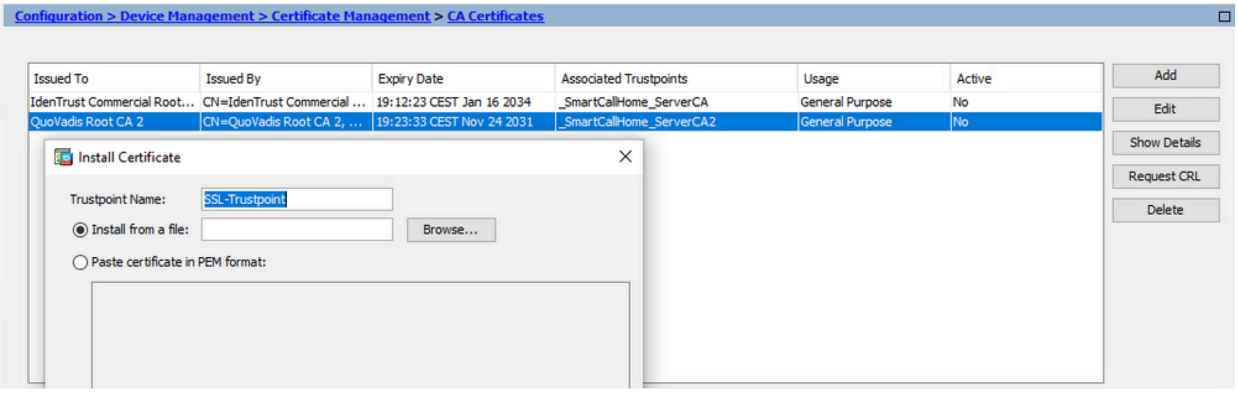
   a. Navigate to **Configuration** > **Device Management** >**Certificate Management** >, and choose **CA Certificates**. Click **Add**.



Configuration > Remote Access VPN > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No

   b. Enter the **Trustpoint name** and select **Install From File**, click **Browse** button, and select the **intermediate certificate**. Alternatively, paste the **PEM encoded CA certificate** from a text file into the **text** field.



Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No

Install Certificate

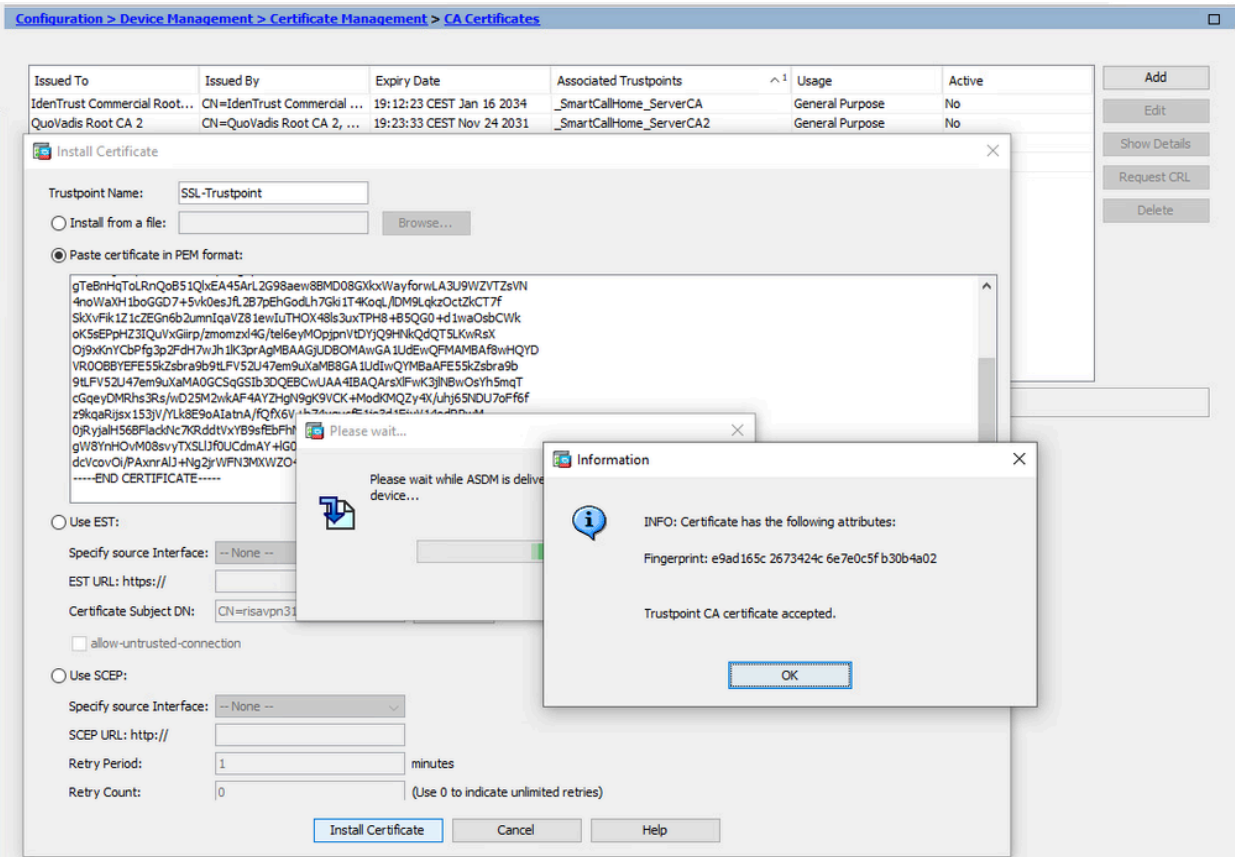
Trustpoint Name: SSL-Trustpoint

● Install from a file:

○ Paste certificate in PEM format:

Note: Install the CA certificate that signed the CSR. Use the same Trust Point name as the Identity Certificate. The other CA certificates higher in the PKI hierarchy can be installed in separate Trust Points.

   c. Click **Install Certificate**.



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No

Trustpoint Name: SSL-Trustpoint

○ Install from a file:

● Paste certificate in PEM format:

```
gTeBnHqToLRnQoB51QlxEA45ArL2G98aew8BMD08GXkxWayforwLA3U9WZVTZsVN
4noWaXH1boGGD7+5vk0esJfL2B7pEhGodLh7Gki1T4KoqL/lDM9LqkzOctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTHOX48ls3uxTPH8+B5QG0+d1waOsbCWk
oK5sEPpHZ3IQuVxGiirp/zmomzxl4G/tel6eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh1lK3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAf8wHQYD
VR0OBBYEFE55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMA0GCSqGSIb3DQEBCwUAA4IBAQArsXlFwK3jlNBwOsYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK9VCK+ModKMQZy4X/uhj65NDU7oFf6f
z9kqaRijsx153jV/YLk8E9oAIatnA/fQfX6V
0jRyjalH56BFlackNc7KRddtVxYB9sfEbFh
gW8YnHOvM08svyTXSLlJf0UCdmAY+lG0
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO
-----END CERTIFICATE-----
```

○ Use EST:

Specify source Interface: -- None --

EST URL: https://

Certificate Subject DN: CN=risavpn31

☐ allow-untrusted-connection

○ Use SCEP:

Specify source Interface: -- None --

SCEP URL: http://

Retry Period: 1 minutes

Retry Count: 0 (Use 0 to indicate unlimited retries)

Please wait while ASDM is deliv
device...

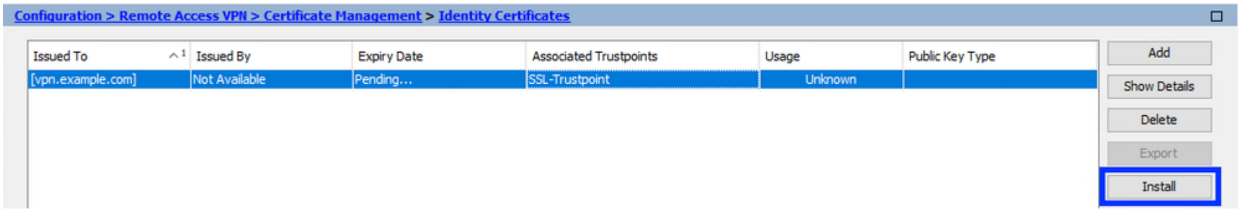
INFO: Certificate has the following attributes:

Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02

Trustpoint CA certificate accepted.

2. **Install Identity Certificate**

a. Choose the **Identity Certificate** created previously during the CSR generation. Click **Install**.

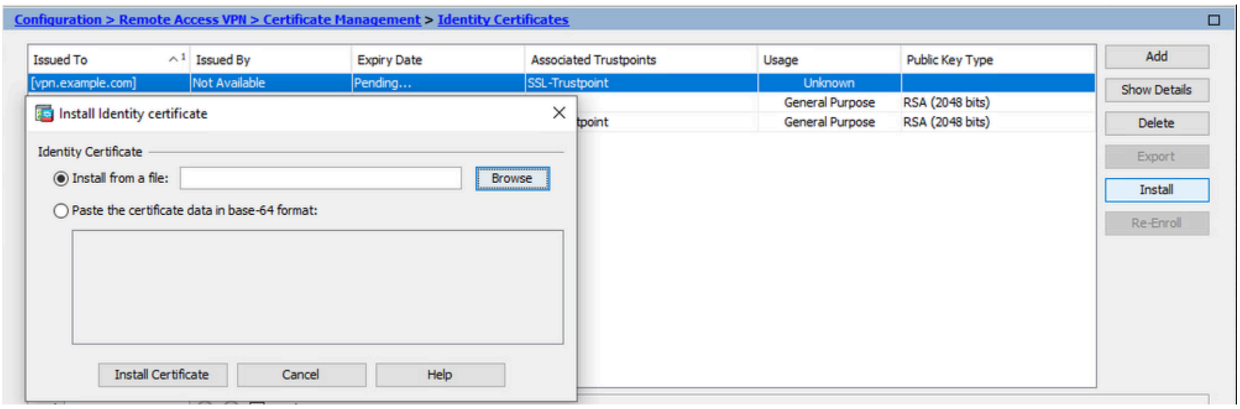


Configuration > Remote Access VPN > Certificate Management > Identity Certificates
Add
Show Details
Delete
Export
Install

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
[vpn.example.com]	Not Available	Pending...	SSL-Trustpoint	Unknown	

Note: The Identity Certificate can have Issued By field as Not available and the Expiry Date field as Pending.

b. Choose a file that contains the **PEM encoded Identity Certificate** received from the CA, or open the **PEM encoded certificate** in a text editor and copy and paste the Identity Certificate provided by the CA into the text field.



Configuration > Remote Access VPN > Certificate Management > Identity Certificates
Add
Show Details
Delete
Export
Install
Re-Enroll
Install Identity certificate
Browse
Install Certificate
Cancel
Help

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
[vpn.example.com]	Not Available	Pending...	SSL-Trustpoint	Unknown	
			tpoint	General Purpose	RSA (2048 bits)
				General Purpose	RSA (2048 bits)

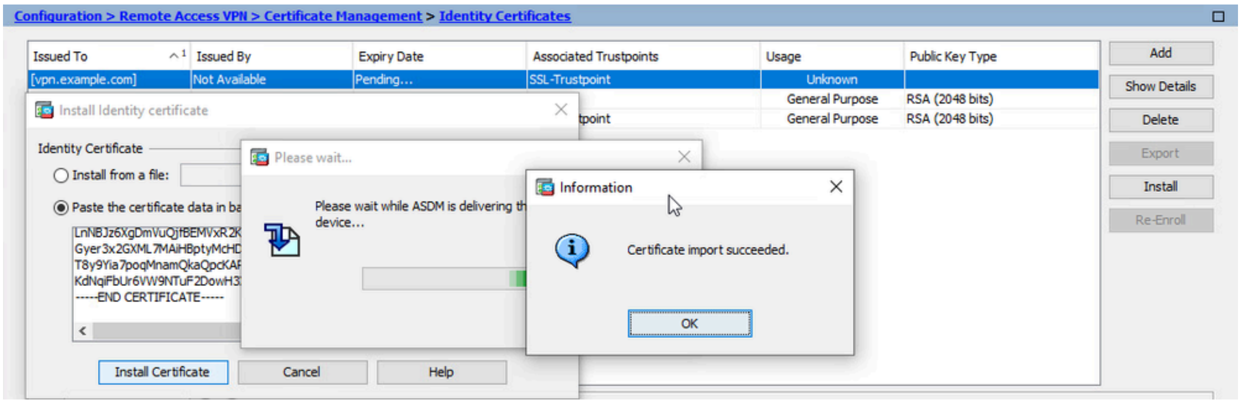
Identity Certificate

● Install from a file:

○ Paste the certificate data in base-64 format:

Note: Identity certificate can be in .pem, .cer, .crt format to install.

c. Click **Install Certificate**.



Configuration > Remote Access VPN > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
[vpn.example.com]	Not Available	Pending...	SSL-Trustpoint	Unknown	
				General Purpose	RSA (2048 bits)
			tpoint	General Purpose	RSA (2048 bits)

Install Identity certificate

Identity Certificate

○ Install from a file:

● Paste the certificate data in ba

```
LnNBJz6XgDmVuQjfBEMVxR2K
Gyer3x2GXML7MAiHBptyMcHD
T8y9Yia7poqMnamQkaQpcKAF
KdNqiFbUr6VW9NTuF2DowH3
-----END CERTIFICATE-----
```

Please wait...

Please wait while ASDM is delivering th device...

Information

Certificate import succeeded.

3. **Bind the New Certificate to Interface with ASDM**

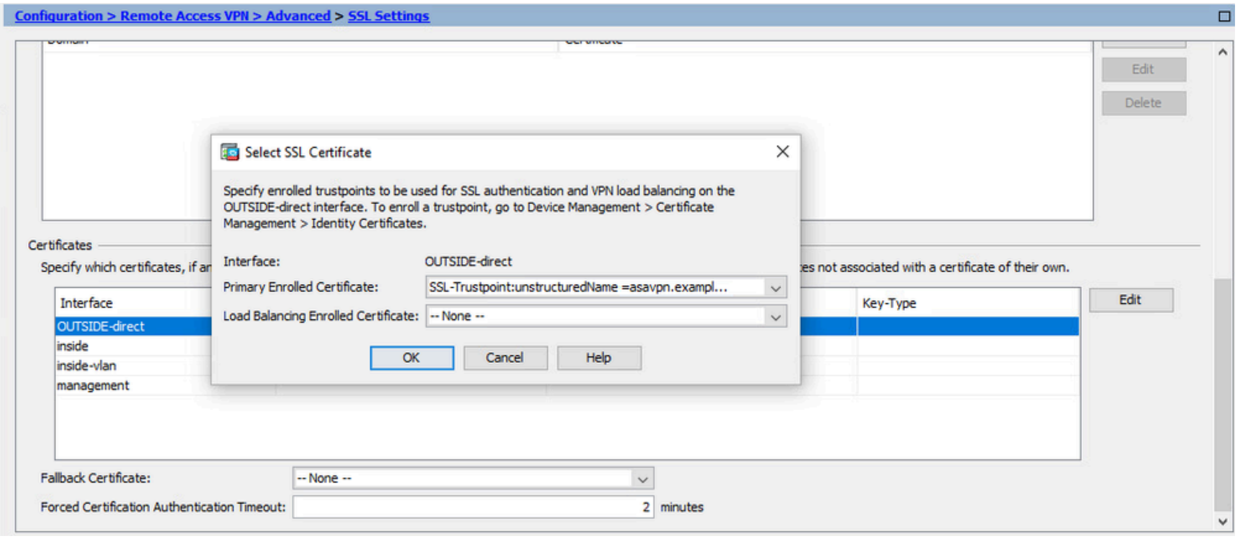
The ASA needs to be configured to use the new Identity Certificate for WebVPN sessions that terminate on the interface specified.

a. Navigate to **Configuration** > **Remote Access VPN** > **Advanced** > **SSL Settings**.

b. Under Certificates, choose the **interface** that is used to terminate WebVPN sessions. In this example, the outside interface is used.

Click **Edit**.

c. In the **Certificate** drop-down list, choose the **newly installed certificate**.



Configuration > Remote Access VPN > Advanced > SSL Settings

Certificates

Specify which certificates, if ar ...es not associated with a certificate of their own.

Interface		Key-Type
OUTSIDE-direct		
inside		
inside-vlan		
management		

Fallback Certificate: -- None --

Forced Certification Authentication Timeout: 2 minutes

Select SSL Certificate

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate Management > Identity Certificates.

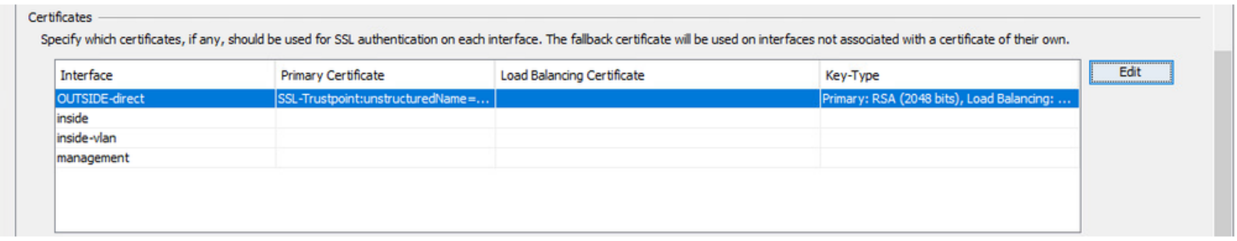
Interface: OUTSIDE-direct

Primary Enrolled Certificate: SSL-Trustpoint:unstructuredName =asavpn.exampl...

Load Balancing Enrolled Certificate: -- None --

d. Click **OK**.

e. Click **Apply**.



Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Primary Certificate	Load Balancing Certificate	Key-Type
OUTSIDE-direct	SSL-Trustpoint:unstructuredName=...		Primary: RSA (2048 bits), Load Balancing: ...
inside			
inside-vlan			
management			

Now the new Identity Certificate is in use.

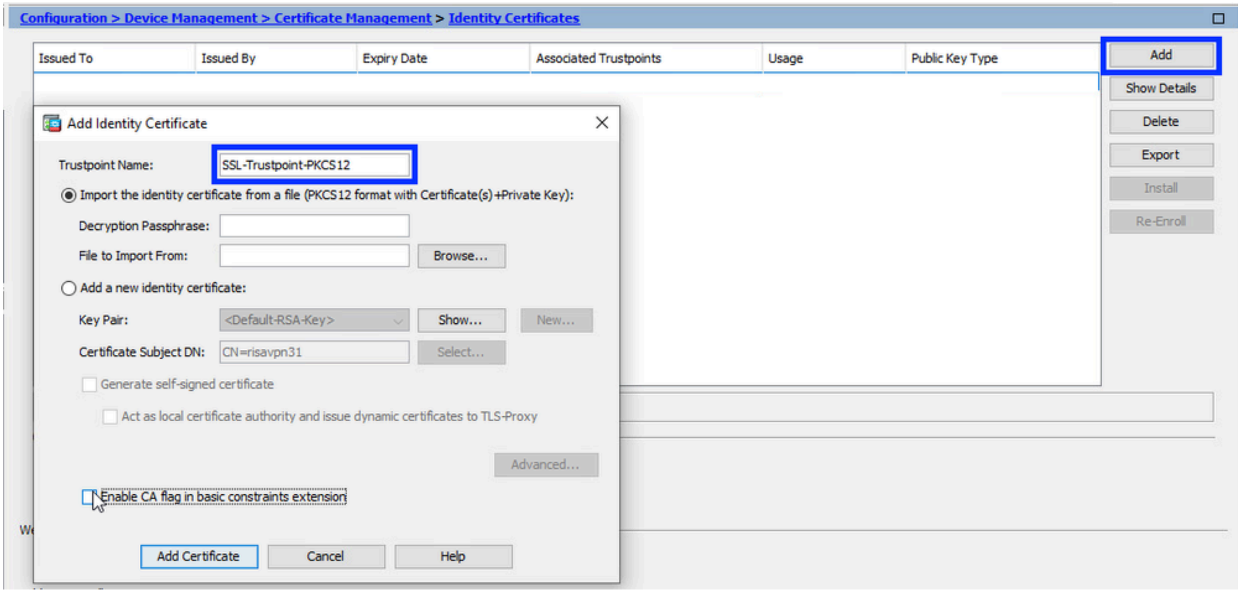
Install an Identity Certificate Received in PKCS12 Format with ASDM

PKCS12 file (.p12 or .pfx format) contains Identity Certificate, Key Pair, and CA certificate(s). It is created by the CA, in case of wildcard certificate, or exported from a different device. It is a binary file, and cannot be viewed with text editor.

1. Install the Identity and CA Certificates from a PKCS12 File

Identity Certificate, CA certificate(s) and Key Pair needs to be bundled into a single PKCS12 file.

a. Navigate to **Configuration** > **Device Management** > **Certificate Management**, and choose **Identity Certificates**.
b. Click **Add**.
c. Specify a **Trustpoint Name**.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

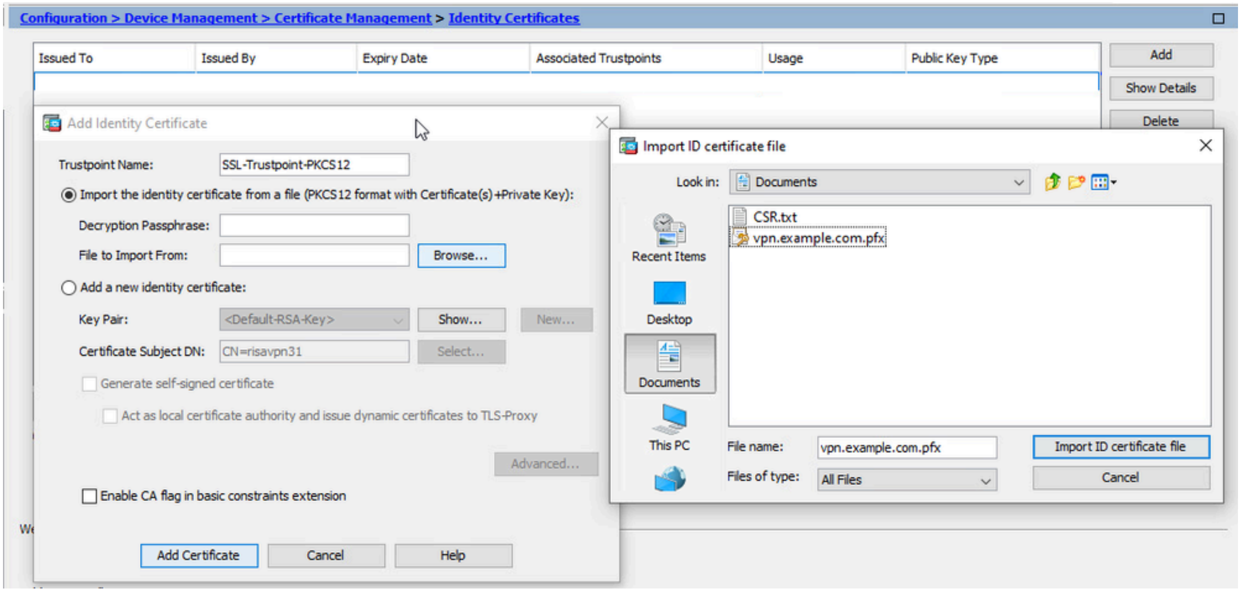
Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

d. Click the **Import The Identity Certificate** from a File radio button.



Configuration > Device Management > Certificate Management > Identity Certificates

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

Import ID certificate file

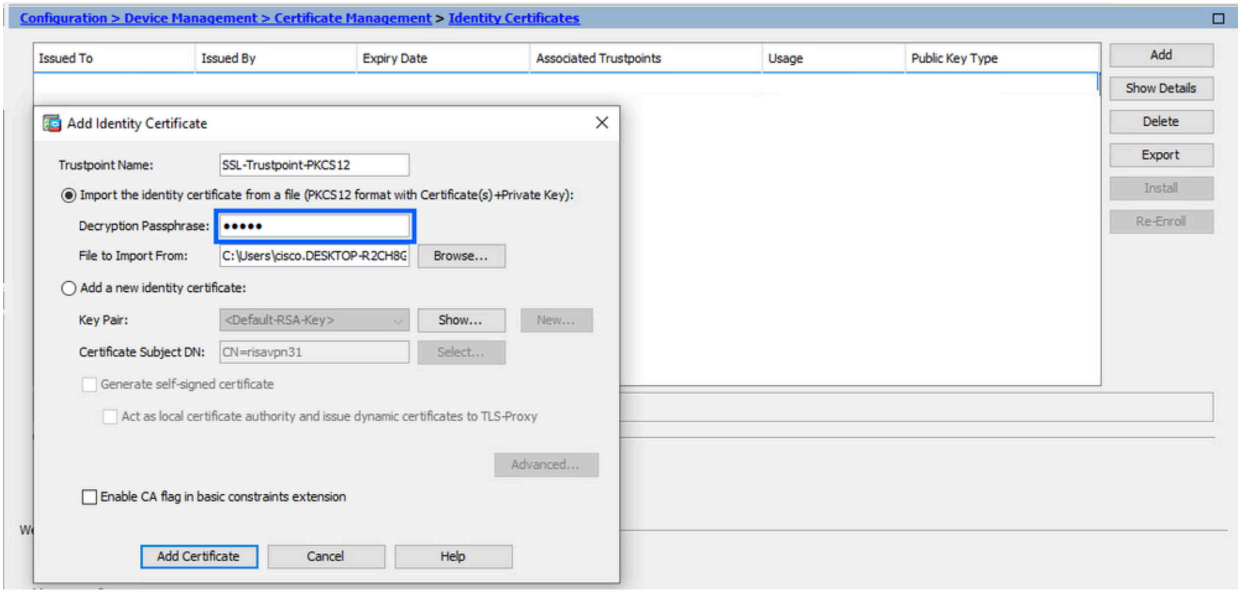
Look in: Documents

CSR.txt
vpn.example.com.pfx

File name: vpn.example.com.pfx

Files of type: All Files

e. Enter the **passphrase** used to create the PKCS12 file.



Configuration > Device Management > Certificate Management > Identity Certificates

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase: •••••

File to Import From: C:\Users\cisco.DESKTOP-R2CH8G

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

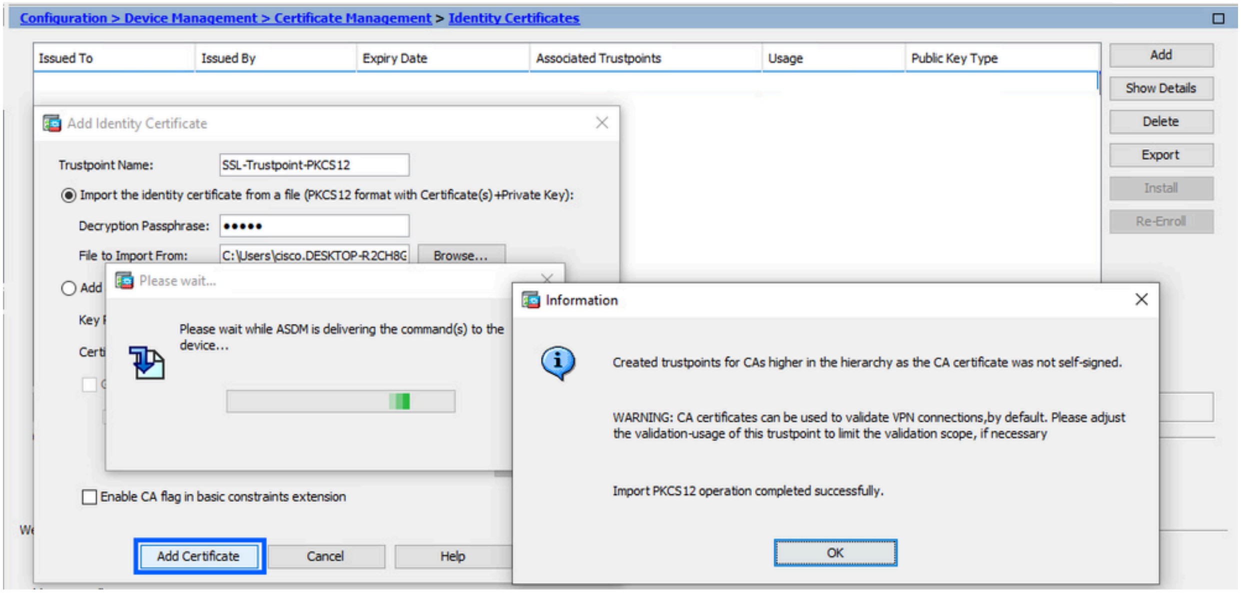
Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

f. Click **Add Certificate**.



Configuration > Device Management > Certificate Management > Identity Certificates

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase: •••••

File to Import From: C:\Users\cisco.DESKTOP-R2CH8G

□ Enable CA flag in basic constraints extension

Please wait...

Please wait while ASDM is delivering the command(s) to the device...

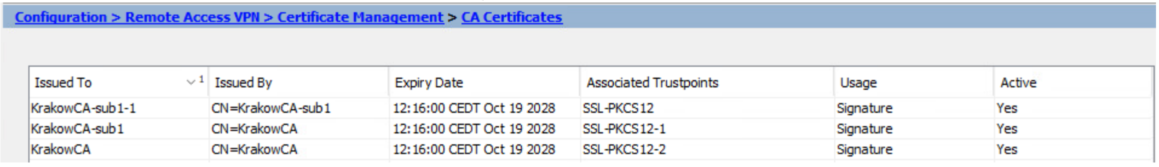
Information

Created trustpoints for CAs higher in the hierarchy as the CA certificate was not self-signed.

WARNING: CA certificates can be used to validate VPN connections,by default. Please adjust the validation-usage of this trustpoint to limit the validation scope, if necessary

Import PKCS12 operation completed successfully.

Note: When you import a PKCS12 with CA certificates chain, the ASDM creates the upstream CA trustpoints automatically with names with added -number suffix.



Configuration > Remote Access VPN > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

2. Bind the New Certificate to Interface with ASDM

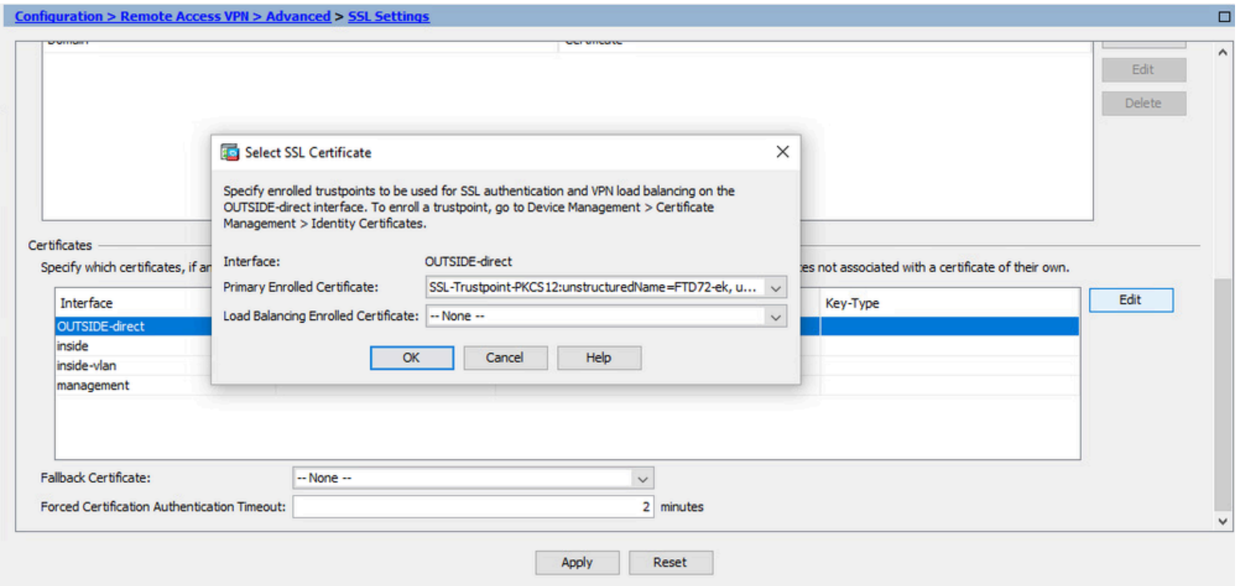
The ASA needs to be configured to use the new Identity Certificate for WebVPN sessions that terminate on the interface specified.

a. Navigate to **Configuration > Remote Access VPN > Advanced > SSL Settings**.

b. Under Certificates, select the interface that is used to terminate WebVPN sessions. In this example, the outside interface is used.

Click **Edit**.

c. In the Certificate drop-down list, choose the newly installed certificate.



Configuration > Remote Access VPN > Advanced > SSL Settings

Select SSL Certificate

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate Management > Identity Certificates.

Interface: OUTSIDE-direct

Primary Enrolled Certificate: SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u...

Load Balancing Enrolled Certificate: -- None --

Certificates

Specify which certificates, if ar ...es not associated with a certificate of their own.

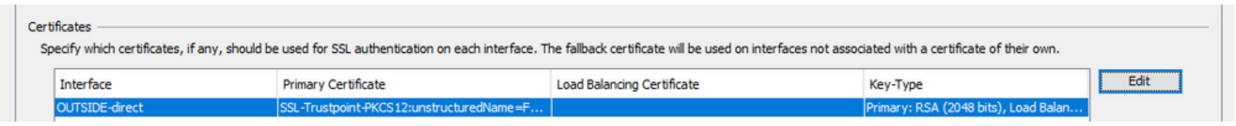
Interface	Key-Type
OUTSIDE-direct	
inside	
inside-vlan	
management	

Fallback Certificate: -- None --

Forced Certification Authentication Timeout: 2 minutes

d. Click **OK**.

e. Click **Apply**.



Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Primary Certificate	Load Balancing Certificate	Key-Type
OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName=F...		Primary: RSA (2048 bits), Load Balan...

Now the new Identity Certificate is in use.

Certificate Renewal

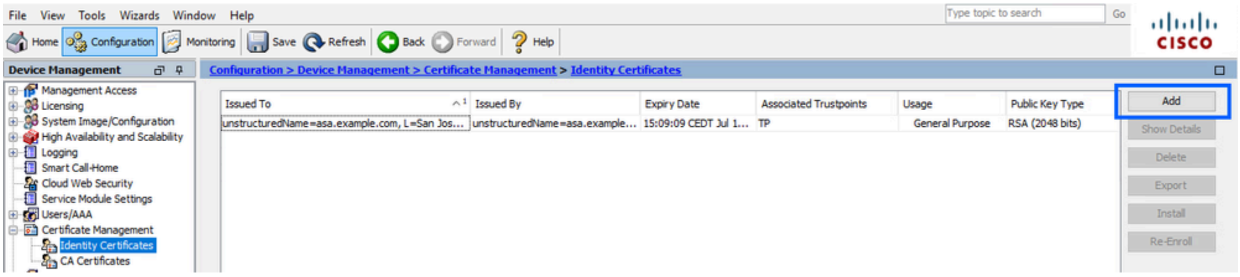
Renew a Certificate Enrolled with Certificate Signing Request (CSR) with ASDM

Certificate renewal of CSR enrolled certificate requires you to create and enroll a new Trustpoint. It needs to have a different name (for example, old name with enroll year suffix). It can use the same parameters and Key Pair as the old certificate, or can use different ones.

Generate a CSR with ASDM

1. **Create a New Trustpoint with a Specific Name**

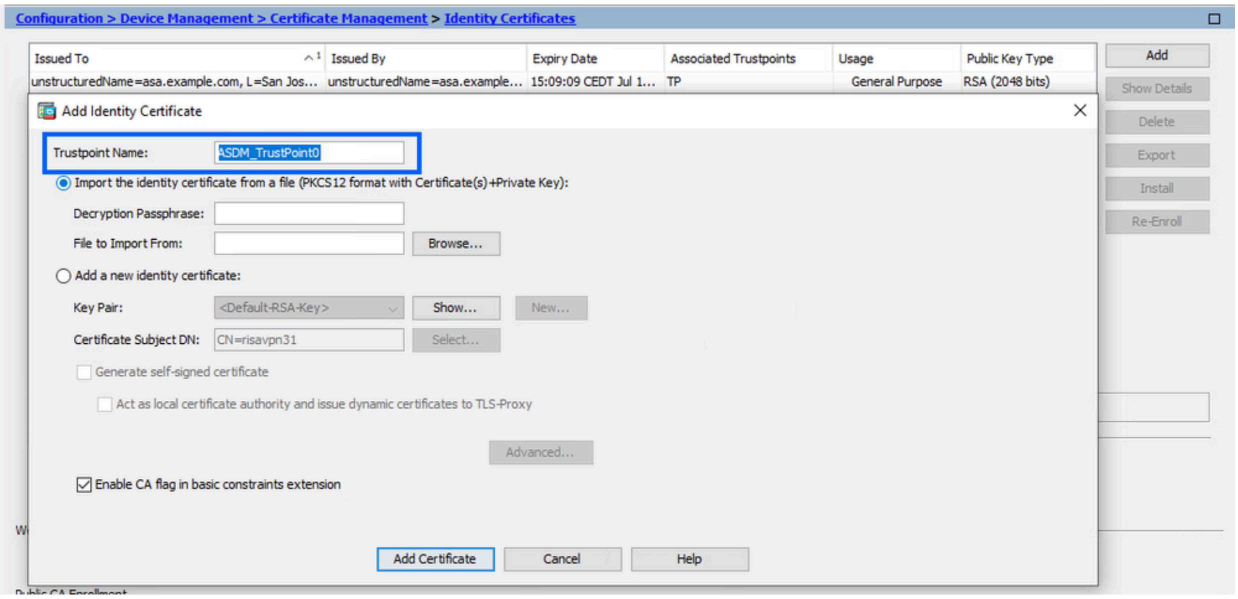
   a. Navigate to **Configuration** > **Device Management** >**Certificate Management** > **Identity Certificates**.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=asa.example.com, L=San Jos...	unstructuredName=asa.example...	15:09:09 CEDT Jul 1...	TP	General Purpose	RSA (2048 bits)

   b. Click **Add**.
   c. Define a **Trustpoint Name**.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=asa.example.com, L=San Jos...	unstructuredName=asa.example...	15:09:09 CEDT Jul 1...	TP	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: ASDM_TrustPoint0

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

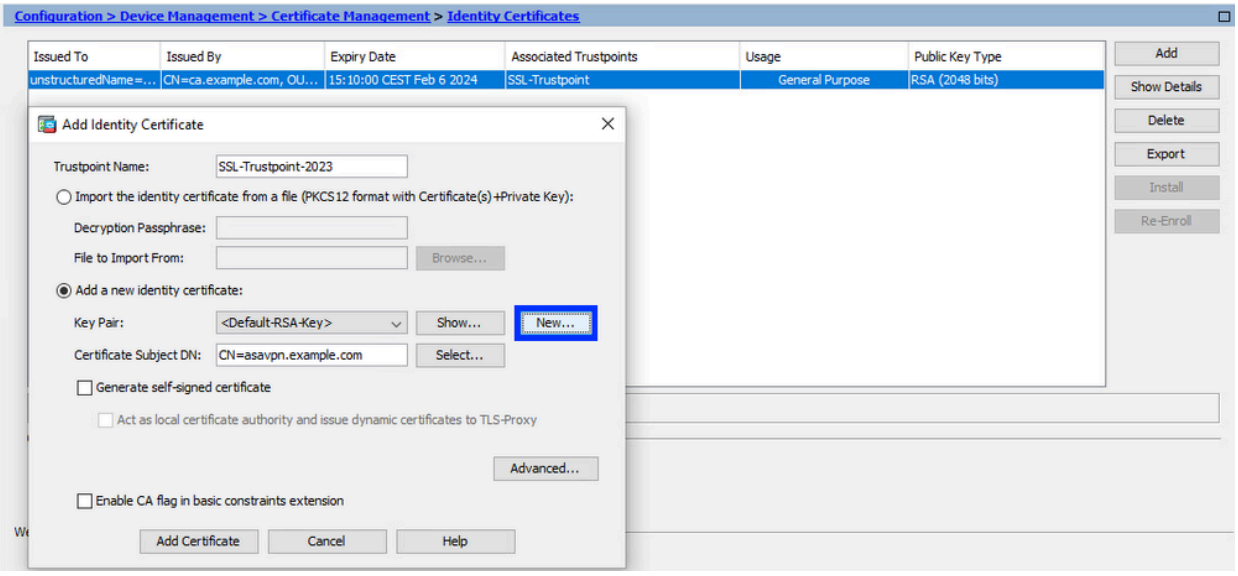
☑ Enable CA flag in basic constraints extension

   d. Click**Add a New Identity Certificate** radio button.

2. **(Optional) Create a New Key Pair**

> **Note:** By default, the RSA key with the name of Default-RSA-Key and a size of 2048 is used; however, it is recommended to use a unique private/public Key Pair for each Identity Certificate.

   a. Click **New** to generate a new Key Pair.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: <Default-RSA-Key>

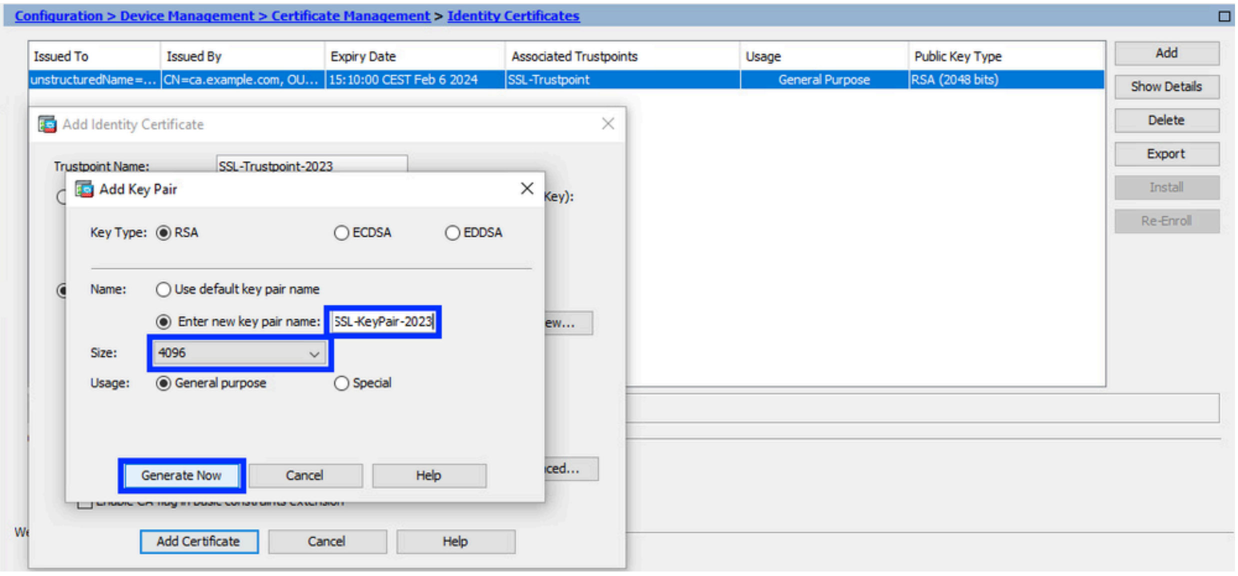
Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

b. Choose the option **Enter new Key Pair name** and enter a **name** for the new Key Pair.
c. Choose the **Key Type** - RSA or ECDSA.
d. Choose the **Key Size**; for RSA, choose General purpose for Usage.
e. Click **Generate Now**. The Key Pair is now created.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

Add Key Pair

Key Type: ● RSA ○ ECDSA ○ EDDSA

Name: ○ Use default key pair name

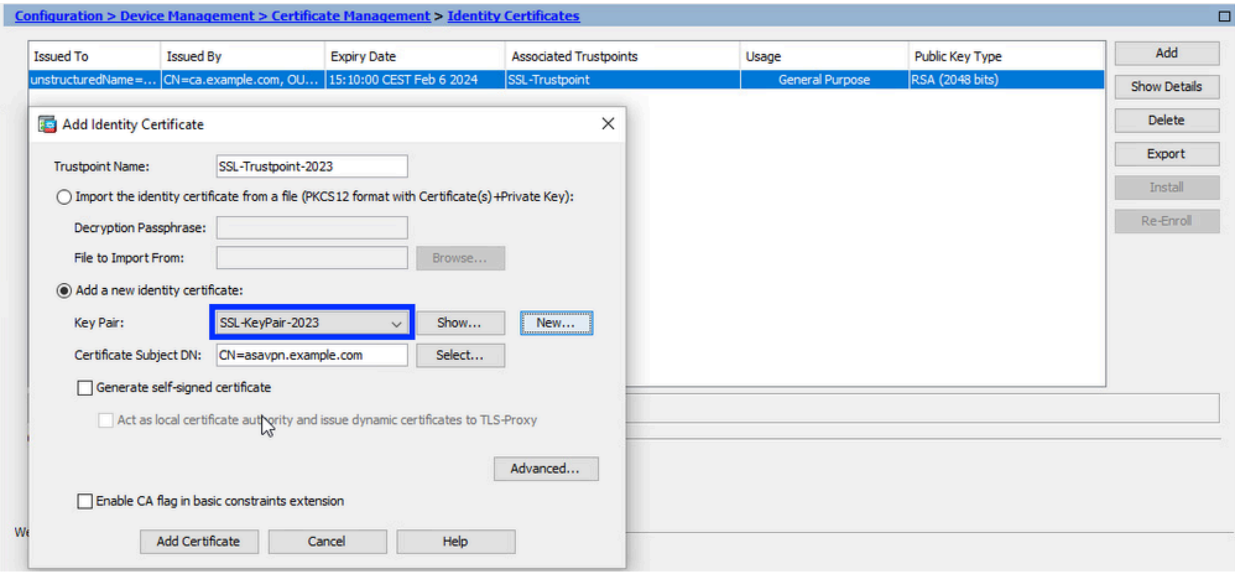
● Enter new key pair name: SSL-KeyPair-2023

Size: 4096

Usage: ● General purpose ○ Special

3. Select the Key Pair Name

Choose the **Key Pair** to sign the CSR with, and to be binded with the new certificate.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-KeyPair-2023

Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

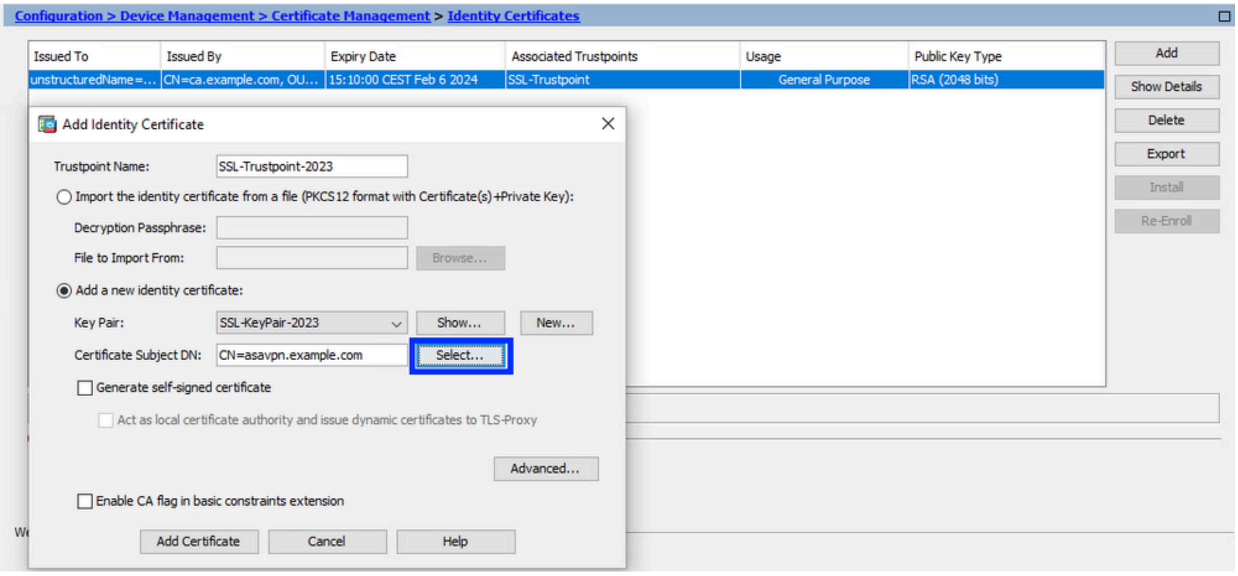
□ Enable CA flag in basic constraints extension

4. **Configure the Certificate Subject and Fully Qualified Domain Name (FQDN)**

Caution: The FQDN parameter must match the FQDN or the IP address of the ASA interface that the certificate is used for. This parameter sets the Subject Alternative Name (SAN) for the certificate. The SAN field is used by SSL/TLS/IKEv2 client to verify if the certificate matches the FQDN it is connects to.

Note: CA can alter the FQDN and Subject Name parameters defined in the trustpoint when it signs the CSR and creates a signed Identity Certificate.

a. Click **Select**.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-KeyPair-2023

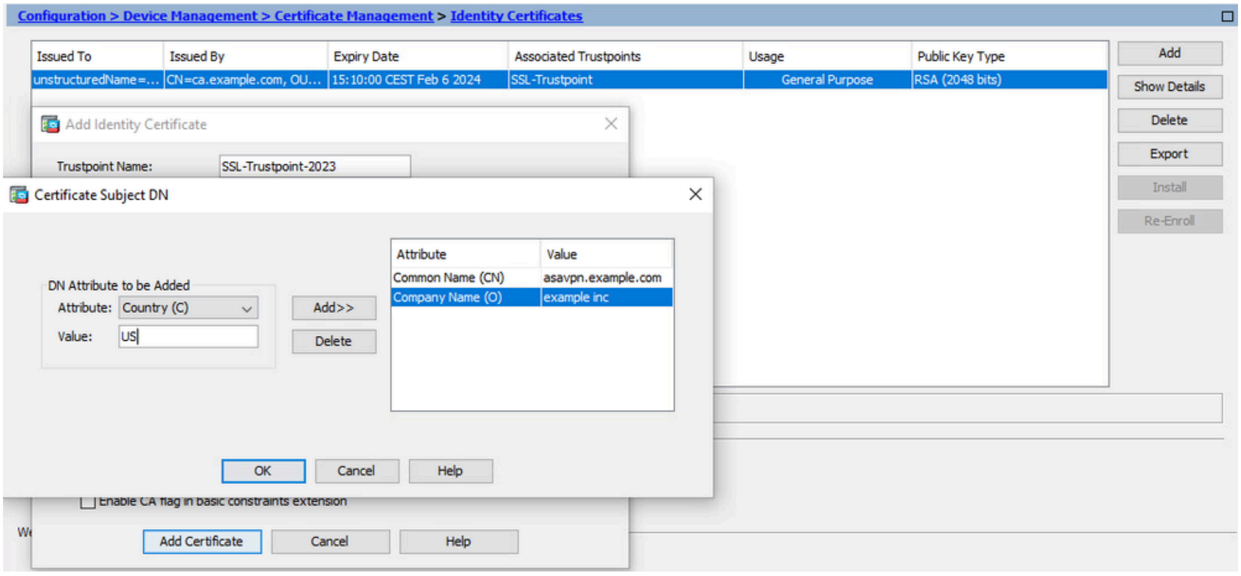
Certificate Subject DN: CN=asavpn.example.com

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

b. In the Certificate Subject DN window, configure **certificate attributes** - select attribute from drop-down list, enter the **value**, click **Add**.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Trustpoint Name: SSL-Trustpoint-2023

Attribute: Country (C)

Value: US

Attribute	Value
Common Name (CN)	asavpn.example.com
Company Name (O)	example inc

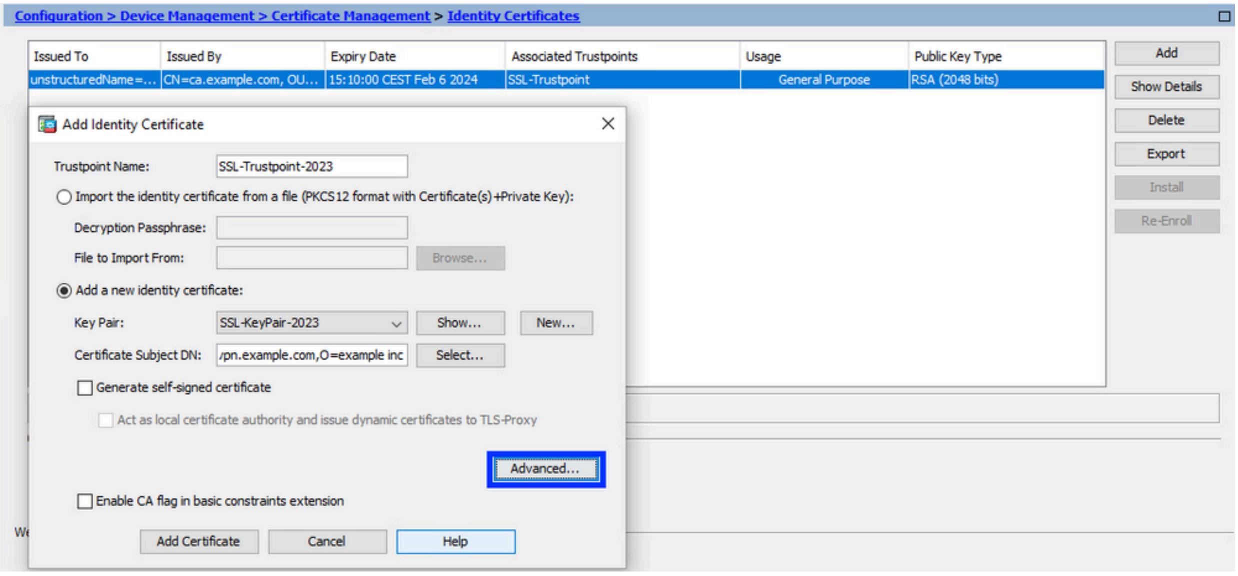
□ Enable CA flag in basic constraints extension

Attribute	Description
CN	The name through which the firewall can be accessed (usually the fully-qualified domain name, for example, vpn.example.com).
OU	The name of your department within the organization.
O	The legally registered name of your organization/company.
C	Country code (2 letter code without punctuation)
ST	The state in which your organization is located.
L	The city in which your organization is located.
EA	Email address

Note: None of the previous fields can exceed a 64-character limit. Longer value could cause problems with the Identity Certificate installation. Also, It is not necessary to define all the DN attributes.

Click **OK** after all the attributes are added.

c. To configure device FQDN, click **Advanced**.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=…	CN=ca.example.com, OU…	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-KeyPair-2023

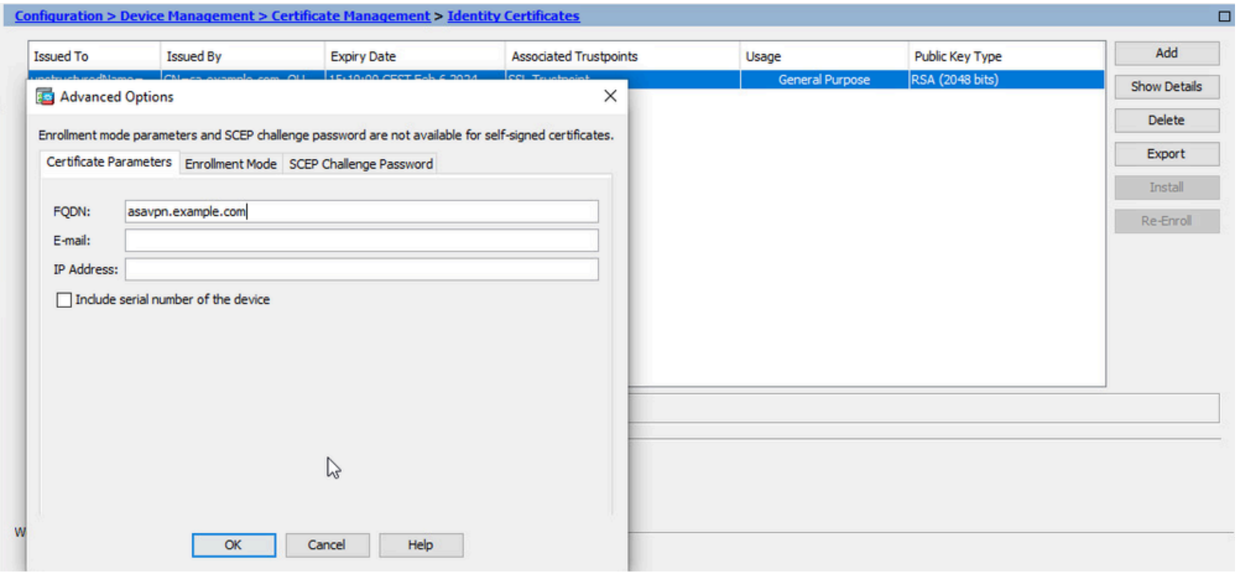
Certificate Subject DN: /pn.example.com,O=example inc

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

d. In the FQDN field, enter the **fully-qualified domain name** through which the device is accessible from the internet. Click **OK**.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
				General Purpose	RSA (2048 bits)

Advanced Options

Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.

FQDN: asavpn.example.com

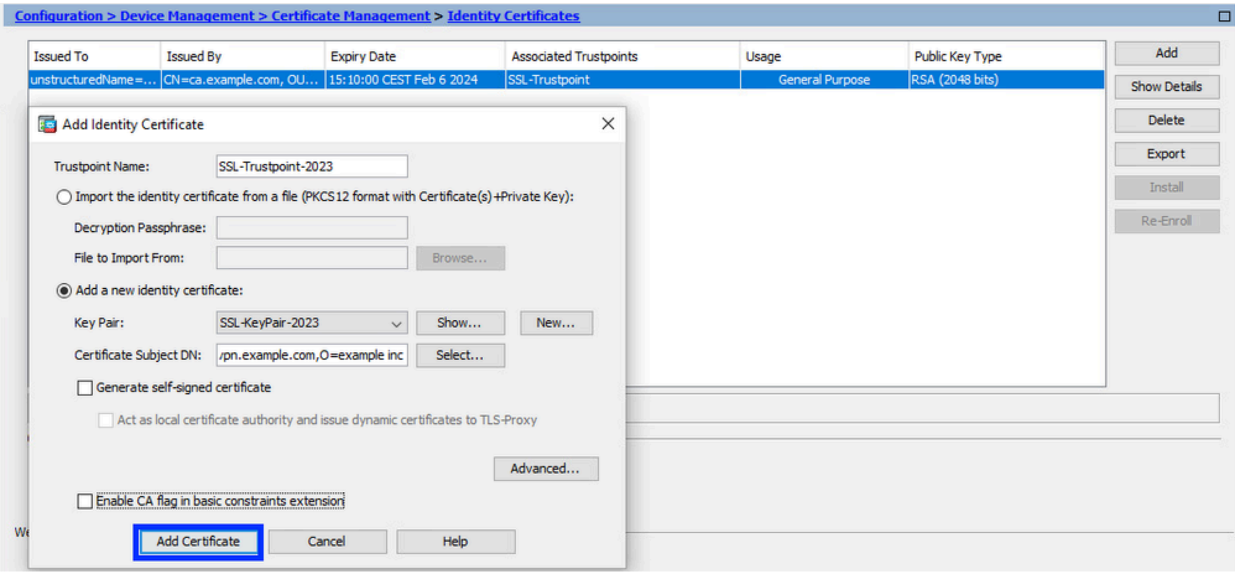
E-mail:

IP Address:

□ Include serial number of the device

5. **Generate and Save the CSR**

a. Click **Add Certificate**.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SSL-KeyPair-2023

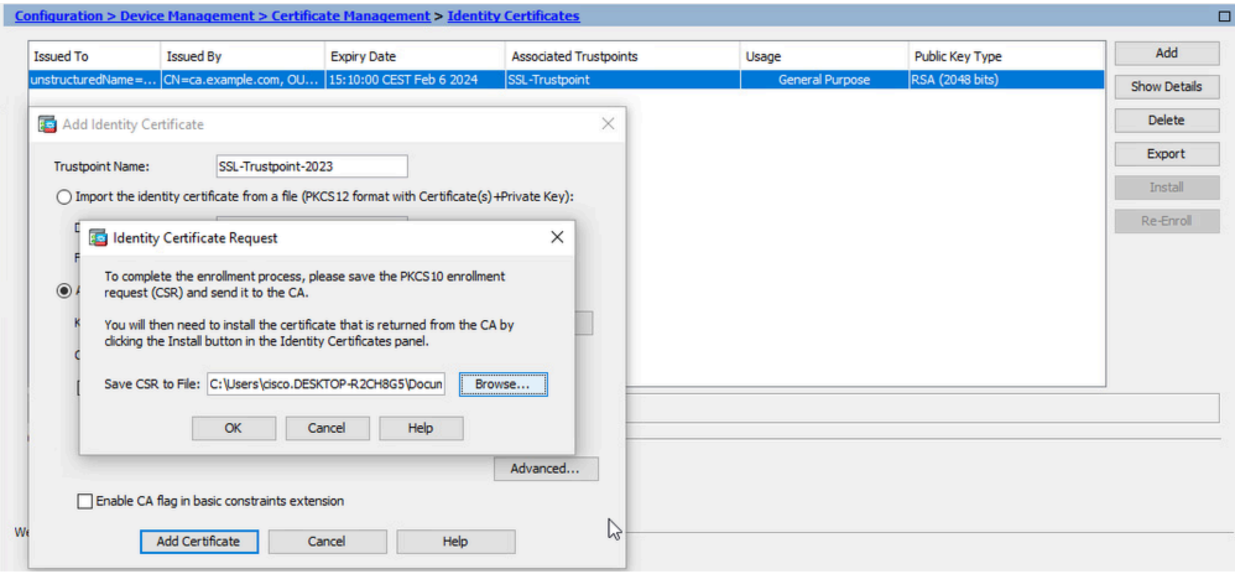
Certificate Subject DN: /pn.example.com,O=example inc

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

b. A prompt displays in order to save the CSR to a file on the local machine.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Identity Certificate Request

To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.

You will then need to install the certificate that is returned from the CA by clicking the Install button in the Identity Certificates panel.

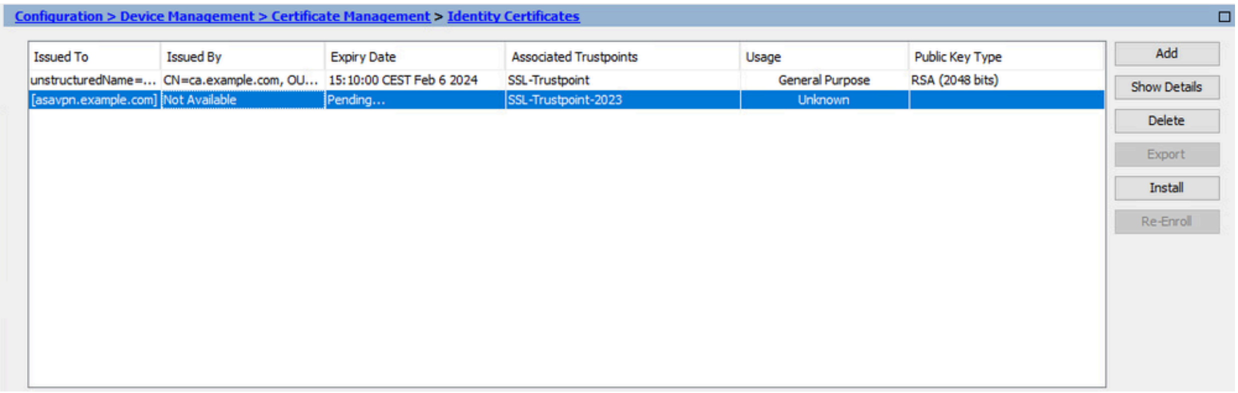
Save CSR to File: C:\Users\cisco.DESKTOP-R2CH8G5\Docun

□ Enable CA flag in basic constraints extension

Click **Browse**. Choose a **location** in which to save the CSR, and **save** the file with the .txt extension.

Note: When the file is saved with a .txt extension, the PKCS#10 request can be opened and viewed with a text editor (such as Notepad).

c. Now the new trustpoint is displayed in a Pending state.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
[asavpn.example.com]	Not Available	Pending...	SSL-Trustpoint-2023	Unknown	

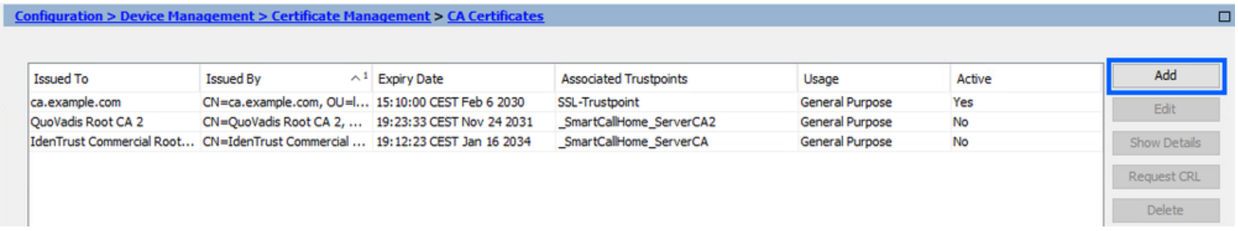
Install the Identity Certificate in PEM Format with ASDM

The installation steps assume that the CA signed the CSR, and provided a PEM encoded (.pem, .cer, .crt) new Identity Certificate and CA certificate bundle.

1. **Install CA Certificate that Signed the CSR**

   The CA certificate that signed the Identity Certificate can be installed in the Trustpoint created for Identity Certificate. If the Identity Certificate is signed by intermediate CA, then this CA certificate can be installed in the Identity Certificate Trustpoint. All the CA certificates upstream in the hierarchy and can be installed in separate CA Trustpoints.

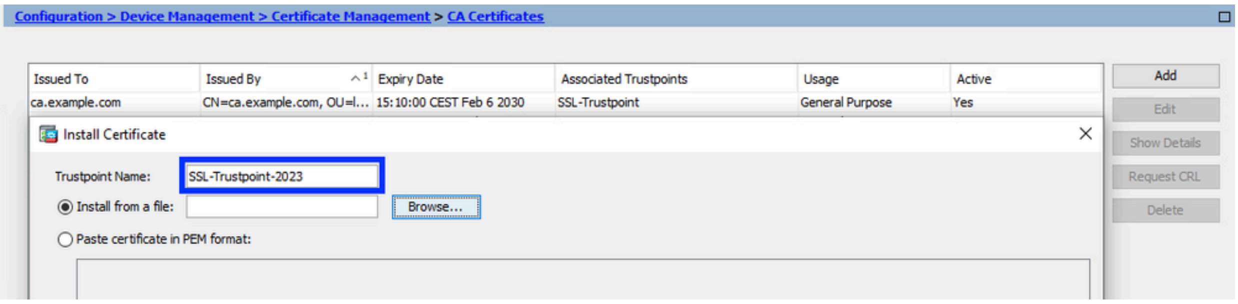
   a. Navigate to **Configuration > Device Management >Certificate Management >**, and choose **CA Certificates**. Click **Add**.



Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
ca.example.com	CN=ca.example.com, OU=l...	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No

   b. Enter the **Trustpoint name** and choose **Install From File**, click **Browse button**, and choose the **intermediate certificate**. Alternatively, paste the **PEM encoded CA certificate** from a text file into the text field.



Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
ca.example.com	CN=ca.example.com, OU=l...	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes

Install Certificate

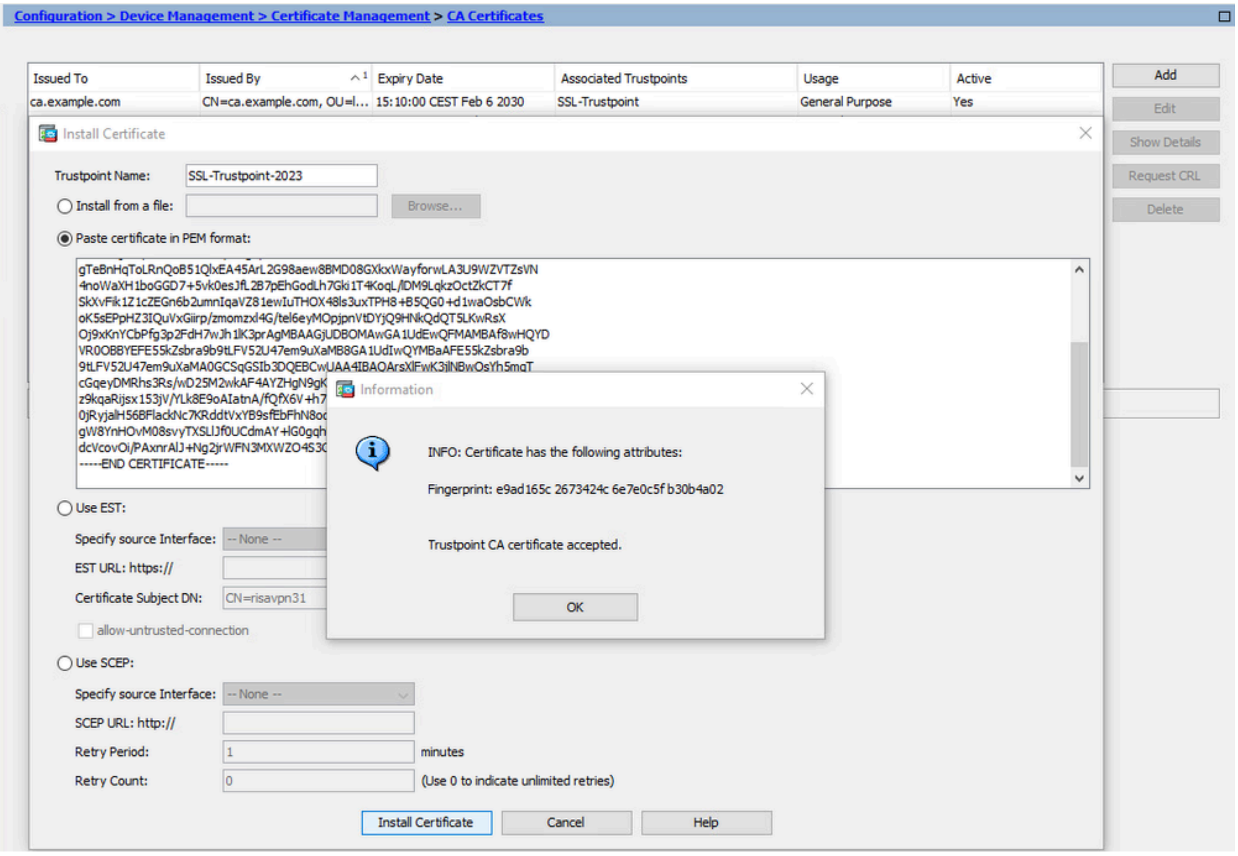
Trustpoint Name: SSL-Trustpoint-2023

● Install from a file:

○ Paste certificate in PEM format:

Note: Install the intermediate certificate with the same trust point name as Identity Certificate trust point name, if Identity Certificate is signed by intermediate CA certificate.

   c. Click **Install Certificate**.



Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
ca.example.com	CN=ca.example.com, OU=l...	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes

Install Certificate

Trustpoint Name: SSL-Trustpoint-2023

○ Install from a file:

● Paste certificate in PEM format:

```
gTeBnHqToLRnQoB51QlxEA45ArL2G98aew8BMD08GXkxWayforwLA3U9WZVTZsVN
4noWaXH1boGGD7+5vk0esJfL2B7pEhGodLh7Gki1T4KoqL/lDM9LqkzOctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTHOX48ls3uxTPH8+B5QG0+d1waOsbCWk
oK5sEPpHZ3IQuVxGiirp/zmomzxl4G/tel6eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh1lK3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAf8wHQYD
VR0OBBYEFE55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMA0GCSqGSIb3DQEBCwUAA4IBAQArsXlFwK3jlNBwOsYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK
z9kqaRijsx153jV/YLk8E9oAIatnA/fQfX6V+h7
0jRyjalH56BFlackNc7KRddtVxYB9sfEbFhN8oc
gW8YnHOvM08svyTXSLlJf0UCdmAY+lG0gqh
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3C
-----END CERTIFICATE-----
```

○ Use EST:

Specify source Interface: -- None --

EST URL: https://

Certificate Subject DN: CN=risavpn31

□ allow-untrusted-connection

○ Use SCEP:

Specify source Interface: -- None --

SCEP URL: http://

Retry Period: 1 minutes

Retry Count: 0 (Use 0 to indicate unlimited retries)

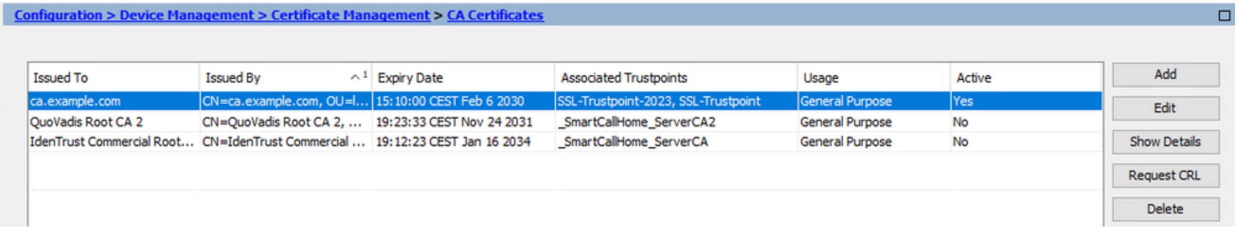
Information

INFO: Certificate has the following attributes:

Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02

Trustpoint CA certificate accepted.

In the example, the new certificate is signed with the same CA certificate as the old one. The same CA certificate is associated with two Trustpoints now.

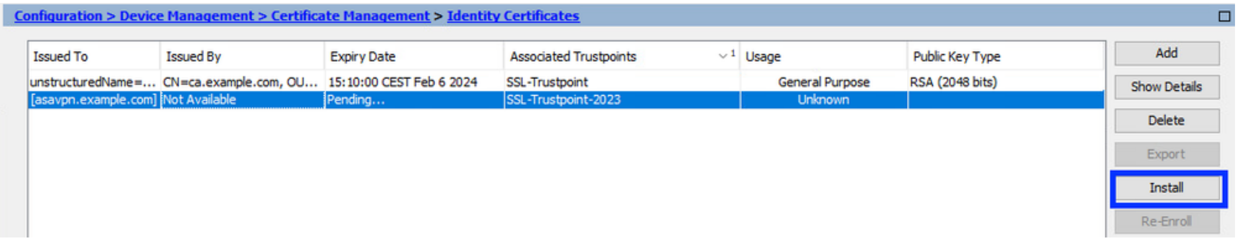


Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
ca.example.com	CN=ca.example.com, OU=l...	15:10:00 CEST Feb 6 2030	SSL-Trustpoint-2023, SSL-Trustpoint	General Purpose	Yes
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No

2. **Install Identity Certificate**

   a. Choose the **Identity Certificate** created previously with the CSR generation. Click **Install**.

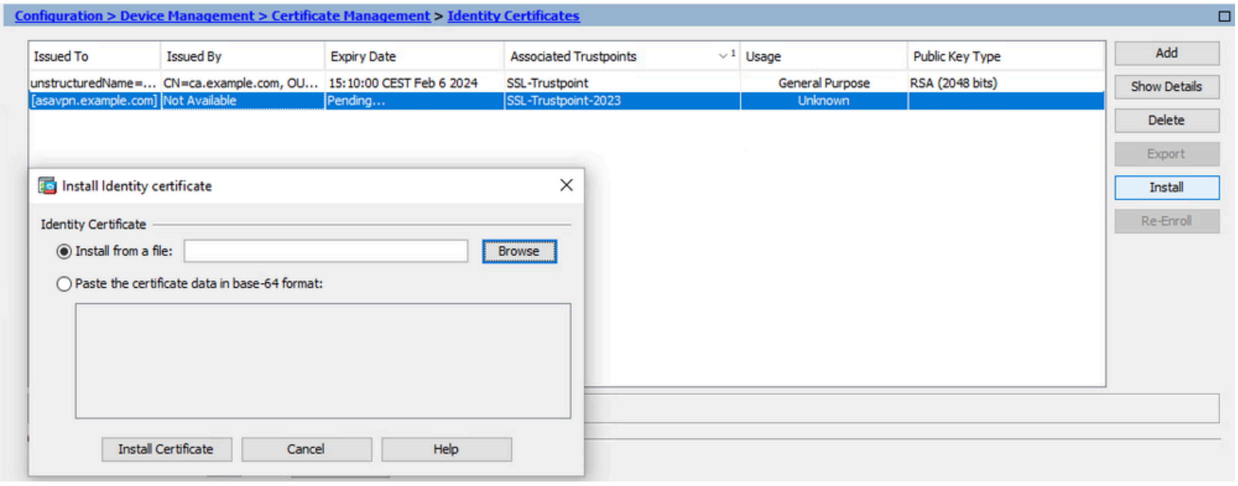


Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
[asavpn.example.com]	Not Available	Pending...	SSL-Trustpoint-2023	Unknown	

Note: The Identity Certificate can have **Issued By** field as **Not available**, and the **Expiry Date** field as **Pending**.

   b. Choose a **file** that contains the PEM encoded Identity Certificate received from the CA, or open the **PEM encoded certificate** in a text editor, and copy and paste the **Identity Certificate** provided by the CA into the **text** field.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
[asavpn.example.com]	Not Available	Pending...	SSL-Trustpoint-2023	Unknown	

Install Identity certificate

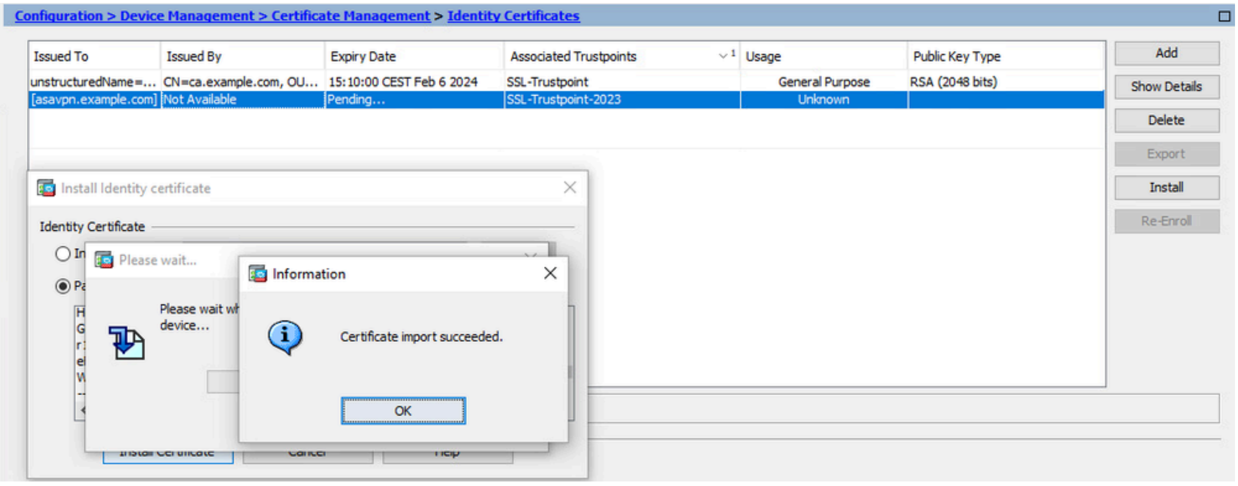
Identity Certificate

● Install from a file:

○ Paste the certificate data in base-64 format:

Note: Identity certificate can be in .pem, .cer, .crt format to install.

c. Click **Install Certificate**.

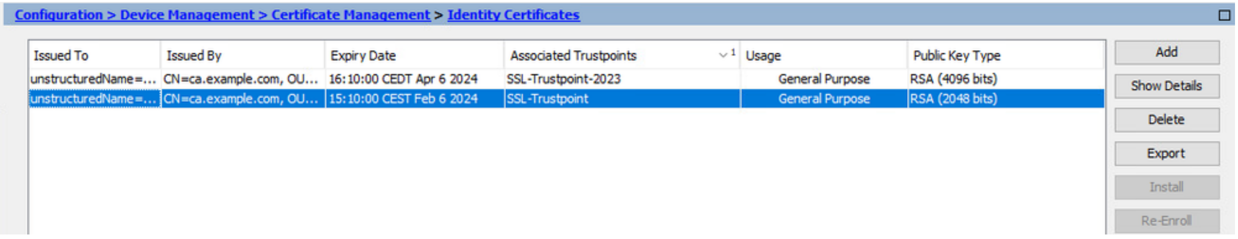


Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
[asavpn.example.com]	Not Available	Pending...	SSL-Trustpoint-2023	Unknown	

Certificate import succeeded.

After the installation, there are old and new Identity Certificates present.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023	General Purpose	RSA (4096 bits)
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

3. Bind the New Certificate to Interface with ASDM

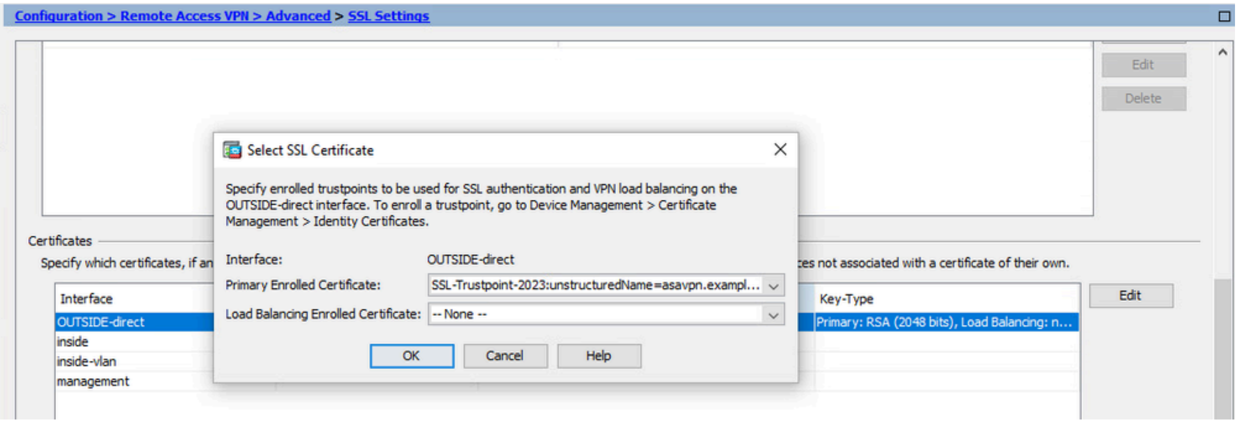
The ASA needs to be configured to use the new Identity Certificate for WebVPN sessions that terminate on the interface specified.

a. Navigate to **Configuration** > **Remote Access VPN** > **Advanced** > **SSL Settings**.

b. Under Certificates, choose the **interface** that is used to terminate WebVPN sessions. In this example, the outside interface is used.

Click **Edit**.

c. In the **Certificate** drop-down list, choose the **newly installed certificate**.


Configuration > Remote Access VPN > Advanced > SSL Settings

Select SSL Certificate

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate Management > Identity Certificates.

Interface: OUTSIDE-direct

Primary Enrolled Certificate: SSL-Trustpoint-2023:unstructuredName=asavpn.exampl...

Load Balancing Enrolled Certificate: -- None --

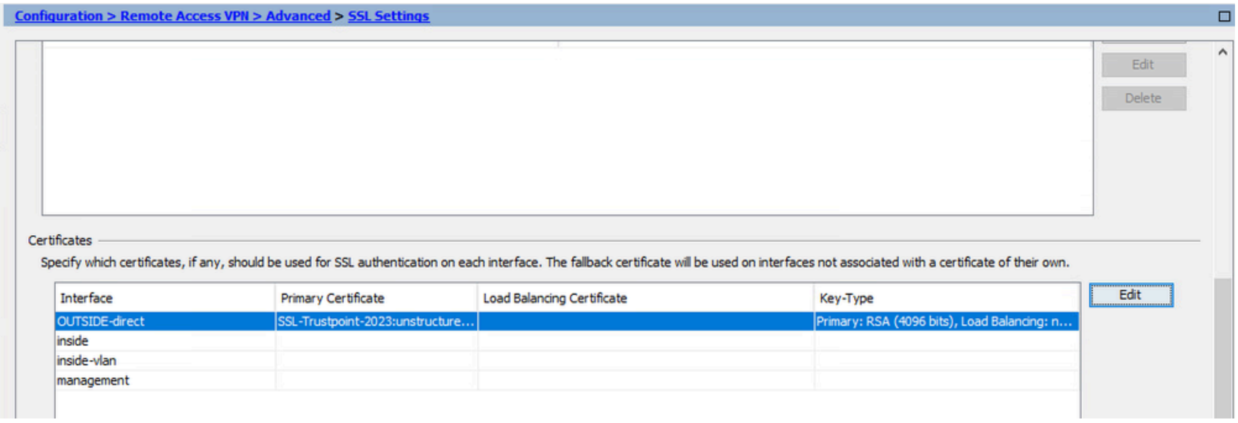
Certificates

Specify which certificates, if an ... es not associated with a certificate of their own.

Interface	Key-Type
OUTSIDE-direct	Primary: RSA (2048 bits), Load Balancing: n...
inside	
inside-vlan	
management	

d. Click **OK**.

e. Click **Apply**. Now the new Identity Certificate is in use.


Configuration > Remote Access VPN > Advanced > SSL Settings

Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Primary Certificate	Load Balancing Certificate	Key-Type
OUTSIDE-direct	SSL-Trustpoint-2023:unstructure...		Primary: RSA (4096 bits), Load Balancing: n...
inside			
inside-vlan			
management			

Renew a Certificate Enrolled with PKCS12 File with ASDM

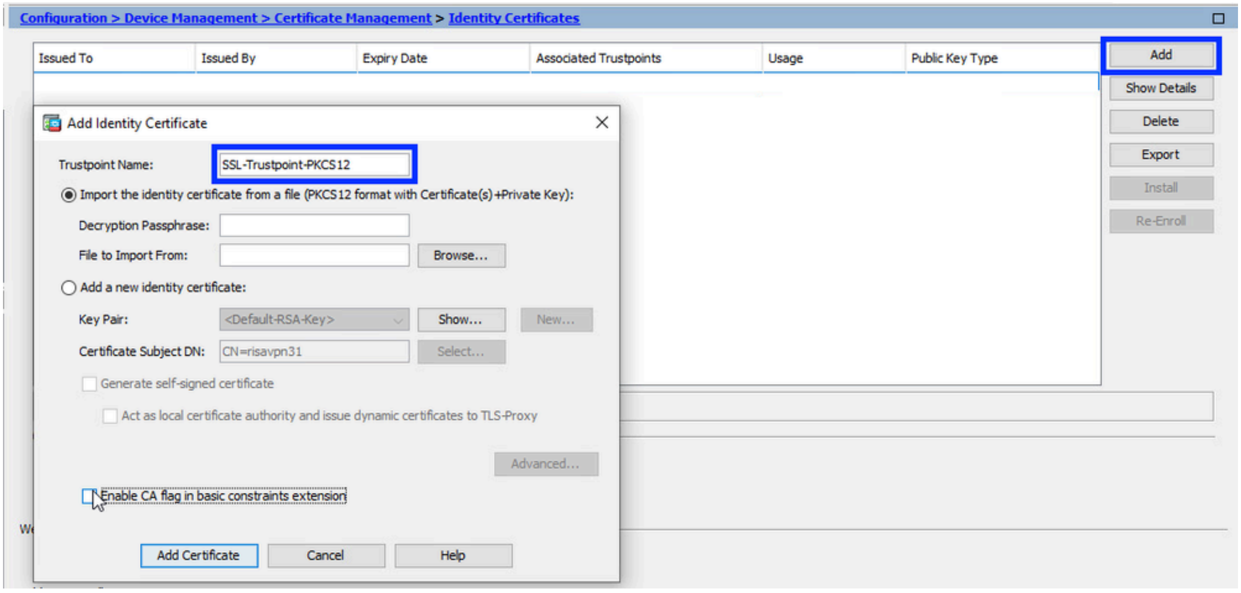
Certificate renewal of PKCS12 enrolled certificate requires you to create and enroll a new Trustpoint. It needs to have a different name (for example, old name with enroll year suffix).

PKCS12 file (.p12 or .pfx format) contains Identity Certificate, Key Pair, and CA certificate(s). It is created by the CA, for example, in case of wildcard certificate, or exported from a different device. It is a binary file, and cannot be viewed with text editor.

1. Install the Renewed Identity Certificate and CA Certificates from a PKCS12 File

The Identity Certificate, CA certificate(s) and Key Pair needs to be bundled into a single PKCS12 file.

a. Navigate to **Configuration > Device Management > Certificate Management**, and choose **Identity Certificates**.
b. Click **Add**.
c. Specify a new **Trustpoint Name**.



Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

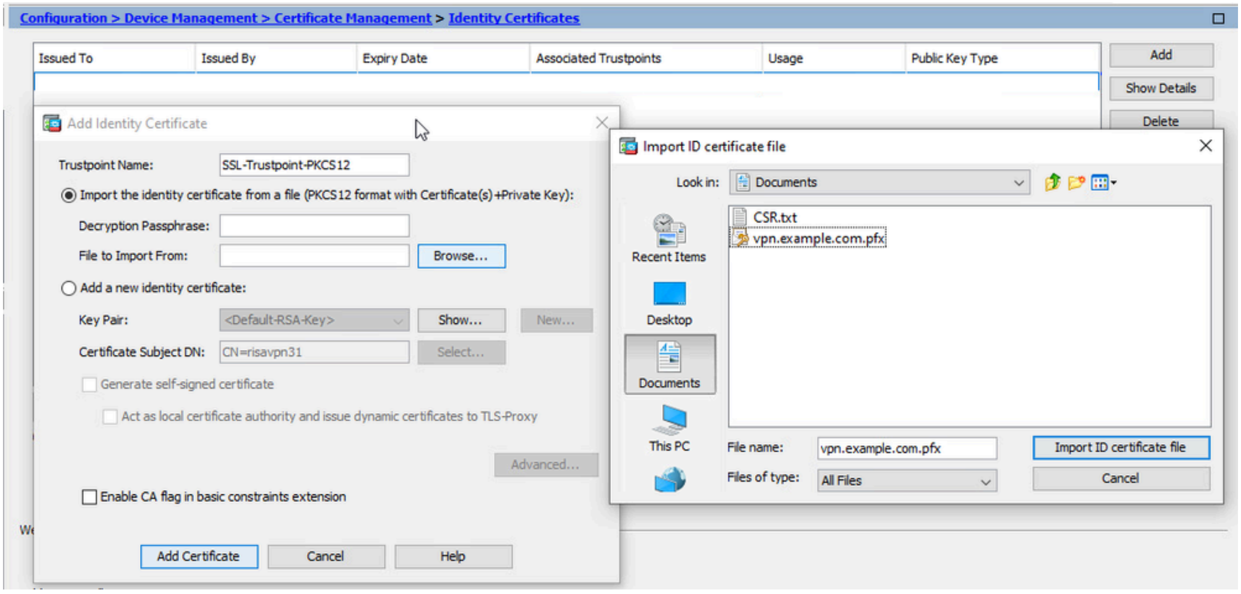
Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

d. Click the **Import The Identity Certificate** from a File radio button.



Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

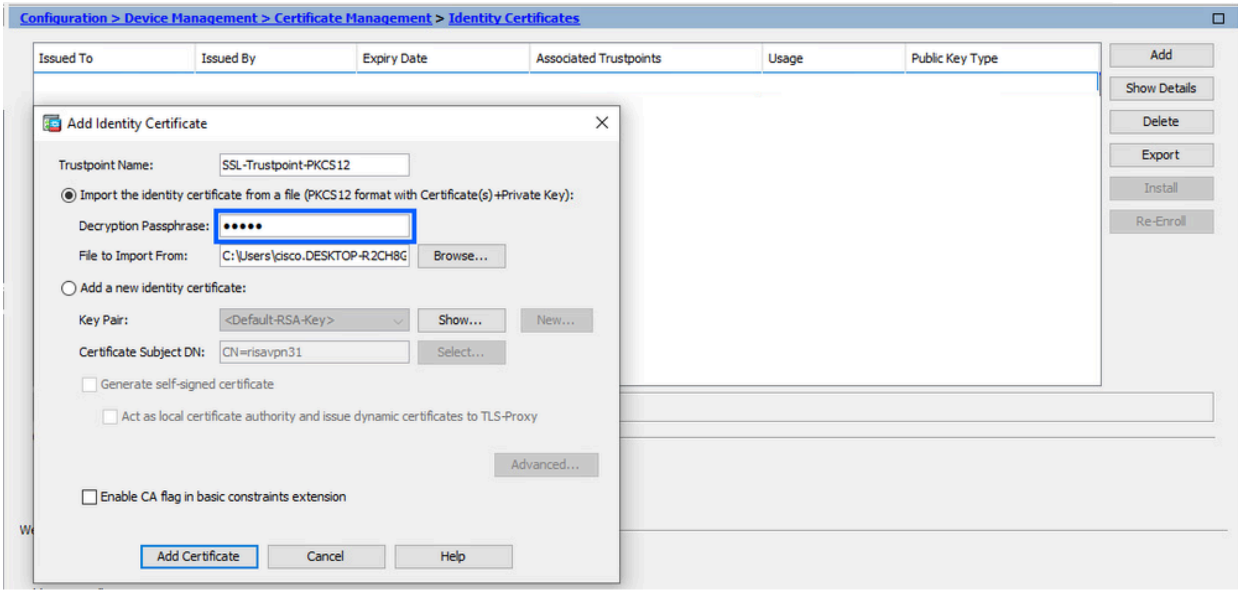
□ Enable CA flag in basic constraints extension

CSR.txt
vpn.example.com.pfx

File name: vpn.example.com.pfx

Files of type: All Files

e. Enter the **passphrase** used to create the PKCS12 file.



Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase: •••••

File to Import From: C:\Users\cisco.DESKTOP-R2CH8G

○ Add a new identity certificate:

Key Pair: <Default-RSA-Key>

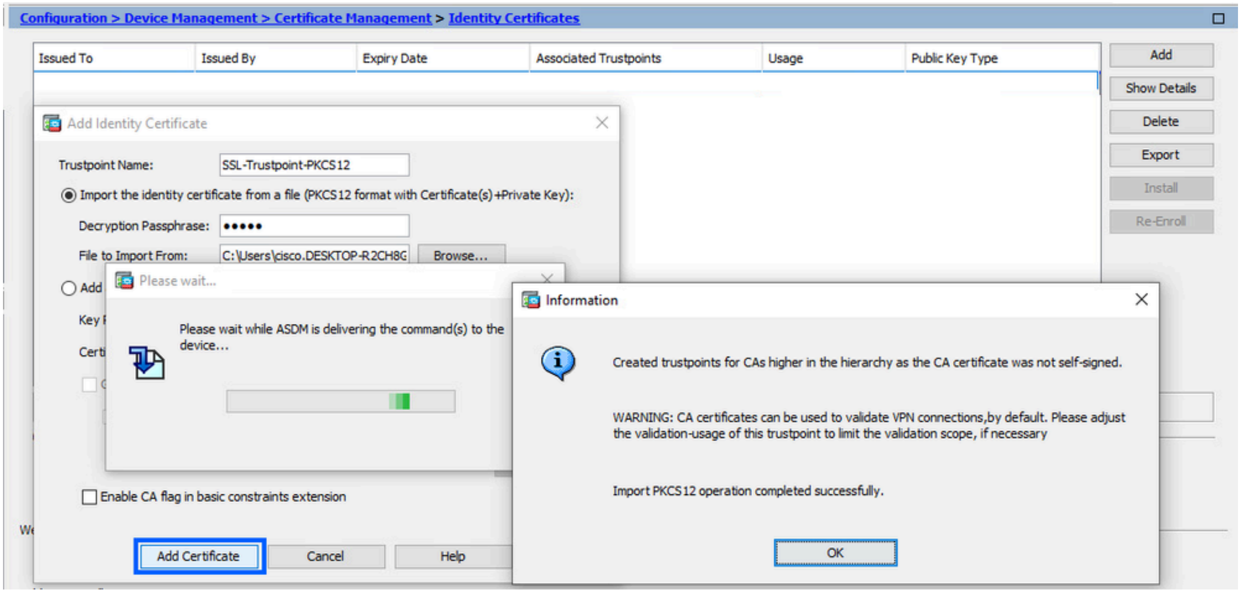
Certificate Subject DN: CN=risavpn31

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

□ Enable CA flag in basic constraints extension

f. Click **Add Certificate**.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type

Add Identity Certificate

Trustpoint Name: SSL-Trustpoint-PKCS12

● Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase: •••••

File to Import From: C:\Users\cisco.DESKTOP-R2CH8G

○ Add

□ Enable CA flag in basic constraints extension

Please wait...

Please wait while ASDM is delivering the command(s) to the device...

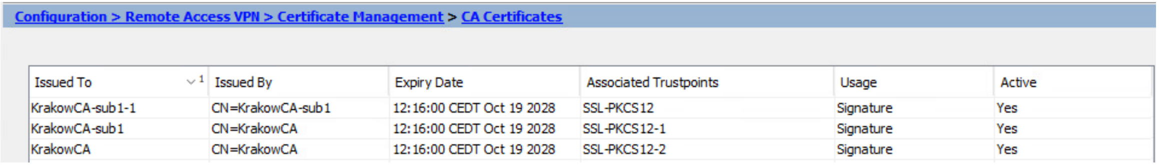
Information

Created trustpoints for CAs higher in the hierarchy as the CA certificate was not self-signed.

WARNING: CA certificates can be used to validate VPN connections,by default. Please adjust the validation-usage of this trustpoint to limit the validation scope, if necessary

Import PKCS12 operation completed successfully.

Note: When a PKCS12 with CAs certificates chain is imported the ASDM creates the upstream CAs trustpoints automatically with names with added -number suffix.



Configuration > Remote Access VPN > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

2. Bind the New Certificate to Interface with ASDM

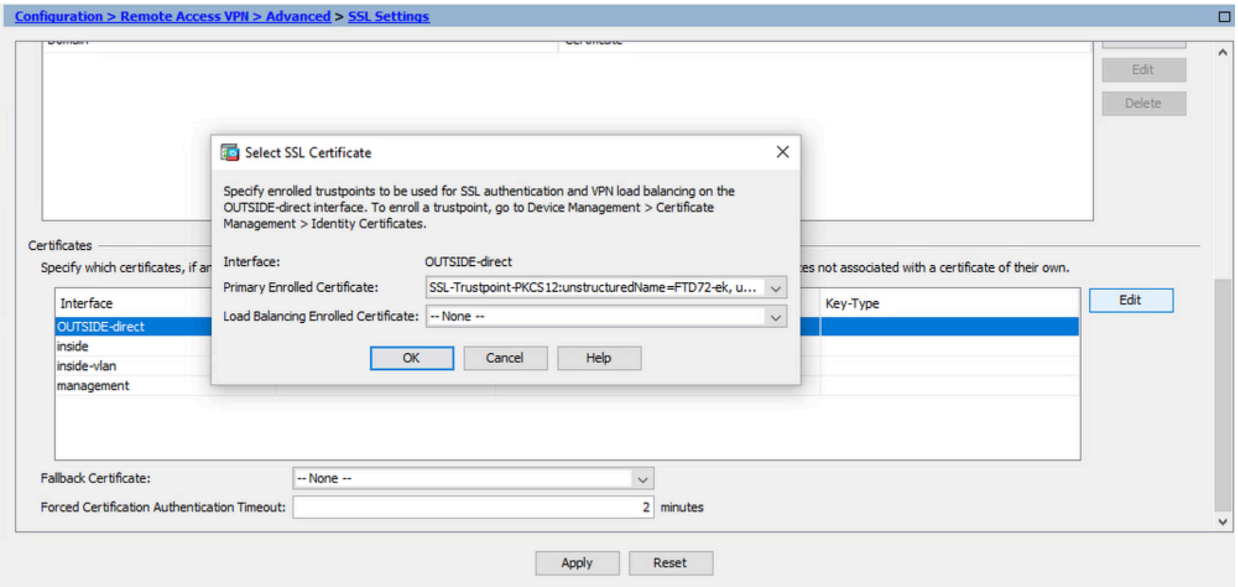
The ASA needs to be configured to use the new Identity Certificate for WebVPN sessions that terminate on the interface specified.

a. Navigate to **Configuration** > **Remote Access VPN** > **Advanced** > **SSL Settings**.

b. Under Certificates, choose the **interface** that is used to terminate WebVPN sessions. In this example, the outside interface is used.

Click **Edit**.

c. In the Certificate drop-down list, choose the **newly installed certificate**.



Configuration > Remote Access VPN > Advanced > SSL Settings

Select SSL Certificate

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate Management > Identity Certificates.

Interface: OUTSIDE-direct

Primary Enrolled Certificate: SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u...

Load Balancing Enrolled Certificate: -- None --

Certificates

Specify which certificates, if ar... ...es not associated with a certificate of their own.

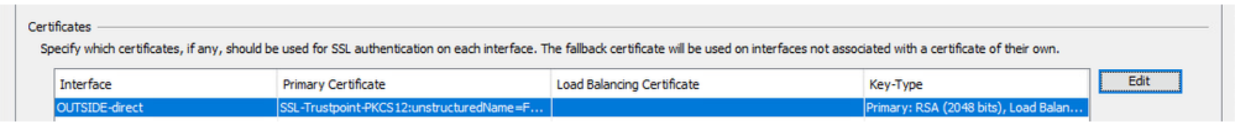
Interface	Key-Type
OUTSIDE-direct	
inside	
inside-vlan	
management	

Fallback Certificate: -- None --

Forced Certification Authentication Timeout: 2 minutes

d. Click **OK**.

e. Click **Apply**.



Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Primary Certificate	Load Balancing Certificate	Key-Type
OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName=F...		Primary: RSA (2048 bits), Load Balan...

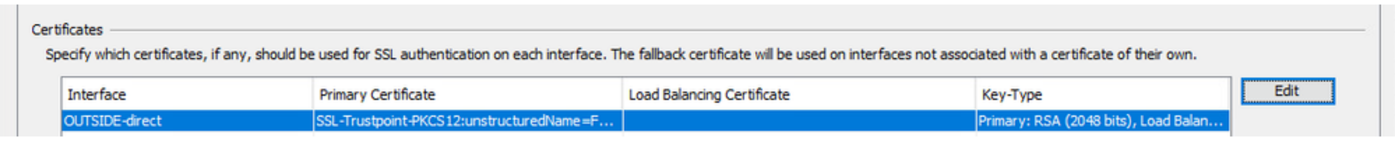
Now the new Identity Certificate is in use.

Verify

Use these steps in order to verify successful installation of the third-party Vendor Certificate and use for SSL VPN connections.

View Installed Certificates via ASDM

1. Navigate to **Configuration > Remote Access VPN > Certificate Management**, and choose **Identity Certificates**.
2. The Identity Certificate issued by the third-party vendor can appear.



Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Primary Certificate	Load Balancing Certificate	Key-Type
OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName=F...		Primary: RSA (2048 bits), Load Balan...

Troubleshoot

This debug command is to be collected on the CLI in the case of an SSL Certificate Installation failure.

- **debug crypto ca 14**

Frequently Asked Questions

Q. What is a PKCS12?
A. In cryptography, PKCS12 defines an archive file format created to store many cryptography objects as a single file. It is commonly used to bundle a private key with its X.509 certificate or to bundle all the members of a chain of trust.

Q. What is a CSR?
A. In public key infrastructure (PKI) systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a registration authority of the public key infrastructure in order to apply for a digital Identity Certificate. It usually contains the public key for which the certificate can be issued, information that is used to identify the signed certificate (such as a domain name in Subject) and integrity protection (for example, a digital signature).

Q. Where is the password of the PKCS12?
A. When certificates and Key Pairs are exported to a PKCS12 file, the password is given in the export command. For importing a pkcs12 file the password needs to be delivered by the owner the CA Server or person that exported the PKCS12 from another device.

Q. What is the difference between the root and the identity?
A. In cryptography and computer security, a root certificate is a public key certificate that identifies a root certificate authority (CA). Root certificates are self-signed (and it is possible for a certificate to have multiple trust paths, say, if the certificate was issued by a root that was cross-signed) and form the basis of an X.509-based public key infrastructure (PKI). A public key certificate, also known as a digital certificate or Identity Certificate, is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the signature is valid, and the software that examins the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject.

Q. I installed the cert, why does it not work?
A. This could be due to many reasons, for example:

1. The certificate and trustpoint are configured, but they have not been bound to the process that uses it. For example, the trustpoint to be used is not binded to the outside interface which terminates Anyconnect clients.

2. A PKCS12 file is installed, but gives errors due to the intermediate CA certificate missing in the PKCS12 file. The clients that have the intermediate CA certificate as trusted, but do not have root CA certificate as trusted, are not able to verify the whole certificate chain and report the server Identity Certificate as not trusted.

3. A certificate populated with incorrect attributes can cause installation failure, or client side errors. For example, certain attributes are encoded using the wrong format. Another reason is that the Identity Certificate is missing Subject Alternative Name (SAN), or the domain name used to access the server is not present as a SAN.

Q. Does a installation of a new cert require a maintenance window or causes downtime?
A. Installation of a new certificate (identity or CA) is not intrusive and does not cause downtime or requre a maintenance window. To enable a new certificate to be used for a service that exists is a change and require a change request / maintenance window.

Q. Can adding or changing a certificate disconnect the connected users?
A. No, the users that are currently connected stay connected. The certificate is used at connection establishment. Once the users reconnect, the new certificate is used.

Q. How can I create a CSR with a wildcard? Or a Subject Alternative Name (SAN)?
A. Currently, the ASA/FTD cannot create a CSR with wildcard; however, this process can be done with OpenSSL. In order to generate the CSR and ID key, you can run the commands:

```
openssl genrsa -out id.key 2048

openssl req -out id.csr -key id.key -new
```

When a trustpoint is configured with Fully Qualified Domain Name (FQDN) attribute, the CSR created by ASA/FTD contains the SAN with that value. More SAN attributes can be added by the CA when it signs the CSR, or the CSR can be created with OpenSSL

Q. Does certificate replacement take effect immediately?

A. The new server Identity Certificate is used only for the new connections. The new certificate is ready to be used immediately after the change, but is actually used with new connections.

Q. How can I check if the installation worked?
A. The CLI command to verify: **show crypto ca cert <trustpointname>**

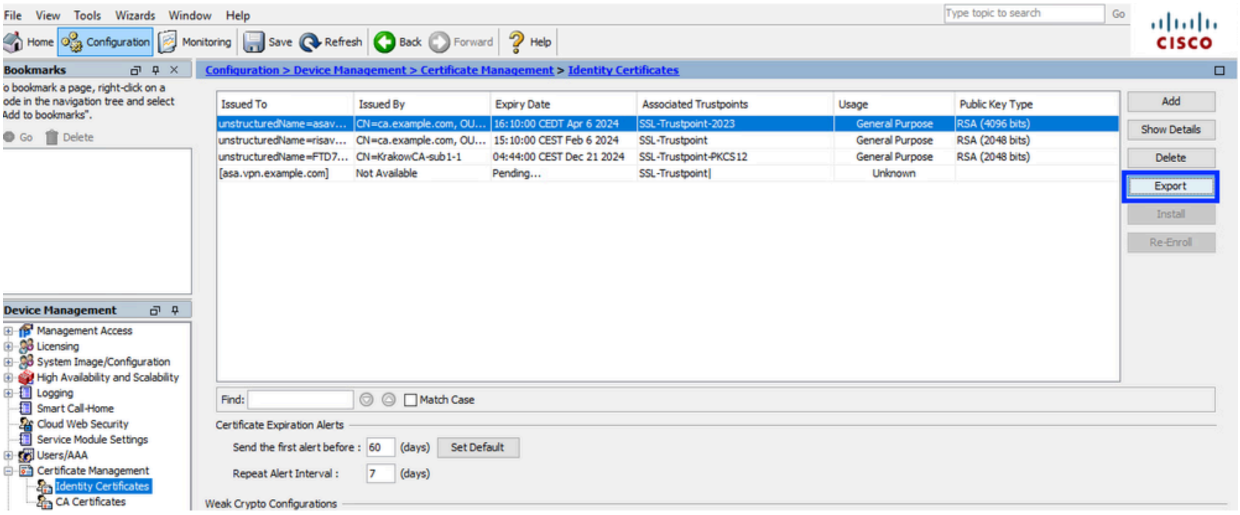
Q. How to generate PKCS12 from The Identity Certificate, CA certificate, and private key?
A. PKCS12 can be created with OpenSSL, with the command:

```
openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt
```

Q. How to export a certificate to install it in a new ASA?
A.

- With CLI: use the command: **crypto ca export <trustpointname> pkcs12 <password>**
- With ASDM:

a. Navigate to **Configuration > Device Management > Certificate Management > Identity Certificates** and choose the **Identity Certificate**. Click **Export**.



o bookmark a page, right-click on a ode in the navigation tree and select Add to bookmarks".

Configuration > Device Management > Certificate Management > Identity Certificates

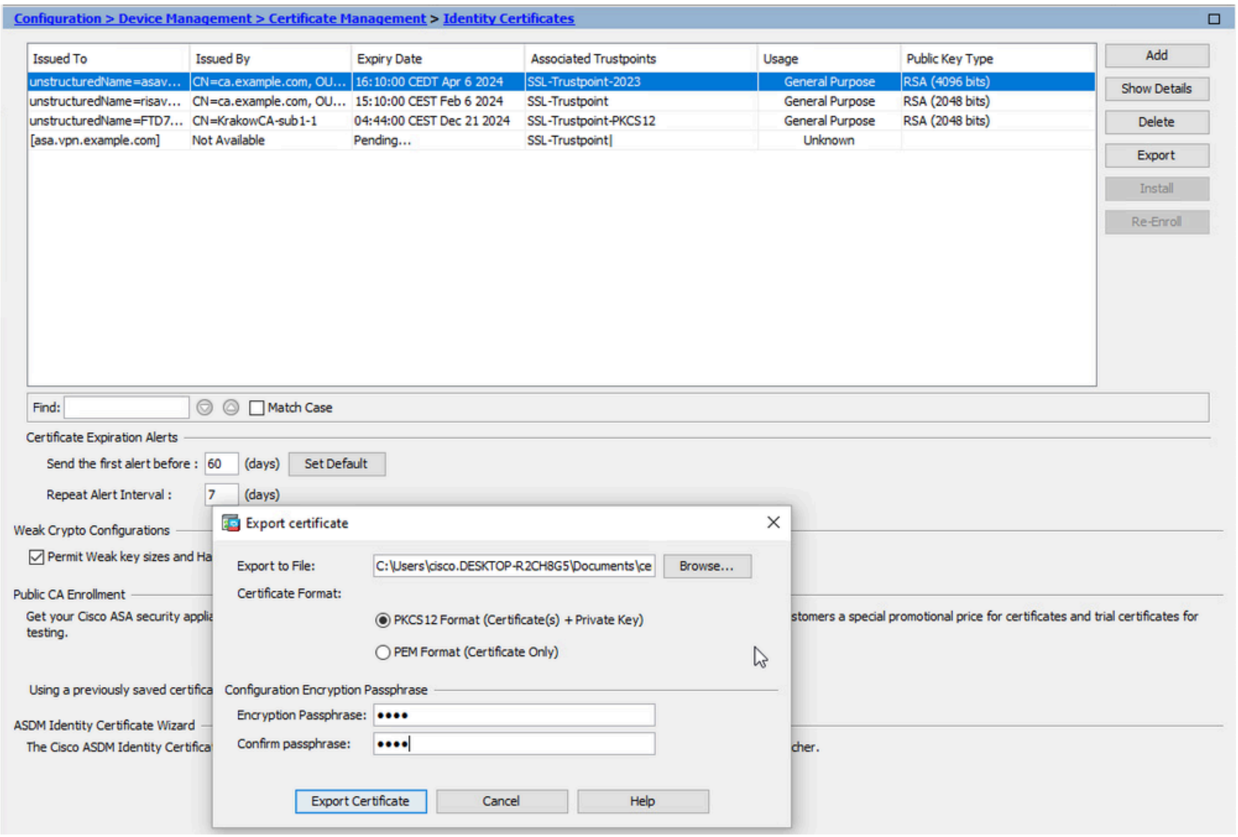
Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=asav...	CN=ca.example.com, OU...	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023	General Purpose	RSA (4096 bits)
unstructuredName=risav...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
unstructuredName=FTD7...	CN=KrakowCA-sub1-1	04:44:00 CEST Dec 21 2024	SSL-Trustpoint-PKCS12	General Purpose	RSA (2048 bits)
[asa.vpn.example.com]	Not Available	Pending...	SSL-Trustpoint|	Unknown	

Certificate Expiration Alerts

Send the first alert before : 60 (days)

Repeat Alert Interval : 7 (days)

b. Choose where to export the file, specify the export password, click **Export Certificate**.



Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=asav...	CN=ca.example.com, OU...	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023	General Purpose	RSA (4096 bits)
unstructuredName=risav...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
unstructuredName=FTD7...	CN=KrakowCA-sub1-1	04:44:00 CEST Dec 21 2024	SSL-Trustpoint-PKCS12	General Purpose	RSA (2048 bits)
[asa.vpn.example.com]	Not Available	Pending...	SSL-Trustpoint|	Unknown	

Find: □ Match Case

Certificate Expiration Alerts

Send the first alert before : 60 (days)

Repeat Alert Interval : 7 (days)

Weak Crypto Configurations

☑ Permit Weak key sizes and Ha

Public CA Enrollment

Get your Cisco ASA security applia ... stomers a special promotional price for certificates and trial certificates for testing.

Using a previously saved certifica

ASDM Identity Certificate Wizard

The Cisco ASDM Identity Certifica ... cher.

Export certificate

Export to File: C:\Users\cisco.DESKTOP-R2CH8G5\Documents\ce

Certificate Format:

● PKCS12 Format (Certificate(s) + Private Key)

○ PEM Format (Certificate Only)

Configuration Encryption Passphrase

Encryption Passphrase: ••••

Confirm passphrase: ••••

The exported certificate can be on the computer disk. Please put the passphrase in a safe place, the file is useless without it.

Q. If ECDSA keys are used, is the SSL certificate generation process different?
A. The only difference in configuration is the keypair generation step, where an ECDSA keypair can be generated instead of an RSA keypair. The rest of the steps remain the same.

Q. Is it always required to generate a new Key Pair?
A.The Key Pair generation step is optional. Existing Key Pair can be used, or in case of PKCS12 the Key Pair is imported with the certificate. Please see the Select the Key Pair Name section for the respective enrollment / re-enrollment type.

Q. Is it safe to generate a new Key Pair for a new Identity Certificate?
A. The process is safe as long as a new Key Pair name is used. In such a case, the old Key Pairs are not changed.

Q. Is it required to generate the key again when a firewall is replaced (like RMA)?
A. The new firewall by design does not have Key Pairs present on the old firewall.
The backup of running-configuration does not contain the Key Pairs. The full backup done with ASDM can contain the Key Pairs.
The Identity Certificates can be exported from an ASA with ASDM or CLI, before it fails. In case of failover pair, the certificates and Key Pairs are synchronised to a standby unit with **write standby** command. In case one node of failover pair is replaced, it is enough to configure the basic failover and push the config to the new device.
In case a Key Pair is lost with the device and there is no backup, a new certificate needs to be signed with Key Pair present on the new device.