Install and Renew Certificates on ASA Managed by ASDM

Contents

Frequently Asked Questions

Introduction Prerequisites Requirements Components Used **Background Information 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 (FODN) 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**

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 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 synchronise 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.

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:

- 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.
- Use PKCS12 file obtained from a CA, or exported from a different device. The PKCS12 file contains

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.



b. Click Add.

c. Define a trustpoint name.

ssued To	Issued By	Expiry Date	Associated Trustpoints	^1	Usage	Public Key Type	Add
🔄 Add Identity C	Certificate					×	Show Deta
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the ide	entity certificate from a file (PKCS12 format with Certificate(s)+Private Key):				Export
Decryption Pa	assphrase:						Install
File to Import	From:	Browse					Re-Enrol
Add a new ide	entity certificate:						0
Key Pair:	<default-rsa+< td=""><td>Key> v Show</td><td>New</td><td></td><td></td><td></td><td></td></default-rsa+<>	Key> v Show	New				
Certificate Su	bject DN: CN=asavpn.exa	ample.com Select					
Generate	self-signed certificate						
Act as	s local certificate authority ar	nd issue dynamic certificates to "	TLS-Proxy				
			Advanced				
Enable C/	A flag in basic constraints ext	tension					

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.

Issued To	Issued By	Expiry Date	Associated Trust	tpoints	Usage	Public Key Type	Add
🔄 Add Identity (Certificate			×	General Purpose	RSA (4096 bits)	Show Deta
-				-	General Purpose	RSA (2048 bits)	Delete
Trustpoint Name	SSL-Trustpoint						Export
 Import the id 	entity certificate from a file	(PKCS12 format with Certificate	(s)+Private Key):				Coport
Decryption Pa	assphrase:						Install
File to Import	From:	Browse.					Re-Enro
Add a new id	entity certificate:						
Key Pair:	<default-rsa-< td=""><td>Key> v Show</td><td>. New</td><td></td><td></td><td></td><td></td></default-rsa-<>	Key> v Show	. New				
Certificate Su	bject DN: CN=asavpn.ex	cample.com Select.	•				
Generate	self-signed certificate						
Act a	s local certificate authority a	and issue dynamic certificates to	TLS-Proxy				
			Advanced				
Enable C	A flag in basic constraints ex	rtension					

- 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.

ssued to	Issued By	Expiry Date	Associated Trustpoir	nts	Usage	Public Key Type	Add
🔁 Add Identity Certifi	cate			×	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)	Show Detai
Trustpoint Name:	SSL-Trustpoint						Delete
🔿 Impor 📑 Add K	ey Pair		×				Export
Decry			DDCA				Install
File to	e. Onan	U ECDSA U E	LUUSA				Re-Enrol
Add a Name:	O Use default key	pair name					
Key Pa	Enter new key	pair name: SSL-Keypair					
Certifi Size:	2048		N				
Ge Usage:	General purpose	e 🔿 Special	63				
L							
	Generate Now	Cancel	Help				
E Fr							

3. Choose the Key Pair Name

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

Add Identity Certificate			Associated musipolints		Usage	Public Key Type	Auu
			×		General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)	Show Detai
Trustpoint Name:	SL-Trustpoint						Delete
Import the identity certification	ate from a file (PKCS12	format with Certificate(s)+	Private Key):				Export
Decryption Passphrase:							Install
File to Import From:		Browse					Re-Enroll
Add a new identity certification	ate:						
Key Pair:	SSL-Keypair	Show	New				
Certificate Subject DN:	CN=asavpn.example.c	om Select					
Generate self-signed of	ertificate						
Act as local certifica	ate authority and issue	dynamic certificates to TLS	-Proxy	-			
		-	Advanced				
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.

sued To	Issued By	Expiry Date	Associated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Cer	tificate					×	Show Detai
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the iden	tity certificate from a file (P	KCS12 format with Certificate(s))+Private Key):				Export
Decryption Pass	sphrase:						Install
File to Import Fr	rom:	Browse					Re-Enrol
Add a new iden	tity certificate:						
Key Pair:	SSL-Keypair	~ Show	New				
Certificate Subje	ect DN: CN=asavpn.exa	mple.com Select					
Generate se	elf-signed certificate						
Act as lo	ocal certificate authority an	d issue dynamic certificates to TI	LS-Proxy				
			Advanced				
Enable CA f	lan in basic constraints exte	ension	Auvanceu				

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

sued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
Add Identity Certificate	e				×	Show Detail
Trustpoint Name:	SSL-Trustpoint					Delete
O Import the identity ce	Cartificate Subjec	* DN		×		Export
Decryption Passphrase	Certificate Subjec			^		Install
File to Import From:			Attribute Value			Re-Enroll
Add a new identity cer Key Pair: Certificate Subject DN Generate self-sign Act as local cer	DN Attribute to t Attribute: Cor Value: asa	e Added nmon Name (CN) v .vpn.example.com	Add>> Delete			
Enable CA flag in t		ОК	Cancel Help			

Issued To	Issued By	Expiry Date	Assoc	ciated Trustpoints	^¹ Usage		Public Key Type	Add
Add Identity Certificat	e						×	Show Details
Trustpoint Name:	SSL-Trustpoint							Delete
Import the identity ce						~		Export
Decryption Passphras	Certificate Subject	t DN				^		Install
File to Import From:				Attribute	Value			Re-Enroll
Add a new identity ce	DN Attribute to	e Added		Common Name (CN)	asa.vpn.exam			
Key Pair:	Attribute: Co	untry (C) 🗸 🗸	Add>>					
Certificate Subject DN	Value: Cor Dep	nmon Name (CN) partment (OU)	Delete					
Generate self-sign	Cor	npany Name (O)						
Act as local ce	Sta	te (St)						
	Em	ail Address (EA)						
		ОК	Cancel	Help				
Enable CA flag in I						_		
		Add Carlifornia	Canad	ttala	-			

Attribute	Description
CN	The name through which the firewall can be accessed (usually the fully-qualified

Attribute	Description
	domain name, for example, vpn.example.com).
OU	The name of your department within the organization
0	The legally registered name of your organization/company
С	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**.

Issued To	Issued By	Expiry Date	Associated Trustpoints	^1	Usage	Public Key Type	Add
🛓 Add Identity Certi	ficate	· · ·				×	Show Detai
Trustpoint Name:	SSL-Trustpoint						Delete
Import the identit	ty certificate from a file (P	KCS12 format with Certificate(s)+	Private Kev):				Export
Decryption Passo	hrase:						Install
File to Import Fro	m:	Browse					Re-Enroll
Add a new identities	ty certificate:						
Key Pair:	SSL-Keypair	✓ Show	New				
Certificate Subject	ct DN: CN=asa.vpn.exa	ample.com Select]				
Generate self	f-signed certificate						
Act as loc	al certificate authority an	d issue dynamic certificates to TLS	-Proxy				
			Advanced			_	
Enable CA fla	n in basic constraints exte	ension	Advanced				
		Add Cast Casts	Count	-			

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

Issued To	ISSUNT Du Evolution Data Associated Tevatasista Al Hasso	Public Key Type	Add
Add Identity Cer	Advanced Options K Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.	×	Show Detail
Trustpoint Name:	S Certificate Parameters Enrollment Mode SCEP Challenge Password		Delete
O Import the iden	bity certifica		Export
Decryption Pass	phrase: FQDN: asavpn.example.com		Install
File to Import Fr	om: E-mail:		Re-Enrol
Add a new iden	IP Address:		
Key Pair:	Include serial number of the device		
Certificate Subj	ect DN: C		
Generate se	lf-signed ce		
Act as k	cal certifica		
Enable CA f	lag in basic		

5. Generate and Save the CSR

a. Click Add Certificate.

Issued To	Issued By	Expiry D	ate	Associated Trustpoints	^1	Usage	Public Key Type		Add
Add Identity Certifica	ate						×		Show Detail
Trustpoint Name:	SSL-Trustpoint								Delete
Import the identity of	certificate from a file (PK	CS12 format with	Certificate(s)+Pri	vate Kev):					Export
Decryption Passobra	ase:								Install
File to Import From:			Browse						Re-Enroll
Add a new identity of a new	certificate:								
Key Pair:	SSL-Keypair	~	Show	New					
Certificate Subject D	N: CN=asa.vpn.exa	mple.com	Select						
Generate self-sig	gned certificate								
Act as local o	certificate authority and	issue dynamic ce	rtificates to TLS-Pr	oxy				-	
			A	dvanced					
Enable CA flag in	n basic constraints exter	nsion							
		6			-				
		Add Certif	icate C	ancel Help				-	

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

ssued To	Issued By	Expiry Date	Associated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Cer	rtificate	· · · · · · · · · · · · · · · · · · ·				×	Show Detail
Trustpoint Name:	SSL-Trustp	oint					Delete
O Import the iden	itity certificate from a	file (PKCS12 format with Certificate	e(s) +Private Key):				Export
Decryption Pass	sphrase:						Install
File to Import Fi	rom:	Identity Certificate Reques	t	×			Re-Enrol
Add a new iden	tity certificate:	To complete the enrollment pro request (CSR) and send it to t	ocess, please save the PKCS10 enrollmer he CA.	t			
Key Pair:	SSL-Keypa	You will then need to install the	e certificate that is returned from the CA	by			
Certificate Subj	ect DN: CN=asa.vp	clicking the Install button in the	e Identity Certificates panel.				
Generate s	elf-signed certificate	Save CSR to File:	Bro	vse			
Act as k	ocal certificate author	ОК	Cancel Help				
		inter and international statements and intern	Advanced				
Enable CA f	flag in basic constraint	s 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.

figuration > Device M	anagement > Certifi	icate Management > Iden	tity Certificates			
Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
asa.vpn.example.com]	Not Available	Pending	SSL-Trustpoint	Unknown		Show Details
						Delete
						Export
						Install
						Re-Enroll

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 Acc	ess VPN > Certificate Mana	igement > <u>CA Certificates</u>				
Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active	Add
IdenTrust Commercial Root	CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Edit
QuoVadis Root CA 2	CN=QuoVadis Root CA 2,	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	Lore

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

sued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active	Add
enTrust Commercial Root	CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Edit
JoVadis Root CA 2	CN=QuoVadis Root CA 2,	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	
Install Certificate			×			Show Detai
						Request CF
Trustpoint Name:	SSL-Trustpoint					Delete
Install from a file:		Browse				
O 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 By	Expiry Date	Associated Trustpoints	Usage	Active	Add
denTrust Commercial Root	CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Edit
uoVadis Root CA 2	CN=QuoVadis Root CA 2,	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	Luit
Install Certificate					×	Show Details
Trustpoint Name: SS	SL-Trustpoint	1.				Request CRI
O Install from a file:		Browse				Delete
Paste certificate in PET	M format:					
cGqeyDMRhs3Rs/wD2 z9kqaRijsx153jV/YLk8	25M2wkAF4AYZHgN9gK9VCK+M E9oAIatnA/fOfX6V	lodKMQZy4X/uhj65NDU7oFf6f				
OR yjali S68Fladwc% gW8YnHOwM08xvyTX gW8YnHOwM08xvyTX ddv(covO)/PAxrrAl3 + +END CERTIFICATE O Use EST: Specify source Interfa EST URL: https:// Certificate Subject DN: allow-untrusted-co Use SCEP: Search course Interfa	Rddtwxr99sftbFhn II Please SLJ/DUCdmAY+IGG garwFN3MXWZO E ce:None :: CN=risavpn31 nnection	e wait Please wait while ASDM is delive device	X INFO: Certificate has the Fingerprint: e9ad165c 26	following attributes: 73424c 6e7e0c5f b30b- iccepted.	4002	
OR yightSBFladArc7K gW8YnHOvM08xvyTX dCVcor0/PAxrnAl3+ END CERTIFICATE O Use EST: Specify source Interfa EST URL: https:// Certificate Subject DN: allow-untrusted-co O Use SCEP: Specify source Interfa SCED URL: http://	RddtWxY95sftbFhin SLIJOUCdmAY+IG E ce:None : CN=risavpn31 mnection	e wait Please wait while ASDM is delive device	X INFO: Certificate has the Fingerprint: e9ad165c 26 Trustpoint CA certificate	following attributes: 73424c 6e7e0c5f b30b4 accepted.	4e02	
OR ysall SEBFiadAxC# gW8YnHOvM08xvyTX deVcovOl/PAxrrAl H END CERTIFICATE DUse EST: Specify source Interfa EST URL: https:// Certificate Subject DN: allow-untrusted-co DUse SCEP: Specify source Interfa SCEP URL: http:// Betry Period:	RddTWxY95sftDeFh SLIJfOUCdmAY+IG E ce:None : CN=risavpn31 mnection	e wait Please wait while ASDM is delividevice	X Information INFO: Certificate has the Fingerprint: e9ad165c 26 Trustpoint CA certificate a	following attributes: 73424c 6e7e0c5f b30b4 cccepted.	4a02	

2. Install Identity Certificate

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

C	onfiguration > Remot	te A	ccess VPN > Certificate M	anagement > Identity Cert	<u>ificates</u>					
	Issued To	^1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	1	Add	
	[vpn.example.com]		Not Available	Pending	SSL-Trustpoint	Unknown			Show Details	
									Delete	
									Export	
									Install	
	1									

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.

sued To ^1 Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
n.example.com] Not Available	Pending	SSL-Trustpoint	Unknown		Show Details
Install Identify contificate		×	General Purpose	RSA (2048 bits)	
a install identity certificate		tpoint	General Purpose	RSA (2048 bits)	Delete
entity Certificate					Export
Install from a file:		Browse			Testall
Install from a file: Paste the certificate data in base-64 forma	ıt:	Browse			Install
Install from a file: Paste the certificate data in base-64 forma	it:	Browse			Install Re-Enroll
Install from a file: Paste the certificate data in base-64 forma	it:	Browse			Install Re-Enroll
Install from a fle: Paste the certificate data in base-64 forma	it:	Browse			Install Re-Enroll
Install from a file: Paste the certificate data in base-64 forma	lt:	Browse			Install Re-Enroll
Install from a file: Paste the certificate data in base-64 forma	t:	Browse			Install Re-Enroll
Install from a file: Paste the certificate data in base-64 forma	it:	Browse			Re-Enroll



c. Click Install Certificate.

sued To ^1 Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
n.example.com] Not Availab	le Pending	SSL-Trustpoint	Unknown		Show Detail
Install Identify costificate		~	General Purpose	RSA (2048 bits)	anon betai
Install Identity certificate		tpoint	General Purpose	RSA (2048 bits)	Delete
dentity Certificate	S Please wait	×			Export
Install from a file:		Information	×		Install
Paste the certhtcate data in be InNBJ26XgDmVuQIBEMVxR2K Gyer 3x2GXML7MAIHBytMdH2 TBy9Yia7boqMnamQkaQpcKAF KdNqIFbUr6VW9NTUF2DowH3 END CERTIFICATE K	evice	Certificate impo	ort succeeded.		Re-Enroll

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.

ooman		OCT ONCORE			
					Edit Delete
	Select SSL Certificate		×		
	Specify enrolled trustpoints to be u OUTSIDE-direct interface. To enrol Management > Identity Certificate:	sed for SSL authentication and VPN load balancing on the a trustpoint, go to Device Management > Certificate			
tificates	Interface:	OUTSIDE-direct	-		hata anna
specity which certificates, it ar	Primary Enrolled Certificate:	SSL-Trustpoint:unstructuredName =asavpn.exampl	~ -	s not associated with a certificate of t	neir own.
Interface	Load Balancing Enrolled Certificate:	None		Key-Type	Edit
OUTSIDE-direct			_		k
inside	OK	Cancel Help			
inside-vlan					
management					
allback Certificate:	None				
and det det and det	- Horice				

- d. Click OK.
- e. Click Apply.

Interface	Primary Certificate	Load Balancing Certificate	Кеу-Туре	Edit
OUTSIDE-direct	SSL-Trustpoint:unstructuredN	ame=	Primary: RSA (2048 bits), Load Balancing:	
nside				
nside-vlan				
management				
- agenere				

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, e.g in case of wildcard certificate, or exported from a different device. It is a binary file, 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.

Issued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
							Show Deta
🔄 Add Identity (Certificate			×			Delete
Trustpoint Name	: SSL-Trustpoint-	PKCS12					Export
 Import the id 	lentity certificate from a file (PKCS12 format with 0	Certificate(s)+Pri	ivate Key):			Install
Decryption P	assphrase:						Re-Enro
File to Impor	t From:		Browse				
O Add a new id	lentity certificate:						
Key Pair:	<default-rsa-k< td=""><td>(ey> 🗸</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-k<>	(ey> 🗸	Show	New			
Certificate Si	ubject DN: CN=risavpn31		Select				
Generate	e self-signed certificate						
Act a	s local certificate authority ar	nd issue dynamic cert	ficates to TLS-P	roxy			
				Advanced			
REnable C	A flag in basic constraints avi	tansion		Auvanceu			
L Cridole C	A hag in basic constraints ext	(criatori)					

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

ssued To	Issued By	Expiry Dat	e	Associated T	rustpoints	Usage	Publ	с Кеу Туре		Add
										Show Detail
🧧 Add Identity Certifi	cate	C	de la companya	×					-	Delete
Trustpoint Name:	SSL-Trustpoint-PK	(CS12			Look in:	tificate file	s	~	/ 🤌 📂 🖽	-
 Import the identity Decryption Passph Sile to Import From 	rase:	KCS12 format with	Certificate(s) +Pri	vate Key):		CSR.txt	ple.com.pfx			
Add a new identity	certificate:		browse							
Key Pair: Certificate Subject	<default-rsa-ke cn="risavpn31</td" dn:=""><td>y> ∨ [</td><td>Show</td><td>New</td><td>Desktop</td><td></td><td></td><td></td><td></td><td></td></default-rsa-ke>	y> ∨ [Show	New	Desktop					
Generate self-	signed certificate	l issue dynamic cer	tificates to TLS-Pr	оху	Documents					
			4	Advanced	This PC	File name:	vpn.example.com.pf:	x	Import ID	certificate file
Enable CA flag	in basic constraints exte	nsion			L	Files of type:	All Files	~	Ca	ancel

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



f. Click Add Certificate.

ssued to	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
🔁 Add Identity C	ertificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-F	PKCS12				Export
Import the id	entity certificate from a file (F	PKCS12 format with Certificate(s)+Private Key):			Install
Decryption Pa	assphrase: ••••					Re-Enroll
File to Import	From: C:\Users\cisco.E	DESKTOP-R2CH8G Browse				
🔿 Add 🔨 Pl	ease wait		Information			×
Certi	Please wait while ASDM device	is delivering the command(s) to	the Created trustpoi	ints for CAs higher in the hie ertificates can be used to vi	erarchy as the CA certificate was not so alidate VPN connections,by default. Ple	elf-signed.
[the validation-us	age of this trustpoint to limi	it the validation scope, if necessary	ase aujust
Enable C/	A flag in basic constraints ext	ension	the validation-us	age of this trustpoint to limi	it the validation scope, if necessary sfully.	ase adjust

N
- T 1

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
conquiations nethole netess this certaindice nanagement	err ceremences

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

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.

Domain		Geroneute		
rtificates Specify which certificates, if ar Interface OUTSIDE-direct Inside Inside-vlan management	Specify enrolled trustpoints to be OUTSIDE-direct interface. To enror Management > Identity Certificat Interface: Primary Enrolled Certificate: Load Balancing Enrolled Certificate	used for SSL authentication and VPN load balancing on the all a trustpoint, go to Device Management > Certificate es. OUTSIDE-direct SSL-Trustpoint-PKCS 12:unstructuredName =FTD72-ek, u e: None K Cancel Help	x res not associated with a certific Key-Type	Edit Delete
Fallback Certificate:	None	2 minutes		

- d. Click OK.
- e. Click Apply.

Certi Sp	ficates — ecify which certificates, if any, should be	e used for SSL authentication on each interface. Th	he fallback certificate will be used on interfaces not assoc	iated with a certificate of their own.	
	Interface	Primary Certificate	Load Balancing Certificate	Кеу-Туре	Edit
	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 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.



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

sued To	~1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
structuredName=asa.example	e.com, L=San Jos	unstructuredName=asa.example	15:09:09 CEDT Jul 1	тр	General Purpose	RSA (2048 bits)	Show Detail
Add Identity Certificate						×	Delete
Trustpoint Name:	ASDM_TrustPoint0						Export
 Import the identity certif 	ficate from a file (PKC	S12 format with Certificate(s)+Priva	te Key):				Install
Decryption Passphrase:							Re-Enrol
File to Import From:		Browse					
O Add a new identity certif	ficate:						
Key Pair:	<default-rsa-key< td=""><td>> v Show</td><td>New</td><td></td><td></td><td></td><td></td></default-rsa-key<>	> v Show	New				
Certificate Subject DN:	CN=risavpn31	Select					
Generate self-signed	l certificate						
Act as local certif	ficate authority and is	ssue dynamic certificates to TLS-Prox	у			6	
		Adv	vanced				
🗹 Enable CA flag in bas	sic constraints extens	ion					

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.

sued to Issued	Ву	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
structuredName= CN=ca.	example.com, OU	15:10:00 CEST F	Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
a Add Identity Certificate				×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
O Import the identity cert	ficate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Passphrase:							Re-Enroll
File to Import From:			Browse				
Add a new identity cert	ificate:						
Key Pair:	<default-rsa-key< td=""><td>y> ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-key<>	y> ~	Show	New			
Certificate Subject DN:	CN=asavpn.exam	ple.com	Select				
Generate self-signe	d certificate						
Act as local cert	ficate authority and	issue dynamic cer	tificates to TL	S-Proxy			
				Advanced			
Enable CA flag in ba	sic constraints exter	nsion					

- 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.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName=.	CN=ca.example.com, OU	15: 10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
add Identity C	Certificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23				Export
C 🔤 Add Key	/ Pair		× _{Key):}			Install
Key Type:	() RSA		A			Re-Enroll
	-					
Name:	O Use default key pair name					
Size.	Enter new key pair name:	SSL-KeyPair-2023	ew			
Usage:	General purpose	Special				
G	enerate Now Cance	el Help	iced			
	n nug er busic const dents catter	131011				
	Add Certificate Ca	ancel Help				

3. Select the Key Pair Name

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

ssued to	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName=.	CN=ca.example.com, OU	. 15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
🔄 Add Identity C	Certificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-20	023				Export
O Import the ide	entity certificate from a file (Pi	KCS12 format with Certificate	:(s)+Private Key):			Install
Decryption Pa	assphrase:					Re-Enroll
File to Import	From:	Browse				
Add a new ide	entity certificate:					
Key Pair:	SSL-KeyPair-2023	3 v Show	New			
Certificate Su	bject DN: CN=asavpn.exan	nple.com Select.	•• 11			
Generate	self-signed certificate					
Act as	s local certificate aut grity and	l issue dynamic certificates to	TLS-Proxy			
			Advanced			
	A flag in basic constraints exte	nsion				

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.

ssued To Issu	ied By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName= CN=	ca.example.com, OU	15:10:00 CEST F	Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🔄 Add Identity Certifica	ate			×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
O Import the identity of	ertificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Passphra	se:						Re-Enroll
File to Import From:			Browse				
Add a new identity of	ertificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate Subject D	N: CN=asavpn.exam	ple.com	Select				
Generate self-sig	gned certificate						
Act as local of	ertificate authority and	issue dynamic cer	tificates to TL	S-Proxy			
				Advanced			
Enable CA flag in	basic constraints exter	nsion					

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

Issued To	Issued By		Expiry Da	te	Associated Trustpoints		Usage	Public Key Type	Add
InstructuredNar	ne= CN=ca.exan	nple.com, OU	15:10:00	CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detai
🧧 Add Ident	ity Certificate				×				Delete
Trustpoint N	ame: SS	L-Trustpoint-20	23		-				Export
Certificate Sub	ect DN					×			Install
						_			Re-Enroll
				Attribute	Value				
DN Attribute t	o be Added Country (C)	× A	dd>>	Company Name (O)	example inc				
Value:	usl		elete						
			chette						
						_			
		OK	Cancel	Help					
Enat	le CA flag in basic ci	onstraints exter	ision	nop					

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
0	The legally registered name of your organization/company
С	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**.

sued to Issued	By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
structuredName= CN=ca	example.com, OU	15:10:00 CEST	Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
add Identity Certificate				×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
O Import the identity cert	ificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Passphrase							Re-Enroll
File to Import From:			Browse				
Add a new identity cert	ificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate Subject DN:	/pn.example.com,	O=example inc	Select				
Generate self-signe	d certificate						
Act as local cert	ificate authority and	issue dynamic cer	tificates to TL	S-Proxy			
			- T	Advanced			
Enable CA flag in b	asic constraints exter	sion					

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

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
Advanced (ntions	DU LIEUTOLOGIOSET SAN E D	24 SCI Trusteeint	General Purpose	RSA (2048 bits)	Show Detail
Auvanceu (puons .		~			Delete
Enrollment mode	parameters and SCEP cha	SCEP Challenge Password are not available	e for self-signed certificates.			Export
	Enfoiment Mode	SCEP Challenge Password				Install
FQDN:	asavpn.example.com					Re-Enroll
E-mail:						
IP Address:						
Include se	rial number of the device					
		N				
		63				

5. Generate and Save the CSR

a. Click Add Certificate.

ssued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName= (CN=ca.example.com, OU	15:10:00 CEST F	eb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
🗧 Add Identity Cert	ificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
O Import the identi	ity certificate from a file (PK	CS12 format with	Certificate(s)+	+Private Key):			Install
Decryption Pass	phrase:						Re-Enroll
File to Import Fro	om:		Browse				
Add a new identi	ity certificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate Subje	ct DN: /pn.example.com,	O=example inc	Select				
Generate sel	If-signed certificate						
Act as los	cal certificate authority and	issue dynamic cert	tificates to TLS	S-Proxy			
			r	Advanced			
Enable CA fi	an in basic constraints exter	nion	L	Plana la calina			
	מע ווי שמאר כטוואי מוונא באנבו	131013					

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

sued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
structuredNam	e= CN=ca.example.com,	OU 15:10:00 CEST Feb 6 202	4 SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🧧 Add Identi	ty Certificate		×			Delete
Trustopint Na	mer CSL Truston	int-2022				Export
	e identity certificate from a f	ile (PKCS12 format with Certificat	e(s)+Private Kev):			Install
(Re-Enrol
F	entity Certificate Request		^			
To c requ	omplete the enrollment proce lest (CSR) and send it to the	ess, please save the PKCS10 enro CA.	llment			
K You click	will then need to install the c ing the Install button in the I	ertificate that is returned from th dentity Certificates panel.	e CA by			
[Sav	e CSR to File: C:\Users\cisco	D.DESKTOP-R2CH8G5\Docun	Browse			
	ОК	Cancel Help				
			Advanced			
🗌 Enabl	e 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.

sued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
structuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detai
savpn.example.com]	Not Available	Pending	SSL-Trustpoint-2023	Unknown		
						Delete
						Export
						Install
						Re-Enrol

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 can be installed in separate CA Trustpoints.

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

Issued To	Issued By ^1	Expiry Date	Associated Trustpoints	Usage	Active	Add
a.example.com	CN=ca.example.com, OU=I	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes	Edit
QuoVadis Root CA 2	CN=QuoVadis Root CA 2,	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	Luit
denTrust Commercial Root	. CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Show Detail

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.

ssued To	Issued By ^1	Expiry Date	Associated Trustpoints	Usage	Active		Add
a.example.com	CN=ca.example.com, OU=l	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes		Edit
Install Certificate						×	Show Detail
Trustpoint Name:	SSL-Trustpoint-2023					1	Request CR
		Browse					Delate

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

c. Click Install Certificate.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active	Add
.example.com	CN=ca.example.com, OU=l	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes	Edit
🧧 Install Certificate						× Show Detail
Trustpoint Name:	SSL-Trustpoint-2023					Request CR
O Install from a file:		Browse				Delete
Paste certificate in I	PEM format:					
VROOBBYEFESSKZs 9ttFV52U42m9UX cGqeyDMRhs3Rs/w 29kqaRijsx153JV/H 0jRyaJH58BFladMv gW8YnHOvM08svy dcVcov0/jPAxmAJ END CERTIFIC Use EST: Specify source Inter	bra9b9LLFV52U47em9UXaM83GA MAGCSQGSIb3DQEBCWUAAHB XAGCSQGSIb3DQEBCWUAAHB X8E90ALatnA/fQ7K04H7 XRRdHVXM9SRbEhN80G TXSUJf0UCdmAYHG0gqh +Hg2yWFN3MXWZ0453C ATE	1UdIwQYMBaAFE55kZsbra9b AOArsXlFwK3lNBwOsYh5maT iformation INFO: Certificate har Fingerprint: e9ad165 Trustpoint CA certific	s the following attributes: 5c 2673424c 6e7e0c5f b30b4a02 cate accepted.	×		~
EST URL: https:// Certificate Subject I allow-untrusted	CN=risavpn31		ОК			
EST URL: https:// Certificate Subject I allow-untrusted Use SCEP: Specify source Inter	CN=risavpn31 -connection	~	ОК			
EST URL: https:// Certificate Subject I allow-untrusted Use SCEP: Specify source Inter SCEP URL: http://	CN=risavpn31 connection face: None		ОК			

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 ^1	Expiry Date	Associated Trustpoints	Usage	Active	Add
ca.example.com	CN=ca.example.com, OU=I	15:10:00 CEST Feb 6 2030	SSL-Trustpoint-2023, SSL-Trustpoint	General Purpose	Yes	Edit
QuoVadis Root CA 2	CN=QuoVadis Root CA 2,	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	Luit
denTrust Commercial Root	CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Show Details
						Request CRL
						Delete

п

2. Install Identity Certificate

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

sued To	Issued By	Expiry Date	Associated Trustpoints	~1	Usage	Public Key Type	Add
structuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Deta
savpn.example.com]	Not Available	Pending	SSL-Trustpoint-2023		Unknown		
							Delete
							Export
							Install

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.

ssued To	Issued By	Expiry Date	Associated Trustpoints	~1	Usage	Public Key Type	Add
nstructuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Details
savpn.example.com	n] Not Available	Pending	SSL-Trustpoint-2023		Unknown		Delete
							Delete
							Export
Install Identity	certificate		×				Install
dentity Certificate							Re-Enroll
Install from a	file:		Browse				
		L					
O Paste the cer	tificate data in base-64 format	:					

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

c. Click Install Certificate.

sued To	Issued By	Expiry Date	Associated Trustpoints	~1	Usage	Public Key Type	Add
structuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detai
savpn.example.com]	Not Available	Pending	SSL-Trustpoint-2023		Unknown		Delete
							Delete
							Export
Install Identity c	ertificate		×				Install
							De Ferd
lentity Certificate							Re-Enrol
lentity Certificate –	wait						Re-Enroll
In Please	wait	tion	×				Re-Enrol
entity Certificate – O In Please Pa	wait	tion	×				Re-Enroll
In Please	wait	tion	×				Re-Enroll
entity Certificate – O In Please Pri G r:	Wait Please wait wf device	tion Certificate import succeede	× d.				Re-Enroll
entity Certificate - O In Please Pr Pr e	wait Please wait wf device	tion Certificate import succeede	× d.				Re-Enrol
entity Certificate – O In Please Pa Pa R G r: W	wait	tion Certificate import succeede	d.				Re-Enroll
entity Certificate - O In Please Pra H G r: H C V - V	wait Please wait wh device	tion Certificate import succeede	×				Re-Enroll

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

Issued To	Issued By	Expiry Date	Associated Trustpoints	v 1	Usage	Public Key Type	Add
nstructuredName=	CN=ca.example.com, OU	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023		General Purpose	RSA (4096 bits)	Show Deta
nstructuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Choir Deta
							Delete
							Export
							Install
							Do Epro

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.

				Edit Delete
[Select SSL Certificate	×		
rtificates	Specify enrolled trustpoints to be us OUTSIDE-direct interface. To enroll Management > Identity Certificates	sed for SSL authentication and VPN load balancing on the a trustpoint, go to Device Management > Certificate 5.		
Specify which certificates, if an	Interface:	OUTSIDE-direct	tes not associated with a certificate of their own.	
Interface	Primary Enrolled Certificate:	SSL-Trustpoint-2023:unstructuredName=asavpn.exampl v	Кеу-Туре	Edit
OUTSIDE-direct	Load Balancing Enrolled Certificate:	None V	Primary: RSA (2048 bits), Load Balancing: n	
inside				
inside-vlan	OK	Cancel Help		
management				

- d. Click OK.
- e. Click Apply. Now the new Identity Certificate is in use.

anation > Remote Acce	ss VPN > Advanced > <u>SSL Settings</u>			
				Edit Delete
ificates ecify which certificates, if a	19, should be used for SSL authentication on ea	ch interface. The fallback certificate will be u	sed on interfaces not associated with a certificate of their own.	Edit
ificates ecify which certificates, if a Interface	ny, should be used for SSL authentication on ea Primary Certificate	ch interface. The fallback certificate will be u: Load Balancing Certificate	sed on interfaces not associated with a certificate of their own. Key-Type	Edit
ificates ecify which certificates, if ar Interface CUTSIDE-direct	ny, should be used for SSL authentication on ea Primary Certificate SSL-Trustpoint-2023:unstructure	ch interface. The fallback certificate will be u Load Balancing Certificate	sed on interfaces not associated with a certificate of their own. Key-Type Primary: RSA (4096 bits), Load Balancing: n	Edit
ficates — ecify which certificates, if ar Interface OUTSIDE-drect inside	ny, should be used for SSL authentication on ea Primary Certificate SSL-Trustpoint-2023:unstructure	ch interface. The fallback certificate will be u Load Balancing Certificate	sed on interfaces not associated with a certificate of their own. Key-Type Primary: RSA (4096 bits), Load Balancing: n	Edit
ificates ecify which certificates, if a Interface OUTSIDE-direct inside inside_vlan	ny, should be used for SSL authentication on ea Primary Certificate SSL-Trustpoint-2023;unstructure	ch interface. The fallback certificate will be u Load Balancing Certificate	sed on interfaces not associated with a certificate of their own. Key-Type Primary: RSA (4096 bits), Load Balancing: n	Edit

Renew a Certificate Enrolled with PKCS12 File with ASDM

Certificate renewal of PKCS12 enrolled certificate requires 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**.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Detai
🔤 Add Identity Certifi	cate		×			Delete
Trustpoint Name:	SSL-Trustpoint-PK	ICS12				Export
 Import the identity 	certificate from a file (PK	CS12 format with Certificate(s)	+Private Key):			Install
Decryption Passphr	rase:					Re-Enrol
File to Import From	:	Browse				
O Add a new identity	certificate:					
Key Pair:	<default-rsa-ke< td=""><td>y> v Show</td><td>New</td><td></td><td></td><td></td></default-rsa-ke<>	y> v Show	New			
Certificate Subject	DN: CN=risavpn31	Select				
Generate self-s	signed certificate					
Act as local	certificate authority and	issue dynamic certificates to TL	S-Proxy			
			Advanced			
Nenable CA flag	in basic constraints exter	nsion				
-63						

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

ssued To	Issued By	Expiry Date	Associated	Trustpoints	Usage	Public Key Typ	e	Add
								Show Detail
🧧 Add Identity C	ertificate	L.		×				Delete
Trustpoint Name:	SSL-Trustpoint-F	PKCS12		import ID certifi	cate file			
 Import the ide 	entity certificate from a file (F	PKCS12 format with Certificate	(s) +Private Key):	Look in:	Document	5		-
Decryption Pa	ssphrase:			<u>e</u> .	CSR.txt			
File to Import	From:	Browse.		Recent Items	29 vpn.exam	ple.com.ptx		
O Add a new ide	entity certificate:							
Key Pair:	<default-rsa-k< td=""><td>Show.</td><td>. New</td><td>Desktop</td><td></td><td></td><td></td><td></td></default-rsa-k<>	Show.	. New	Desktop				
Certificate Sul	bject DN: CN=risavpn31	Select.						
Generate	self-signed certificate			Documents				
Act as	local certificate authority an	nd issue dynamic certificates to	TLS-Proxy					
			Advanced	This PC Fi	e name:	vpn.example.com.pfx	Import ID	certificate file
Enable CA	flag in basic constraints ext	rension	Have Nocurri	- 🗳 F	es of type:	All Files	, (Cancel

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

ssued To I	ssued By E	xpiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
Add Identity Certificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-PKCS12					Export
Import the identity cert	tificate from a file (PKCS12 for	mat with Certificate(s)+P	rivate Key):			Install
Decryption Passphrase	:					Re-Enroll
File to Import From:	C: \Users\cisco.DESKTOP-R	2CH8G Browse				
O Add a new identity cert	tificate:					
Key Pair:	<default-rsa-key></default-rsa-key>	Show	New			
Certificate Subject DN:	CN=risavpn31	Select				
Generate self-signe	ed certificate					
Act as local cert	tificate authority and issue dyr	namic certificates to TLS-F	Proxy			
			Advanced			
Enable CA flag in ba	asic constraints extension		Paranceann			
<i>,</i>						

f. Click Add Certificate.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
🔁 Add Identity C	ertificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-	PKCS12				Export
Import the ide	entity certificate from a file (PKCS12 format with Certificate((s)+Private Key):			Install
Decryption Pa	assphrase: ••••		10000			Re-Enroll
File to Import	From: C:\Users\cisco.	DESKTOP-R2CH8G Browse.				
🔿 Add 🔚 Ple	ease wait		Information			×
Certi	Please wait while ASDM device	I is delivering the command(s) to	the Created trustpoint WARNING: CA cert the validation-usage	s for CAs higher in the hie lificates can be used to va je of this trustpoint to limit	rarchy as the CA certificate was not s alidate VPN connections,by default. Ple t the validation scope, if necessary	elf-signed.
Enable CA	A flag in basic constraints ex	tension	Import PKCS 12 ope	eration completed success	fully.	

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

Issued To v1	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.

Domain	Gerbilde	
		Edit Delete
tificates pecify which certificates, if ar Interface OUTSIDE-direct Inside	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-PKCS 12:unstructuredName=FTD72-ek, u v Load Balancing Enrolled Certificate: OK Cancel Help	r own.
management	None V	

- d. Click OK.
- e. Click Apply.

Certi	Certificates								
Sp	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	Кеу-Туре	Edit				
	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	e used for SSL authentication on each interface. The	he fallback certificate will be used on interfaces not assoc	iated with a certificate of their own.	
Interface	Primary Certificate	Load Balancing Certificate	Кеу-Туре	Edit
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 it does 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 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 can 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**.

File View Tools Wizards Wind	ow Help					Type topic to search	Go	ababa
🚮 Home 🦓 Configuration 🔯 Mo	nitoring 🔚 Save 🔇 Refre	esh 🔇 Back 🔘 Forwar	d 🦻 Help					cisco
Bookmarks 🗗 🕂 🗙	Configuration > Device Ma	nagement > Certificate M	lanagement > Identity Ce	rtificates				
o bookmark a page, right-dick on a ode in the navigation tree and select Add to bookmarks".	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type		Add
Go 🏦 Delete	unstructuredName=asav	CN=ca.example.com, OU CN=ca.example.com, OU	15:10:00 CEDT Apr 6 2024 15:10:00 CEST Feb 6 2024	SSL-Trustpoint-2023	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)		Show Details
	unstructuredName=FTD7	CN=KrakowCA-sub1-1	04:44:00 CEST Dec 21 2024	SSL-Trustpoint-PKCS12	General Purpose	RSA (2048 bits)	1	Delete
	[asa.vpn.example.com]	Not Available	Pending	SSL-Trustpoint	Unknown			Eunest
								Export
								Install
								Re-Enrol
Device Management								
Management Access								
System Image/Configuration								
High Availability and Scalability								
E-1 Logging	Find:	O O Match Case						
Smart Call-Home	Cartificate Evolution Alasta							
Service Module Settings	Ceronicate Expiration Alerts							
🕀 🚮 Users/AAA	Send the first alert befor	e: 60 (days) Set Def	ault					
E Certificate Management	Repeat Alert Interval :	7 (days)						
- 2 Identity Certificates	Weak Crypto Configurations -							

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

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage		Public Key Type	Add
nstructuredName=asav	CN=ca.example.com, OU	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023	Gene	ral Purpose	RSA (4096 bits)	Show Details
nstructuredName=risav	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	Gene	ral Purpose	RSA (2048 bits)	Show Details
nstructuredName=FTD7	CN=KrakowCA-sub1-1	04:44:00 CEST Dec 21 2024	SSL-Trustpoint-PKCS12	Gene	eral Purpose	RSA (2048 bits)	Delete
sa.vpn.example.com]	Not Available	Pending	SSL-Trustpoint	U	Inknown		Export
							Coport
							Install
							Re-Enroll
nd:	🗇 🔘 🗌 Match Case						
nd: rtificate Expiration Alerts - Send the first alert before	Match Case (days) Set Defa	ult					
nd: tificate Expiration Alerts – Send the first alert before Repeat Alert Interval :	O Match Case (days) Set Defa (days) (days)	ndt					
nd:	 Match Case 60 (days) Set Defa 7 (days) Export certificate 	ult		×			
nd: tificate Expiration Alerts – Send the first alert before Repeat Alert Interval : : Crypto Configurations — Permit Weak key sizes and	 Match Case (days) Set Defa (days) Export certificate Ha 	ult	27CH8rCS\Documents\ve Rousse	×			
nd: tificate Expiration Alerts - Send the first alert before Repeat Alert Interval : Crypto Configurations - Permit Weak key sizes an	Match Case Match Case (days) Set Defa (days) Export certificate tha Export to File:	ult C:\Users\cisco.DESKTOP4	R2CH8G5\Documents\ce Browse	×			
nd: tificate Expiration Alerts Send the first alert before Repeat Alert Interval : Crypto Configurations Permit Weak key sizes and CA Enrollment	Match Case Match Case (days) Set Defa 7 (days) Export certificate Ha Export to File: Certificate Format:	ult C:\Users\cisco.DESKTOP4	R2CH8G5\Documents\ce Browse	×			
nd: tificate Expiration Alerts - Send the first alert before Repeat Alert Interval : Crypto Configurations Permit Weak key sizes and CA Enrollment	Match Case Match Case Match Case Go (days) Set Defa (days) Export certificate dHa Export to File: Certificate Format: pplie	ult C:\Users\cisco.DESKTOP4 PKCS12 Format (Certif	R2CH8G5\Documents\ce Browse ficate(s) + Private Key)	×	mers a special p	promotional price for certificat	es and trial certificates t
nd: tificate Expiration Alerts - Send the first alert before Repeat Alert Interval : Crypto Configurations Permit Weak key sizes and CA Enrollment	 Match Case (days) Set Defa (days) Export certificate Certificate Format: ppla 	ult C:\Users\cisco.DESKTOP4 @ PKCS12 Format (Certifi PEM Format (Certificat	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	X	ners a special p	promotional price for certificat	es and trial certificates f
nd: tificate Expiration Alerts Send the first alert before Repeat Alert Interval : Crypto Configurations Permit Weak key sizes and CA Enrollment t your Cisco ASA security a ting.	Match Case Match Case Match Case (days) Set Defa (days) Export certificate dHa Export to File: Certificate Format: pplia	ult C:\Users\cisco.DESKTOP+ PKCS12 Format (Certif PEM Format (Certificat	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	× stor	ners a special p	promotional price for certificat	es and trial certificates f
nd: tificate Expiration Alerts - Send the first alert before Repeat Alert Interval : : Crypto Configurations - : CA Enrollment - t your Cisco ASA security a ting.	Match Case Match Case Match Case Go (days) Set Defa (days) Export certificate tha Export to File: Certificate Format: ppla ifica Configuration Encryption	ult C:\Users\cisco.DESKTOP+ @ PKCS 12 Format (Certificat) PEM Format (Certificat an Passphrase	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	× stor	ners a special j	promotional price for certificat	es and trial certificates f
ind: trificate Expiration Alerts - Send the first alert before Repeat Alert Interval : k Crypto Configurations -] Permit Weak key sizes and c CA Enrollment	Match Case Match Case Match Case (days) Set Defa 7 (days) Export certificate Ha Export to File: Certificate Format: pplic fica Configuration Encryption Passphra	U U U U U U U U U U U U U U U U U U U	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	× stor	mers a special p	promotional price for certificat	es and trial certificates f
nd: tificate Expiration Alerts - Send the first alert before Repeat Alert Interval : : Crypto Configurations Permit Weak key sizes and : CA Enrollment	Match Case Match Case Match Case Match Case Certificate Certificate Format: Certificate Format: Description Encryption Encryption Passphra Configuration Encryption	ult C:\Users\cisco.DESKTOP4 PKCS12 Format (Certificat PEM Format (Certificat an Passphrase se:	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	× stor	ners a special p	promotional price for certificat	es and trial certificates f

The exported certificate can be on the computer disk. Please take note of 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 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 of 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.