# Certificaten installeren en verlengen op ASA die door ASDM wordt beheerd

### Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie Een nieuw identiteitscertificaat aanvragen en installeren met ASDM Een nieuw identiteitscertificaat aanvragen en installeren met aanvraag voor certificaatondertekening (CSR) Genereert een CSR met ASDM Een Trustpoint met een specifieke naam maken (Optioneel) Maak een nieuw sleutelpaar De naam van het sleutelpaar kiezen Configureer het certificaatonderwerp en de volledig gekwalificeerde domeinnaam (FQDN) MVO genereren en opslaan Installeer het Identity Certificate in PEM-formaat met ASDM CA-certificaat installeren dat de CSR heeft ondertekend Installeer het identiteitscertificaat Bind het nieuwe certificaat aan Interface met ASDM Installeer een Identity Certificate dat is ontvangen in PKCS 12-formaat met ASDM Installeer de Identity en CA-certificaten uit een PKCS12-bestand Bind het nieuwe certificaat aan Interface met ASDM Certificaat-verlenging Verleng een certificaat dat is ingeschreven met aanvraag voor certificaatondertekening (CSR) met ASDM Genereert een CSR met ASDM Maak een nieuw Trustpoint met een specifieke naam. (Optioneel) Maak een nieuw sleutelpaar Selecteer de naam van het sleutelpaar Configureer het certificaatonderwerp en de volledig gekwalificeerde domeinnaam (FQDN) MVO genereren en opslaan Installeer het identiteitscertificaat in PEM-formaat met ASDM CA-certificaat installeren dat de CSR heeft ondertekend Installeer het identiteitscertificaat Bind het nieuwe certificaat aan Interface met ASDM Verleng een certificaat dat is ingeschreven voor PKCS 12-bestand met ASDM Installeer het vernieuwde identiteitscertificaat en CA-certificaten uit een PKCS12-bestand Bind het nieuwe certificaat aan Interface met ASDM Verifiëren

Geïnstalleerde certificaten bekijken via ASDM Problemen oplossen Veelgestelde vragen

## Inleiding

Dit document beschrijft hoe u bepaalde typen certificaten kunt aanvragen, installeren, vertrouwen en verlengen op Cisco ASA-software die met ASDM wordt beheerd.

### Voorwaarden

### Vereisten

- Voordat u begint te controleren of de adaptieve security applicatie (ASA) de juiste kloktijd, datum en tijdzone heeft. Met certificaatverificatie wordt aanbevolen een NTP-server (Network Time Protocol) te gebruiken om de tijd op de ASA te synchroniseren. Controleer verwante informatie voor referentie.
- Om een certificaat aan te vragen dat gebruik maakt van certificaatondertekeningsaanvraag (CSR), moet het toegang hebben tot een vertrouwde interne of externe certificeringsinstantie (CA). Voorbeelden van CA-leveranciers van derden zijn onder meer Entrust, Geotrust, GoDaddy, Thawte en VeriSign.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASAv 9.18.1
- Voor het maken van PKCS12 wordt OpenSSL gebruikt.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Het soort certificaten dat in dit document wordt vermeld, is:

- zelfondertekende certificaten
- certificaten ondertekend door een certificeringsinstantie van een derde partij of een interne CA

De Secure Socket Layer (SSL), Transport Layer Security (TLS) en IKEv2 rfc7296 voor EAPverificatieprotocollen schrijven voor dat de SSL/TLS/IKEv2-server de client een servercertificaat biedt waarmee de client serververificatie kan uitvoeren. Het wordt aanbevolen vertrouwde externe CA's in te schakelen voor het verstrekken van SSL-certificaten voor de ASA. Cisco raadt het gebruik van een zelfondertekend certificaat niet aan, omdat een gebruiker daarbij per ongeluk een browser kan configureren om het certificaat van een onbetrouwbare server te vertrouwen. Bovendien moeten gebruikers dan reageren op een security waarschuwing wanneer verbinding wordt gemaakt met de beveiligde gateway.

## Een nieuw identiteitscertificaat aanvragen en installeren met ASDM

Een certificaat kan worden aangevraagd bij een certificeringsinstantie (CA) en op twee manieren worden geïnstalleerd op een ASA:

- Aanvraag voor certificaatondertekening (CSR) gebruiken. Genereer een sleutelpaar, vraag een identiteitscertificaat aan bij CA met een CSR, installeer het ondertekende identiteitscertificaat dat is verkregen van de CA.
- Gebruik PKCS12-bestand dat is verkregen van een CA of dat is geëxporteerd van een ander apparaat. Het PKCS12-bestand bevat sleutelpaar, identiteitscertificaat, CA-certificaat(s).

## Een nieuw identiteitscertificaat aanvragen en installeren met aanvraag voor certificaatondertekening (CSR)

Er wordt een CSR gemaakt op het apparaat dat een identiteitscertificaat nodig heeft, gebruik een sleutelpaar dat op het apparaat is gemaakt.

Een MVO bevat:

- informatie over het certificaatverzoek aangevraagd onderwerp en andere eigenschappen, openbare sleutel van het sleutelpaar,
- informatie over handtekeningsalgoritmen;
- digitale handtekening van de informatie van het certificaatverzoek, die met de privé sleutel van het Zeer belangrijke paar wordt ondertekend.

De CSR wordt doorgegeven aan de certificeringsinstantie (CA), zodat deze deze ondertekent, in een PKCS#10-formulier.

Het ondertekende certificaat wordt door CA teruggestuurd in een PEM-formulier.

Opmerking: CA kan de FQDN- en onderwerpnaamparameters die in het Trustpoint zijn gedefinieerd, wijzigen wanneer het de CSR ondertekent en een ondertekend identiteitscertificaat aanmaakt.

### Genereert een CSR met ASDM

- 1. Een Trustpoint met een specifieke naam maken
  - a. Blader naar Configuratie > Apparaatbeheer > Certificaatbeheer > Identity Certificates.



- b. Klik op Add (Toevoegen).
- c. Definieer een trustpoint naam.

sued To	Issued By	Expiry Date	Associated Trustpoints	^¹ Usage	Public Key Type	Add
🗧 Add Identity Cert	tificate				>	K Show Detai
Trustpoint Name:	SSL-Trustpoint	_				Delete
Import the ident	ity certificate from a file (	KCS12 format with Certificate(	s)+Private Key):			Export
Decryption Pass	phrase:					Install
File to Import Fre	om:	Browse				Re-Enrol
Add a new ident Key Pair:	ity certificate:	ev> Show	New			
Key Pair:	<default-rsa-k< td=""><td>iey&gt; v Show</td><td>New</td><td></td><td></td><td></td></default-rsa-k<>	iey> v Show	New			
	If classed costificate	select.	•			
Generate se	IT-signed certificate					
Act as lo	cal certificate authority an	id issue dynamic certificates to	TLS-Proxy			
			Advanced			
Enable CA fla	ag in basic constraints ext	ension				

- d. Klik op het keuzerondje Add a new identity certificate (Voeg een nieuw identiteitscertificaat toe).
- 2. (Optioneel) Maak een nieuw sleutelpaar

Opmerking: standaard wordt de RSA-toets met de naam Default-RSA-Key en een grootte van 2048 gebruikt. Het wordt echter aanbevolen om voor elk Identity Certificate een uniek privaat/publiek sleutelpaar te gebruiken.

a. Klik op Nieuw om een nieuw sleutelpaar te genereren.

sued To	Issued By	Expiry Da	te	Associated Trustp	points	Usage	Public Key Type	Add
Add Identity Cer	tificate				×	General Purpose	RSA (4096 bits)	Show Deta
					_	General Purpose	RSA (2048 bits)	Delete
Trustpoint Name:	SSL-Trustpoint							
O Import the ident	tity certificate from a file (	PKCS12 format with	Certificate(s)+P	rivate Key):				Export
Decryption Pass	phrase:							Install
File to Import Fr	om:		Browse					Re-Enrol
Add a new iden	tity certificate:							
Key Pair:	<default-rsa+< td=""><td>Key&gt; ~</td><td>Show</td><td>New</td><td></td><td></td><td></td><td></td></default-rsa+<>	Key> ~	Show	New				
Certificate Subje	ect DN: CN=asavpn.ex	ample.com	Select					
Generate se	elf-signed certificate							
Act as lo	ocal certificate authority a	nd issue dynamic ce	rtificates to TLS-f	roxy				
				Advanced				
Enable CA f	lag in basic constraints ex	tension						

- b. Kies de optie Voer een nieuwe sleutelpaarnaam in en voer een naam in voor het nieuwe sleutelpaar.
- c. Selecteer RSA of ECDSA bij Key Type (Sleuteltype).
- d. Kies de sleutelgrootte; voor RSA, kies algemeen doel voor gebruik.
- e. Klik op Generate Now (Nu genereren). Het sleutelpaar wordt nu gecreëerd.

isued To	Issued By	Expiry Date	Associated Trustpoints		Usage	Public Key Type	Add
Add Identity Certif	cate			×	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)	Show Deta
Trustpoint Name:	SSL-Trustpoint						Delete
🔿 Impor 🔁 Add I	(ey Pair		×				Export
Decry	0.000	0.000					Install
File to Key Typ	e: () RSA	() ECDSA () ED	DSA				Re-Enro
Add a     Name:	O Use default key r	pair name					
Key Pa	Enter new key p	pair name: SSL-Keypair					
Certifi Size:	2048	~	N				
	General purpose	O Special	2				
Ge Usage:							
Ge Usage:							
Ge Usage:			_				

3. De naam van het sleutelpaar kiezen

Kies het sleutelpaar om de MVO te ondertekenen met, en te worden gebonden aan het nieuwe certificaat.

sued To	Issued By	Expiry Date	Associated Trustp	oints	Usage	Public Key Type	Add
🔄 Add Identity Ce	ertificate			×	General Purpose	RSA (4096 bits)	Show Detai
				_	General Purpose	RSA (2048 bits)	Delete
Trustpoint Name:	SSL-Trustpoint						
O Import the ide	ntity certificate from a file (	(PKCS12 format with Certificate(	s)+Private Key):				Export
Decryption Pas	ssphrase:						Install
File to Import I	From:	Browse					Re-Enrol
Add a new ide	ntity certificate:						
Key Pair:	SSL-Keypair	> Show	New				
Certificate Sub	nject DN: CN=asavpn.ex	ample.com Select					
Generate	self-signed certificate						
Act as	local certificate authority a	nd issue dynamic certificates to T	TLS-Proxy				
			Advanced				
Enable CA	flag in basic constraints ex	tension	600 <del>0</del>				

4. Configureer het certificaatonderwerp en de volledig gekwalificeerde domeinnaam (FQDN)

Waarschuwing: de FQDN-parameter moet overeenkomen met de FQDN of het IPadres van de ASA-interface waarvoor het identiteitscertificaat wordt gebruikt. Deze parameter stelt de gevraagde extensie voor de alternatieve onderwerpnaam (SAN) voor het identiteitscertificaat in. De SAN-extensie wordt gebruikt door SSL/TLS/IKEv2client om te controleren of het certificaat overeenkomt met de FQDN waarmee verbinding wordt gemaakt.

a. Klik op Selecteren.

0.07	Expiry Date	Associated Trustpoints	^1 Usage	Public Key Type	Add
				×	Show Deta
L-Trustpoint	_				Delete
e from a file (PKCS12 for	mat with Certificate(s)+F	Private Kev):			Export
					Install
	Browse				Re-Enro
2:					
L-Keypair	v Show	New			
=asavpn.example.com	Select				
tificate		•			
authority and issue dyr	namic certificates to TLS-	Proxy			
		Adversed			
		Auvanceu			
instraints extension					
	-Trustpoint e from a file (PKCS12 for e: 	-Trustpoint -TrustpointTrustpoint	-Trustpoint  -Trustpoint  -Trustpoint Trustpoint	-Trustpoint  -Trustpoint  -Trustpoint  -Trustpoint Trustpoint	Trustpoint :-Trustpoint : from a file (PKCS12 format with Certificate(s) +Private Key): Browse Browse :: L-Keypair Show New savpn.example.com Select tificate : authority and issue dynamic certificates to TLS-Proxy Advanced instraints extension

b. In het venster Certificaat Onderwerp DN, vorm certificaatattributen - kies attribuut van vervolgkeuzelijst, ga de waarde in, klik op Add.

sued To	Issued By	Expiry Date	Associated Trustpoints	^1 Usage	Public Key Type	Add
Add Identity Certificat	e				×	Show Detail
Trustpoint Name:	SSL-Trustpoint					Delete
O Import the identity ce	Cartificata Subject	DN		×		Export
Decryption Passphrase	Certificate Subject	DIN		^		Install
File to Import From:			Attribute	Value		Re-Enroll
Add a new identity certificate Subject DN Generate self-sion	DN Attribute to b Attribute: Com Value: asa.	e Added mon Name (CN) V vpn.example.com	Add>> Delete			
Act as local ce		ОК	Cancel Help			
Enable CA flag in t						

Configuration > Device Management > Certificate Management > Identity Certificates
--

Issued To	Issued By	Expiry Date	Assoc	iated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Certific	ate		1				×	Show Detail
Trustpoint Name:	SSL-Trustpoint							Delete
O Import the identity	el 🕞 Cartificata Subi	ect DN				×		Export
Decryption Passphra	ertificate subj	ect Div				^		Install
File to Import From:				Attribute	Value			Re-Enroll
Add a new identity	DN Attribute to	o be Added		Common Name (CN)	asa.vpn.e	xam		
Key Pair:	Attribute:	Country (C) 🗸 🗸	Add>>					
Certificate Subject I	N Value: D	Common Name (CN) Department (OU)	Delete					
Generate self-si	gn C	Company Name (O)						
Act as local	cer S	tate (St)						
	E	imail Address (EA)						
Enable CA flag i	nt	ОК	Cancel	Help				
Enable CA flag i	nt				-			
		Add Certificate	Cancel	Help				

Kenmerk	Beschrijving
CN	De naam waardoor de firewall kan worden benaderd (meestal de volledig gekwalificeerde domeinnaam, bijvoorbeeld vpn.example.com).
OU	De naam van uw afdeling binnen de organisatie
0	De wettelijk geregistreerde naam van uw organisatie/bedrijf
С	Landnummer (2-lettercode zonder punctuatie)
ST	De staat waarin uw organisatie is gevestigd.
L	De stad waar uw organisatie zich bevindt.
EA	E-mailadres

N.B.: Geen van de vorige veldwaarden kan een tekenlimiet van 64 tekens overschrijden. Een langere waarde kan problemen opleveren met de installatie van het identiteitscertificaat. Het is ook niet nodig om alle DN-kenmerken te definiëren.

Klik op OK nadat alle kenmerken zijn toegevoegd.

c. Configureer het apparaat FQDN - klik op Advanced.

ssued To	Issued By	Expiry Date		Associated Trustpoints	^1	Usage	Public Key	Туре	Add
Add Identity Certifie	cate							×	Show Deta
Trustpoint Name:	SSL-Trustpoint								Delete
Import the identity	certificate from a file (PK	CS12 format with Ce	rtificate(s)+Priva	ite Kev):					Export
Decryption Passohr	ase:								Install
File to Import From	:		Browse						Re-Enrol
Add a new identity	certificate:								
Key Pair:	SSL-Keypair	~	Show	New					
Certificate Subject	DN: CN=asa.vpn.exa	nple.com	Select						
Generate self-s	igned certificate								
Act as local	certificate authority and	issue dynamic certific	ates to TLS-Pro:	(y					
								_	
			Ad	vanced					
Enable CA flag	in basic constraints exter	nsion							

d. Voer in het veld FQDN de volledig gekwalificeerde domeinnaam in via welke het apparaat via internet toegankelijk is. Klik op OK.

Issued To	Issund Der	Everine Date	Accession Trustasiate	A 1 110000	Public Key Type	Add
Add Identity Ce	ertificate Advanced	Options		×	×	Show Detai
	Enrollment mode	e parameters and SCEP challenge	e password are not available for se	lf-signed certificates.		Delete
Trustpoint Name:	S Certificate Par	ameters Enrollment Mode SC	EP Challenge Password			Export
O Import the ide	entity certifica	asavon example com				Install
Decryption Pas	ssphrase: F-mail:	asavpritexemplet.com				21500
File to Import F	From:					Re-Enrol
Add a new ider	entity certifica	articl as wellow a <b>6</b> kbar day taa				
Key Pair:	S	erial number of the device				
Certificate Sub	oject DN: C					
Generate s	self-signed ce					
Act as	local certifica					
Enable CA	nag in basic i					
			e 1			

- 5. MVO genereren en opslaan
  - a. Klik op Add Certificate (Certificaat toevoegen).

sued To	Issued By	Expiry Date	Associated Trustpoints	^1 Usa	age Public Ke	у Туре	Add
Add Identity Certifi	cate					×	Show Detai
Trustpoint Name:	SSL-Trustpoint						Delete
Import the identity	certificate from a file (PK	CS12 format with Certificate	(s)+Private Key):				Export
Decryption Passphr	ase:						Install
File to Import From	:	Browse					Re-Enrol
Add a new identity	certificate:						
Key Pair:	SSL-Keypair	<ul> <li>✓ Show</li> </ul>	. New				
Certificate Subject	DN: CN=asa.vpn.exam	select.					
Generate self-s	igned certificate						
Act as local	certificate authority and	issue dynamic certificates to	TLS-Proxy			-	
	in hanis constraints outer		Advanced				
	in basic constraints exten	SION					

b. Vervolgens wordt een scherm getoond met het verzoek de CSR op te slaan.

ssued To	Issued By	Expiry Date	Associated Trustpoi	nts ^1	Usage	Public Key Type	Add
Add Identity Certi	ficate					×	Show Details
Trustpoint Name:	SSL-Trustor	pintl					Delete
Import the identit	v certificate from a	file (PKCS12 format with Certifica	te(s)+Private Kev):				Export
Decryption Passp	hrase:				_		Install
File to Import Fro	m:	Identity Certificate Reque	est	×			Re-Enroll
Key Pair: Certificate Subject	SSL-Keypa t DN: CN=asa.vr -signed certificate	request (CSR) and send it to You will then need to install t clicking the Install button in t Save CSR to File:	the CA. he certificate that is returned from he Identity Certificates panel.	b the CA by Browse			
Act as loc	al certificate author	ОК	Cancel Help				
			Advanced	- 1918			
Enable CA fla	g in basic constraints	s extension					

Klik op Browse (Bladeren), selecteer de locatie waar u de CSR wilt opslaan en sla het bestand op met de extensie .txt.

Opmerking: Wanneer het bestand met de extensie .txt wordt opgeslagen, kan het PKCS#10-verzoek worden geopend en bekeken met een teksteditor (zoals Kladblok).

c. Nu wordt het nieuwe trustpoint weergegeven in een hangende staat.

figuration > Device M	anagement > Certifi	<u>cate Management</u> > <u>Iden</u>	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-Enrol

Installeer het Identity Certificate in PEM-formaat met ASDM

De installatiestappen gaan ervan uit dat de CA de CSR heeft ondertekend en een PEM-gecodeerd identiteitscertificaat en CA-certificaatbundel (pem, .cer, .crt) heeft geleverd.

- 1. CA-certificaat installeren dat de CSR heeft ondertekend
  - a. Navigeer naar Configuration > Device Management >Certificate Management > en kies CA-certificaten. Klik op Add (Toevoegen).

onfiguration > Remote Acc	ess VPN > Certificate Mana	igement > <u>CA Certificates</u>				
2						
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	Lonc

b. Voer de naam van het Trustpoint in en selecteer Installeren uit bestand, klik op de knop Bladeren en selecteer het tussenliggende certificaat. U kunt ook het PEM-gecodeerde CA-certificaat vanuit een tekstbestand in het tekstveld plakken.

ssued 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
uoVadis 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:					
1						

Opmerking: Installeer het CA-certificaat dat de CSR heeft ondertekend en gebruik dezelfde naam als het Identity Certificate. De andere CA-certificaten hoger in de PKI-hiërarchie kunnen in afzonderlijke Trust Points worden geïnstalleerd.

c. Klik op Install Certificate (Certificaat installeren).

ssued To	Issued By	Expiry Date	Associated Trustpoints	^1 Usage	Active	Add
enTrust 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:	SSL-Trustpoint					Request CRI
O Install from a files		Province				Delete
Unstall from a file:		browse				
Paste certificate in F	PEM format:					
9LFV52U47em9xX cGqey0MRh3Rs/w 29kqaRijsx153JV/L 0JRyJah/S68Fladku gW3YnHvM08svy dc/CoovO//PAomrAJ END CERTIFIC/ Use EST: Specify source Inter EST URL: https:// Certificate Subject [	MAOGCSqGSIb3DQEBCVUAA4 D25M2vk474724J909(9VCK. k8E90A1athA/fQfK6y-+	BAQarsXIFwK3)NBWOSYN5mgT WodKWQ2yKJUN5SNDU70Ff6f estada estada sedanowi Ise wait Please wait while ASDM is delive device	X INFO: Certificate has Fingerprint: e9ad165c Trustpoint CA certificat	the following attributes: 2673424c 6e7e0c5f b30l te accepted.	94802	
Use SCEP:	connection			ОК		
Specify source Inter	face: None	~		2.0		
SCEP URL: http://						
Retry Period:	1	minutes				

- 2. Installeer het identiteitscertificaat
  - a. Kies het identiteitscertificaat dat eerder tijdens de MVO-generatie is gemaakt. Klik op Install (Installeren).

<u>Conf</u>	quration > Remo	te Ac	cess VPN > Certificate	<u> Management</u> > <u>Identi</u>	ty Certificates			
Is	sued To	^1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
[1	n.example.com]		Not Available	Pending	SSL-Trustpoint	Unknown		Show Details
								Delete
								Export
								Install

Opmerking: het identiteitscertificaat kan per veld zijn afgegeven als niet beschikbaar en het veld Vervaldatum als hangend.

b. Kies een bestand dat het PEM-gecodeerde identiteitscertificaat bevat dat u van de CA hebt ontvangen, of open het PEM-gecodeerde certificaat in een teksteditor en kopieer en plak het door de CA verstrekte identiteitscertificaat in het tekstveld.

sued To	^1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
on.example.com]		Not Available	Pending	SSL-Trustpoint	Unknown		Show Detail
lastall Islandia as				×	General Purpose	RSA (2048 bits)	
Install identity ce	ertifica	ite		A tpoint	General Purpose	RSA (2048 bits)	Delete
entity Certificate							Export
	_						
Install from a file	le:			Browse			
Install from a file	le:			Browse			Install
<ul> <li>Install from a fil</li> <li>Paste the certification</li> </ul>	le: ficate d	ata in base-64 forma	t:	Browse			Install
Install from a fil     Paste the certifi	le: ficate d	ata in base-64 forma	t:	Browse			Install Re-Enroll
Install from a fil     Paste the certifi	le:	ata in base-64 forma	tı	Browse			Install Re-Enroll
Install from a fil     Paste the certifi	le:	ata in base-64 forma	tı	Browse			Install Re-Enroll
Install from a fil     Paste the certifi	le:	ata in base-64 forma	tı	Browse			Install Re-Enroll
Install from a fil     Paste the certifi	le:	ata in base-64 forma	tı	Browse			Install Re-Enroll
Install from a fil     Paste the certif	le:	ata in base-64 forma	t:	Browse			Install Re-Enroll

Opmerking: identiteitscertificaat kan worden geïnstalleerd in .pem, .cer, .crt formaat.

c. Klik op Install Certificate (Certificaat installeren).

sued To ^1 Issued By	y Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
on.example.com] Not Availa	able Pending	SSL-Trustpoint	Unknown		Show Details
		×	General Purpose	RSA (2048 bits)	Show De tall
Install Identity certificate			General Purpose	RSA (2048 bits)	Delete
dentity Certificate	🔁 Please wait	×			Export
Install from a file:	_	Information	×		Install
Paste the certificate data in ba InNBJ26XgDmVUQjfBEMVXR2K Gyer3x2GXML7MAIHBptyMcHD T8y9Yia7poqMnamQkaQpCAF KdNqFbUr6VW9NTUF2DowH3 END CERTIFICATE <	evice	envering tr	oort succeeded.		Re-Enroll

3. Bind het nieuwe certificaat aan Interface met ASDM

ASA moet worden geconfigureerd om het nieuwe identiteitscertificaat te gebruiken voor WebVPN-sessies die eindigen op de gespecificeerde interface.

- a. Ga naar Configuration > Remote Access VPN > Advanced > SSL Settings (Configuratie > VPN voor externe toegang > Geavanceerd > SSL-instellingen).
- b. Selecteer onder Certificates (Certificaten) de interface waarop WebVPN-sessies moeten eindigen. In dit voorbeeld wordt de buiteninterface gebruikt.

Klik op Edit (Bewerken).

c. Kies in de vervolgkeuzelijst Certificate (Certificaat) het nieuw geïnstalleerde certificaat.

- Comun		eer oncore			Edit
					Delete
	Select SSL Certificate		×		
	Specify enrolled trustpoints to be u OUTSIDE-direct interface. To enrol	sed for SSL authentication and VPN load balancing on the a trustpoint, go to Device Management > Certificate			
rtificates	Management > Identity Certificate:	S.			
Specify which certificates, if ar	Primary Enrolled Certificate:	SSI -TrustopintruptructuredName -asswop exampl	e	es not associated with a certificate of their of	wn.
Interface	Lond Delension Secolled Contiference			Кеу-Туре	Edit
OUTSIDE-direct	Load balancing Enrolled Certificate:	None	~		
inside	OK	Cancel Help			
inside-vlan		Concer Thep			
management					
allback Certificate:	None	~			

- d. Klik op OK.
- e. Klik op Apply (Toepassen).

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

Nu wordt het nieuwe identiteitsbewijs gebruikt.

## Installeer een Identity Certificate dat is ontvangen in PKCS 12formaat met ASDM

Het PKCS12-bestand (.p12- of .pfx-formaat) bevat identiteitsbewijs, sleutelpaar en CAcertificaat(en). Het wordt gemaakt door de CA, bijvoorbeeld in het geval van wildcard certificaat, of geëxporteerd van een ander apparaat. Het is een binair bestand, kan niet worden bekeken met teksteditor.

1. Installeer de Identity en CA-certificaten uit een PKCS12-bestand

Het identiteitsbewijs, CA-certificaat(en) en sleutelpaar moeten worden gebundeld in één PKCS12-bestand.

- a. Navigeer naar Configuratie > Apparaatbeheer > Certificaatbeheer en kies Identity Certificates.
- b. Klik op Add (Toevoegen).
- c. Geef een naam op bij Trustpoint Name (Naam van vertrouwenspunt).

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Detail
Add Identity Certific	ate		×			Delete
Trustpoint Name:	SSL-Trustpoint-PKG	C\$12				Export
<ul> <li>Import the identity of</li> </ul>	certificate from a file (PK	CS12 format with Certificate(s	:)+Private Key):			Install
Decryption Passphra	ase:					Re-Enrol
File to Import From:		Browse				
O Add a new identity of	certificate:					
Key Pair:	<default-rsa-key< td=""><td>/&gt; Show</td><td>New</td><td></td><td></td><td></td></default-rsa-key<>	/> Show	New			
Certificate Subject D	ON: CN=risavpn31	Select				
Generate self-si	gned certificate					
Act as local	certificate authority and	issue dynamic certificates to T	LS-Proxy			
			Advanced			
Nenable CA flag in	n basic constraints exten	sion				
45						

d. Klik op het keuzerondje Import the identity certificate from a file (Identiteitscertificaat importeren uit een bestand).

Issued To	Issued By	Exp	iry Date	Associated	Trustpoints	Usage	Public Key	Туре	Add
									Show Detail
Table Add Identity C	Certificate			(	×				Delete
Trustooint Name	SSI -Trustopint-	PKCS12	~		import ID certi	ficate file			
Import the id	entity certificate from a file (	PKCS12 forma	t with Certificate(c)+P	rivate Kev):	Look in:	Document	ts	<ul> <li>Image: state of the state of th</li></ul>	<b></b>
Decruption P	accobrace:	rico 12 forme		ivate key).	0	CSR.txt			
Ele to Import	Erom		Provine		E I	🦻 vpn.exan	ple.com.pfx		
			browse		Recent Items				
O Add a new id	entity certificate:			_					
Key Pair:	<default-rsa-< td=""><td>(ey&gt;</td><td>Show</td><td>New</td><td>Desktop</td><td></td><td></td><td></td><td></td></default-rsa-<>	(ey>	Show	New	Desktop				
Certificate Su	ubject DN: CN=risavpn31		Select		4-				
Generate	self-signed certificate				Documents				
Act a	s local certificate authority a	nd issue dynar	mic certificates to TLS-P	roxy					
					This PC F	ile name:	vpn.example.com.pfx	Import	D certificate file
				Advanced	- 🎿 F	Files of type:	All Files	~	Cancel
Enable C	A flag in basic constraints ext	tension			4				
	Add Certificate	Cancel	Help	1					

e. Geef bij Decryption Passphrase (Wachtwoord voor ontsleuteling) het wachtwoord op dat is gebruikt om het PKCS12-bestand te maken.

ssued To	Issued By	Expiry Da	te	Associated Trustpoints	Usage	Public Key Type	Add
							Show Detail
🗧 Add Identity Ce	rtificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-F	PKCS12					Export
<ul> <li>Import the ider</li> </ul>	ntity certificate from a file (F	PKCS12 format with	Certificate(s)+Pr	ivate Key):			Install
Decryption Pas	sphrase: ••••						Re-Enroll
File to Import F	rom: C:\Users\cisco.E	DESKTOP-R2CH8G	Browse				
O Add a new ider	ntity certificate:						
Key Pair:	<default-rsa-k< td=""><td>(ey&gt; 🗸</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-k<>	(ey> 🗸	Show	New			
Certificate Subj	ect DN: CN=risavpn31		Select				
Generate s	elf-signed certificate						
Act as I	ocal certificate authority an	nd issue dynamic cer	tificates to TLS-P	roxy			
				Advanced			
Enable CA	flag in basic constraints ext	rension					
	ing in pase constants exe						

f. Klik op Add Certificate (Certificaat toevoegen).

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
		,				Show Detail
add Identity C	ertificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-F	PKCS12				Export
Import the ide	entity certificate from a file (i	PKCS12 format with Certificate(	s)+Private Key):			Install
Decryption Pa	assphrase: ••••		100000			Re-Enroll
File to Import	From: C:\Users\cisco.E	DESKTOP-R2CH8G Browse.				
🔿 Add 📮 Ple	ease wait		[] Information			×
Certi 🔟	Please wait while ASDM device	is delivering the command(s) to	the Created trustroin	ts for CAs biober in the bio	erarchy as the CA certificate was not s	elf-signed.
_ < 🚩						
C.		-	WARNING: CA ce the validation-usa	rtificates can be used to va age of this trustpoint to limi	alidate VPN connections,by default. Ple it the validation scope, if necessary	ease adjust
Enable CA	A flag in basic constraints ext	tension	Import PKCS 12 op	peration completed success	sfully.	

Opmerking: Wanneer u een PKCS12 met CA-certificatenketen importeert, creëert de ASDM automatisch de upstream CA-trustpoints met namen met een -

onfiguration > Remote Access VPN > Certificate Management > <u>CA Certificates</u>									
Issued To	√ <sup>1</sup> 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				
	CHUR L CA		001 DK0040 D	e: 1	14				

2. Bind het nieuwe certificaat aan Interface met ASDM

ASA moet worden geconfigureerd om het nieuwe identiteitscertificaat te gebruiken voor WebVPN-sessies die eindigen op de gespecificeerde interface.

a. Ga naar Configuration > Remote Access VPN > Advanced > SSL Settings

(Configuratie > VPN voor externe toegang > Geavanceerd > SSL-instellingen).

b. Selecteer onder Certificates (Certificaten) de interface waarop WebVPN-sessies moeten eindigen. In dit voorbeeld wordt de buiteninterface gebruikt.

Klik op Edit (Bewerken).

c. Kies in de vervolgkeuzelijst Certificate (Certificaat) het nieuw geïnstalleerde certificaat.

- Comon	Germea	ne	
ertificates Specify which certificates, if ar Interface OUTSIDE-direct inside inside -vlan management	Select SSL Certificate Specify enrolled trustpoints to be used for SSL authentication and VPN OUTSIDE-direct interface: OUTSIDE-direct Primary Enrolled Certificate: SSL-Trustpoint-PKCS12:unstructh Load Balancing Enrolled Certificate: None OK Cancel Help	V load balancing on the ement > Certificate uredName=FTD72-ek, u v key-Type	own.
Fallback Certificate:	None	v 2. minutae	

- d. Klik op OK.
- e. Klik op Apply (Toepassen).

Cert Sp	ificates ecify which certificates, if any, should be	used for SSL authentication on each interface. Ti	he fallback certificate will be used on interfaces not assoc	iated 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	

Nu wordt het nieuwe identiteitsbewijs gebruikt.

## Certificaat-verlenging

## Verleng een certificaat dat is ingeschreven met aanvraag voor certificaatondertekening (CSR) met ASDM

Certificaatverlenging van CSR-ingeschreven certificaat vereist om een nieuw Trustpoint te creëren en in te schrijven. Het moet een andere naam hebben (bijvoorbeeld oude naam met jaarachtervoegsel inschrijven). Het kan dezelfde parameters en sleutelpaar gebruiken als het oude certificaat, of verschillende.

Genereert een CSR met ASDM

1. Maak een nieuw Trustpoint met een specifieke naam.

a. Blader naar Configuratie > Apparaatbeheer > Certificaatbeheer > Identity Certificates.



- b. Klik op Add (Toevoegen).
- c. Definieer een trustpoint naam.

ued To	^1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type		Add
tructuredName=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
<ul> <li>Import the identity certif</li> </ul>	ficate from a file (PKC	S12 format with Certificate(s)+Priva	te Key):					Install
Decryption Passphrase:								Re-Enrol
File to Import From:	<u>.</u>	Browse						
O Add a new identity certif	ficate:							
Key Pair:	<default-rsa-key:< td=""><td>&gt; Show</td><td>New</td><td></td><td></td><td></td><td></td><td></td></default-rsa-key:<>	> 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					
			inerad				F	
🗹 Enable CA flag in bas	sic constraints extens	ion	/dilucu					

- d. Klik op het keuzerondje Add a new identity certificate (Voeg een nieuw identiteitscertificaat toe).
- 2. (Optioneel) Maak een nieuw sleutelpaar

Opmerking: standaard wordt de RSA-toets met de naam Default-RSA-Key en een grootte van 2048 gebruikt. Het wordt echter aanbevolen om voor elk Identity Certificate een uniek privaat/publiek sleutelpaar te gebruiken.

a. Klik op Nieuw om een nieuw sleutelpaar te genereren.

sued to Issued	By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
structuredName= CN=ca	ructuredName= CN=ca.example.com, OU 15:10:00 C		ST Feb 6 2024 SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detail
a Add Identity Certificate				×			Delete
Trustpoint Name:	SSL-Trustpoint-202	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	iificate:						
Key Pair:	<default-rsa-key< td=""><td>&gt; ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-key<>	> ~	Show	New			
Certificate Subject DN:	CN=asavpn.examp	ole.com	Select				
Generate self-signe	d certificate						
Act as local cert	tificate authority and i	issue dynamic cer	tificates to TL	S-Proxy			
				Advanced			
_		sion					

- b. Kies de optie Voer een nieuwe naam in voor het sleutelpaar en voer een naam in voor het nieuwe sleutelpaar.
- c. Selecteer RSA of ECDSA bij Key Type (Sleuteltype).
- d. Kies de sleutelgrootte; voor RSA, kies algemeen doel voor Gebruik.
- e. Klik op Generate Now (Nu genereren). Het sleutelpaar wordt nu gecreëerd.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredNam	e= CN=ca.example.com	, OU 15:10:00 CEST Feb 6 20	024 SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
🧧 Add Identi	ty Certificate		×			Delete
Trustpoint Na	me: SSL-Trusto	oint-2023				Export
C 🔽 Add	Key Pair		× <sub>Key):</sub>			Install
Key Ty	rpe: 🖲 RSA	O ECDSA	EDDSA			Re-Enroll
	0.000					
( Name:	Ouse default key pa	r name	814			
Size:	4096	~				
Usage	General purpose	Special				
	Concepto Nov	Consel	iced			

3. Selecteer de naam van het sleutelpaar

Kies het sleutelpaar om de MVO te ondertekenen met, en te worden gebonden aan het nieuwe certificaat.

ISSUED TO ISS	sued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName= CN	=ca.example.com, OU	15:10:00 CEST Feb 6 2024	4 SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🗧 Add Identity Certific	cate		×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23				Export
O Import the identity	certificate from a file (PK	CS12 format with Certificate	e(s)+Private Key):			Install
Decryption Passphr	ase:					Re-Enroll
File to Import From:	:	Browse				
Add a new identity	certificate:					
Key Pair:	SSL-KeyPair-2023	✓ Show.	New			
Certificate Subject	DN: CN=asavpn.exam	ple.com Select.				
Generate self-s	igned certificate					
Act as local	certificate aut grity and	issue dynamic certificates to	o TLS-Proxy			
			Advanced			

4. Configureer het certificaatonderwerp en de volledig gekwalificeerde domeinnaam (FQDN)

Waarschuwing: de FQDN-parameter moet overeenkomen met de FQDN of het IPadres van de ASA-interface waarvoor het certificaat wordt gebruikt. Deze parameter stelt de alternatieve onderwerpnaam (SAN) voor het certificaat in. Het SAN-veld wordt gebruikt door SSL/TLS/IKEv2-client om te controleren of het certificaat overeenkomt met de FQDN waarmee verbinding is gemaakt.

Opmerking: CA kan de FQDN- en onderwerpnamen die in het trustpoint zijn gedefinieerd, wijzigen wanneer het de CSR ondertekent en een ondertekend identiteitscertificaat aanmaakt.

a. Klik op Selecteren.

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 C	ertificate			×			Delete
Trustpoint Name:	Trustpoint Name: SSL-Trustpoint-2023					Export	
O Import the ide	entity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Pa	ssphrase:						Re-Enroll
File to Import	From:		Browse				
Add a new ide	entity certificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate Sul	bject DN: CN=asavpn.exam	ple.com	Select				
Generate	self-signed certificate						
Act as	local certificate authority and	issue dynamic ce	tificates to TL	S-Proxy			
				Advanced			
Enable CA	A flag in basic constraints exter	nsion		Advarced			

b. Configureer in het venster CertificaatonderwerpDN de certificaatkenmerken - selecteer attribuut uit de vervolgkeuzelijst, voer de waarde in en klik op Toevoegen.

Issued To	Issued By	Expiry	Date	Associated Trustpoints	Usage	Public Key Type	Add
instructuredName	e= CN=ca.example.com	n, OU 15:10:	00 CEST Feb 6 2024	T Feb 6 2024 SSL-Trustpoint		rpose RSA (2048 bits)	Show Details
🔄 Add Identit	y Certificate			×			Delete
Trustpoint Na	me: SSL-Trust	point-2023	_	-			Export
Certificate Subje	ct DN				×		Install
							Re-Enroll
			Attribute Common Name (CN	Value			
Attribute: C	be Added ountry (C) v	Add>>	Company Name (O	) example inc			
Value: US	\$	Delete					
	OK	Cance	l Help				
	e CA flag in basic constrair	nts extension					

Kenmerk	Beschrijving
CN	De naam waardoor de firewall kan worden benaderd (meestal de volledig gekwalificeerde domeinnaam, bijvoorbeeld vpn.example.com).
ου	De naam van uw afdeling binnen de organisatie
ο	De wettelijk geregistreerde naam van uw organisatie/bedrijf
С	Landnummer (2-lettercode zonder punctuatie)
ST	De staat waarin uw organisatie is gevestigd.
L	De stad waar uw organisatie zich bevindt.
EA	E-mailadres

N.B.: Geen van de vorige velden kan een waarde van 64 tekens overschrijden. Een langere waarde kan problemen opleveren met de installatie van het identiteitscertificaat. Het is ook niet nodig om alle DN-kenmerken te definiëren.

Klik op OK nadat alle kenmerken zijn toegevoegd.

c. Om apparaat FQDN te configureren klikt u op Geavanceerd.

sued to Issued	By	Expiry Date		Associated Trustpoint	s Usage		Public Key Type	Add
structuredName= CN=ca	.example.com, OU	15:10:00 CEST	Feb 6 2024	SSL-Trustpoint	Ger	eral Purpose	RSA (2048 bits)	Show Detail
🔄 Add Identity Certificate				×				Delete
Trustpoint Name:	SSL-Trustpoint-20	23						Export
O Import the identity cert	tificate 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	tificate:							
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	tificate authority and	issue dynamic cer	tificates to TL	S-Proxy -				
				Advanced				
Enable CA flag in ba	asic constraints exter	sion						

d. Voer in het veld FQDN de volledig gekwalificeerde domeinnaam in via welke het apparaat via internet toegankelijk is. Klik op OK.

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
Advanced (	Ontions	NOLL 15-10-00 CEST SAL 6 T	024 SSI Tructoriat	General Purpose	RSA (2048 bits)	Show Detail
						Delete
Certificate Par	ameters and SCEP cha	SCEP Challenge Password	e for self-signed certificates.			Export
		Sectional and a section of a				Install
FQDN:	asavpn.example.com					Re-Enroll
E-mail:						C
IP Address:						
	erial number of the device					
		2				

- 5. MVO genereren en opslaan
  - a. Klik op Add Certificate (Certificaat toevoegen).

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName	e= CN=ca.example.com, OU	15:10:00 CEST Feb 6 202	24 SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🔄 Add Identit	y Certificate		×			Delete
Trustpoint Nar	me: SSL-Trustpoint-20	23				Export
O Import the	e identity certificate from a file (PK	CS12 format with Certificat	te(s)+Private Key):			Install
Decryption	n Passphrase:					Re-Enroll
File to Imp	port From:	Brows	e			
Add a new	videntity certificate:					
Key Pair:	SSL-KeyPair-2023	Show	New			
Certificate	Subject DN: /pn.example.com	,O=example inc Select	t			
Genera	ate self-signed certificate					
Ac	t as local certificate authority and	issue dynamic certificates	to TLS-Proxy			
			Advanced			
Enable	e CA flag in basic constraints exter	nsion				
Enable	e CA flag in basic constraints exter	nsion				

b. Vervolgens wordt een scherm getoond met het verzoek de CSR op te slaan.

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
Trustooint Name	SSI -Trustopint-20	23				Export
Import the id	dentity certificate from a file (PK	CS12 format with Certificate(s	)+Private Key):			Install
( martine	in California Barran		~			Re-Enrol
F	ity Certificate Request		^			
To com     request	plete the enrollment process, pl t (CSR) and send it to the CA.	lease save the PKCS 10 enrollm	ent			
K You will clicking C	then need to install the certification the Install button in the Identit	ate that is returned from the C y Certificates panel.	A by			
[ Save C	SR to File: C:\Users\cisco.DES	KTOP-R2CH8G5\Docun Br	owse			
	or c	ancol Holo				
6	OK C	ancer nep				
			Advanced			
	A flag in basic constraints exter	nsion				

Klik op Bladeren. Kies een locatie waar u de CSR wilt opslaan en sla het bestand op met de extensie .txt.

Opmerking: Wanneer het bestand met de extensie .txt wordt opgeslagen, kan het PKCS#10-verzoek worden geopend en bekeken met een teksteditor (zoals Kladblok).

c. Nu wordt het nieuwe trustpoint weergegeven in een hangende staat.

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 Detail
asavpn.example.com]	Not Available	Pending	SSL-Trustpoint-2023	Unknown		
						Delete
						Export
						Install
						Re-Enroll
						-

Installeer het identiteitscertificaat in PEM-formaat met ASDM

De installatiestappen gaan ervan uit dat de CA de CSR heeft ondertekend en een PEM-gecodeerd pakket (.pem, .cer, .crt) heeft geleverd met een nieuw identiteitscertificaat en CA-certificaatbundel.

1. CA-certificaat installeren dat de CSR heeft ondertekend

Het CA-certificaat dat het Identity Certificate heeft ondertekend, kan worden geïnstalleerd in het Trustpoint dat voor Identity Certificate is gecreëerd. Als het Identity Certificate is ondertekend door een bemiddelende CA, kan dit CA-certificaat worden geïnstalleerd in het Identity Certificate Trustpoint. Alle CA-certificaten stroomopwaarts in de hiërarchie kunnen worden geïnstalleerd in afzonderlijke CA Trustpoints.

a. Navigeer naar Configuration > Device Management >Certificate Management > en kies CA-certificaten. Klik op Add (Toevoegen).

^ 1     Expiry Date     Associated Trustpoints     Usage     Active     Add       com, OU=I     15:10:00 CEST Feb 6 2030     SSL-Trustpoint     General Purpose     Yes     Edit       vot CA 2,     19:23:33 CEST Nov 24 2031     SmartCallHome_ServerCA2     General Purpose     No     Edit	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       uovadia Root CA 2     CN=QuoVadis Root CA 2,     19:23:33 CEST Nov 24 2031     _SmartCalHome_ServerCA2     General Purpose     No       denTrust Commercial Root     CN=IdenTrust Commercial     19:12:23 CEST Jan 16 2034     _SmartCalHome_ServerCA     General Purpose     No							
com, OU=I 15:10:00 CEST Feb 6 2030 SSL-Trustpoint General Purpose Yes Edit ob CA 2, 19:23:33 CEST Nov 24 2031 _SmartCallHome_ServerCA2 General Purpose No Demorphile 19:12:32 CEST 10: 16:23:44 - SmartCallHome_ServerCA Convertiged Directory No	a.example.com CN=ca.example.com, OU=I 15:10:00 CEST Feb 6 2030 SSL-Trustpoint General Purpose Yes Edit QuoYadis Root CA 2 CN=QuoYadis Root CA 2, 19:23:33 CEST Nov 24 2031 _SmartCallHome_ServerCA2 General Purpose No Show Details denTrust Commercial Root CN=IdenTrust Commercial 19:12:23 CEST Jan 16 2034 _SmartCallHome_ServerCA General Purpose No Show Details Reourest CRI	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active	Add
bot CA 2, 19:23:33 CEST Nov 24 2031 _SmartCallHome_ServerCA2 General Purpose No	QuoVadis Root CA 2       CN=QuoVadis Root CA 2,       19:23:33 CEST Nov 24 2031       _SmartCallHome_ServerCA2       General Purpose       No         denTrust Commercial Root       CN=IdenTrust Commercial       19:12:23 CEST Jan 16 2034       _SmartCallHome_ServerCA       General Purpose       No         Show Details         Request CRI	a.example.com	CN=ca.example.com, OU=I	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes	Edit
mmercial 19:12:23 CEST lan 16 2034 SmartCallHome ServerCA General Purpose No.	denTrust Commercial Root CN=IdenTrust Commercial 19:12:23 CEST Jan 16 2034 Show Detail: Show Detail: Request CR	QuoVadis Root CA 2	CN=QuoVadis Root CA 2,	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	Cuit
Show Detail	Request CR	denTrust Commercial Root	CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Show Deta
	R	ioVadis Root CA 2 enTrust Commercial Root	CN=QuoVadis Root CA 2, CN=IdenTrust Commercial	19:23:33 CEST Nov 24 2031 19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA2 _SmartCallHome_ServerCA	General Purpose General Purpose	No No	SI
								Delete

b. Voer de naam van Trustpoint in en kies Installeren uit bestand, klik op Bladeren knop en kies het tussenliggende certificaat. U kunt ook het PEM-gecodeerde CA-certificaat vanuit een tekstbestand in het tekstveld plakken.

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
Trustpoint Name:	SSL-Trustpoint-2023	1				Show Detai
<ul> <li>Install from a file</li> </ul>	:	Browse				Delete

Opmerking: Installeer het tussentijdse certificaat met dezelfde vertrouwenspuntnaam als de vertrouwenspuntnaam van het identiteitsbewijs,

indien het identiteitsbewijs is ondertekend door een tussenliggend CA-certificaat.

c. Klik op Install Certificate (Certificaat installeren).

sued To	Issued By	∧ <sup>1</sup> Expiry Date		Associated Trustpoints	Usage		Active		Add
.example.com	CN=ca.example.com, Ol	J=l 15:10:00 CES	T Feb 6 2030	SSL-Trustpoint	Genera	l Purpose	Yes		Edit
Install Certificate								×	Show Detail
Trustpoint Name: SS	L-Trustpoint-2023								Request CR
O Install from a file:		Browse							Delete
Paste certificate in PEN	1 format:								
VR0088YEFE35k2sbra 9tLFV52U47em9Xx4M cGqey0MM5x35k,Mov 2RyaqRijsx153yV/Lk8 0RyajaH568FladAvc7x gW8YnHOMM08vy72x dcVcov0/PAxmAJ+N END CERTIFICATE O Use EST: Specify source Interfax EST LIBL: https://	969ELFV32U47em9uXaM NoCCSq0SIb3CQEBcwUy ByoukaF44V219N9gK (199AItanA/fQfx6V+H7 RddtVxYB9sfEbFIN8oc 1Jf0UCdm4V+G0gh 22/WFN3MXW2O453C	38GA LUdiwQYMBAA AAdBAOArsXIEwK3 Information	FE55kZsbra9b NBwOsYh5maT D: Certificate has erprint: e9ad165 stpoint CA certific	the following attributes: ic 2673424c 6e7e0c5f b30b4a02 iate accepted.	×			~	
Certificate Subject DN:	CN=risavon31								
allow-untrusted-co	nnection			OK					
Use SCEP:									
Specify source Interfac	e: None	~							
SCEP URL: http://									
Retry Period:	1	minut	es						

In het voorbeeld wordt het nieuwe certificaat ondertekend met hetzelfde CA-certificaat als het oude. Hetzelfde CA-certificaat is nu gekoppeld aan twee Trustpoints.

Edit
Luit
Show Deta
Decuse of
Request G

- 2. Installeer het identiteitscertificaat
  - a. Kies het identiteitscertificaat dat eerder met de MVO-generatie is gemaakt. Klik op Install (Installeren).

onfiguration > Device	e Management > Certifica	ate Management > Identit	ty Certificates				
Issued To	Issued By	Expiry Date	Associated Trustpoints	~ 1	Usage	Public Key Type	Add
unstructuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Details
[asavpn.example.com]	Not Available	Pending	SSL-Trustpoint-2023		Unknown		
							Delete
							Export
							Install
							Re-Enroll

Opmerking: het identiteitscertificaat kan per veld zijn afgegeven als niet beschikbaar, en het veld Vervaldatum als hangend.

b. Kies een bestand dat het PEM-gecodeerde identiteitscertificaat bevat dat u van de CA hebt ontvangen, of open het PEM-gecodeerde certificaat in een teksteditor en kopieer en plak het door de CA verstrekte identiteitscertificaat naar het tekstveld.

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
avpn.example.c	om] Not Available	Pending	SSL-Trustpoint-2023		Unknown		Dalata
							Delete
							Export
🛓 Install Identi	ty certificate		×				Install
entity Certifica	te						Re-Enrol
Install from	a flat		Province				
			browse				
O Paste the o	ertificate data in base-64 format						

Opmerking: identiteitscertificaat kan worden geïnstalleerd in .pem, .cer, .crt formaat.

c. Klik op Install Certificate (Certificaat installeren).

	1000000)	Expiry Date	Associated Trustpoints	~1	Usage	Public Key Type	Add
tructuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detail
avpn.example.com]	Not Available	Pending	SSL-Trustpoint-2023		Unknown		Delete
							Export
Install Identity ce	rtificate		×				Install
lentity Certificate —							Re-Enroll
	wait						
• Pa	i Informa	tion	×				
H G E	Please wait wł device		. 1				
j 🌄	4	Certificate import succeede	d.				
W							
		OK					

Na de installatie zijn er oude en nieuwe identiteitsbewijzen aanwezig.

issued To	Issued By	Expiry Date	Associated Trustpoints	~ <b>1</b>	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)	Show beta
							Delete
							Export
							Install

3. Bind het nieuwe certificaat aan Interface met ASDM

ASA moet worden geconfigureerd om het nieuwe identiteitscertificaat te gebruiken voor WebVPN-sessies die eindigen op de gespecificeerde interface.

- a. Ga naar Configuration > Remote Access VPN > Advanced > SSL Settings (Configuratie > VPN voor externe toegang > Geavanceerd > SSL-instellingen).
- b. Selecteer onder Certificates (Certificaten) de interface waarop WebVPN-sessies moeten eindigen. In dit voorbeeld wordt de buiteninterface gebruikt.

Klik op Edit (Bewerken).

c. Kies in de vervolgkeuzelijst Certificate (Certificaat) het nieuw geïnstalleerde certificaat.

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

- d. Klik op OK.
- e. Klik op Apply (Toepassen). Nu wordt het nieuwe identiteitsbewijs gebruikt.

		1		
				Edit
ficates ecify which certificates, if ar Interface	y, should be used for SSL authentication on ea Primary Certificate	ach interface. The fallback certificate will be u Load Balancing Certificate	sed on interfaces not associated with a certificate of their own. Key-Type	Edit
ficates ecify which certificates, if ar Interface OUTSIDE-direct	y, should be used for SSL authentication on ea Primary Certificate SSL=Trustpoint=2023;unstructure	ach interface. The fallback certificate will be us 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	y, should be used for SSL authentication on ea Primary Certificate SSL-Trustpoint-2023:unstructure	ach 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-direct inside inside-vlan	y, should be used for SSL authentication on ea Primary Certificate SSL-Trustpoint-2023:unstructure.	ach 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

## Verleng een certificaat dat is ingeschreven voor PKCS 12bestand met ASDM

Certificaat verlenging van PKCS12 ingeschreven certificaat vereist om een nieuw Trustpoint te maken en in te schrijven. Het moet een andere naam hebben (bijvoorbeeld oude naam met jaarachtervoegsel inschrijven).

Het PKCS12-bestand (.p12- of .pfx-formaat) bevat identiteitsbewijs, sleutelpaar en CAcertificaat(en). Het wordt gemaakt door de CA, bijvoorbeeld in het geval van wildcard certificaat, of geëxporteerd van een ander apparaat. Het is een binair bestand en kan niet worden weergegeven met de teksteditor.

1. Installeer het vernieuwde identiteitscertificaat en CA-certificaten uit een PKCS12-bestand

Het identiteitsbewijs, CA-certificaat(en) en sleutelpaar moeten worden gebundeld in één PKCS12-bestand.

- a. Navigeer naar Configuratie > Apparaatbeheer > Certificaatbeheer en kies Identity Certificates.
- b. Klik op Add (Toevoegen).
- c. Geef een nieuwe Trustpoint naam op.

Issued To	Issued By	Expiry	Date	Associated Trustpoints	Usage	Public Key Type	Add
							Show Detail
🔁 Add Identity C	ertificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-	PKCS12					Export
Import the id	entity certificate from a file (	PKCS12 format v	vith Certificate(s)+P	rivate Key):			Install
Decryption Pa	assphrase:						Re-Enroll
File to Import	From:		Browse				
O Add a new id	entity certificate:						
Key Pair:	<default-rsa-h< td=""><td>(ey&gt;</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-h<>	(ey>	Show	New			
Certificate Su	bject DN: CN=risavpn31		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		Auvanceum			

d. Klik op het keuzerondje Import the identity certificate from a file (Identiteitscertificaat importeren uit een bestand).

ssued To	Issued By	Expiry Da	ite	Associated	Trustpoints	Usage	P	ublic Key Type		Add
										Show Detai
🧧 Add Identity Cerl	tificate		L.	(	×					Delete
Trustpoint Name: () Import the ident Decryption Pass	SSL-Trustpoint-P tity certificate from a file (P phrase:	KCS12 KCS12 format with	n Certificate(s) +P	rivate Key):	Look in:	ficate file Documen CSR.txt ypn.exan	is	~	🗊 🗈 🖽 -	
File to Import Fr	om: ity certificate:		Browse		Recent Items					
Key Pair:	<default-rsa-k< td=""><td>ey&gt; 🗸</td><td>Show</td><td>New</td><td>Desktop</td><td></td><td></td><td></td><td></td><td></td></default-rsa-k<>	ey> 🗸	Show	New	Desktop					
Certificate Subje	ect DN: CN=risavpn31		Select		<u>A-</u>					
Generate se	If-signed certificate				Documents					
Act as lo	cal certificate authority an	d issue dynamic ce	rtificates to TLS-f	Proxy						
				Advanced	This PC	File name:	vpn.example.com	pfx	Import ID c	ertificate file
Enable CA fl	ag in basic constraints exte	ension				nies of type:	All Files	~	Ca	ncel

e. Geef bij Decryption Passphrase (Wachtwoord voor ontsleuteling) het wachtwoord op

dat is gebruikt om het PKCS12-bestand te maken.

ssued To	Issued By	Expiry Da	te	Associated Trustpoints	Usage	Public Key Type	Add
							Show Detail
🔁 Add Identity Certifi	cate			×			Delete
Trustpoint Name:	SSL-Trustpoint-P	KCS12					Export
<ul> <li>Import the identity</li> </ul>	certificate from a file (P	KCS12 format with	Certificate(s)+Pr	rivate Key):			Install
Decryption Passph	rase: ••••						Re-Enroll
File to Import From	: C: \Users\cisco.D	ESKTOP-R2CH8G	Browse				
Add a new identity	certificate:						
Key Pair:	<default-rsa-k< td=""><td>ey&gt; v</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-k<>	ey> v	Show	New			
Certificate Subject	DN: CN=risavpn31		Select				
Generate self-	signed certificate						
Act as local	certificate authority an	d issue dynamic ce	tificates to TLS-P	roxy			
				A down and			
	ia hania anastraiata aut			Advanced			
	in basic constraints exte	ension					

f. Klik op Add Certificate (Certificaat toevoegen).

issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
🔁 Add Identity (	Certificate		×			Delete
Trustpoint Name	: SSL-Trustpoint-	PKCS12				Export
<ul> <li>Import the id</li> </ul>	lentity certificate from a file (	PKCS12 format with Certificate	(s) +Private Key):			Install
Decryption P	assphrase: ••••					Re-Enroll
File to Import	t From: C:\Users\cisco.0	DESKTOP-R2CH8G Browse				
🔿 Add 🗧 Pl	lease wait					×
Certi	Please wait while ASDM device	is delivering the command(s) to	Treated trustpoin WARNING: CA cer the validation-usa	ts for CAs higher in the hie tificates can be used to va ge of this trustpoint to limit eration completed success	rarchy as the CA certificate was not s alidate VPN connections, by default. Pk t the validation scope, if necessary sfully.	elf-signed.

Opmerking: Wanneer een PKCS12 met CAs-certificaatketen wordt geïmporteerd, creëert de ASDM automatisch de upstream CAs trustpoints met namen met een - nummer achtervoegsel.

onfiguration > Remote Access VPN > Certificate Management > <u>CA Certificates</u>											
Issued To	~ <b>1</b>	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 het nieuwe certificaat aan Interface met ASDM

ASA moet worden geconfigureerd om het nieuwe identiteitscertificaat te gebruiken voor WebVPN-sessies die eindigen op de gespecificeerde interface.

- a. Ga naar Configuration > Remote Access VPN > Advanced > SSL Settings (Configuratie > VPN voor externe toegang > Geavanceerd > SSL-instellingen).
- b. Selecteer onder Certificates (Certificaten) de interface waarop WebVPN-sessies moeten eindigen. In dit voorbeeld wordt de buiteninterface gebruikt.

Klik op Edit (Bewerken).

c. Kies in de vervolgkeuzelijst Certificate (Certificaat) het nieuw geïnstalleerde certificaat.

- Comain	our unicove	
rtificates Specify which certificates, if ar Interface OUTSIDE-direct Inside Inside-vlan management	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  Interface: OUTSIDE-direct Primary Enrolled Certificate: SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u v Load Balancing Enrolled Certificate: None OK Cancel Help	n. Edit
Fallback Certificate: Forced Certification Authentica	None      z      tion Timeout:         2 minutes	

- d. Klik op OK.
- e. Klik op Apply (Toepassen).

0	ertificates Specify which certificates, if any, should be	e used for SSL authentication on each interface. T	he fallback certificate will be used on interfaces not assoc	ciated with a certificate of their own.	
	Interface	Primary Certificate	Load Balancing Certificate	Кеу-Туре	Edit
	OUTSIDE-direct	${\tt SSL-Trustpoint-PKCS12:} unstructured {\tt Name=F}$		Primary: RSA (2048 bits), Load Balan	

Nu wordt het nieuwe identiteitsbewijs gebruikt.

### Verifiëren

Gebruik deze stappen om te controleren of de installatie van het leverancierscertificaat van een derde succesvol is en of u SSL VPN-verbindingen gebruikt.

Geïnstalleerde certificaten bekijken via ASDM

- Ga naar Configuration > Remote Access VPN > Certificate Management (Configuratie > VPN voor externe toegang > Certificaatbeheer) en selecteer Identity Certificates (Identiteitscertificaten).
- 2. Het door de derde partij afgegeven identiteitsbewijs kan worden weergegeven.

Interface Primary Certificate Load Balancing Certificate Key-Type Edit	0	Certificates Specify which certificates, if any, should b	e used for SSL authentication on each interface. Ti	he fallback certificate will be used on interfaces not asso	ciated with a certificate of their own.		
		Interface	Primary Certificate	Load Balancing Certificate	Кеу-Туре	Edit	l
OUTSIDE-direct SSL-Trustpoint-PKCS 12:unstructuredName ≈ F Primary: RSA (2048 bits), Load Balan		OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName=F		Primary: RSA (2048 bits), Load Balan		l

## Problemen oplossen

Deze debug-opdracht moet worden verzameld op de CLI in het geval van een fout bij de installatie van een SSL-certificaat.

• debug crypto ca 14

## Veelgestelde vragen

### Q.Wat is een PKCS12?

A.In cryptografie, definieert PKCS12 een archiefbestandsindeling die gemaakt is om vele cryptografische objecten als één bestand op te slaan. Het wordt algemeen gebruikt om een privé sleutel met zijn X.509 certificaat te bundelen of alle leden van een ketting van vertrouwen te bundelen.

### V.Wat is een MVO?

A. In PKI-systemen (public key infrastructure) is een verzoek om een certificaat te ondertekenen (ook CSR of certificeringsverzoek) een bericht dat door een aanvrager wordt verzonden naar een registratieautoriteit van de openbare sleutelinfrastructuur om een digitaal identiteitscertificaat aan te vragen. Het bevat gewoonlijk de openbare sleutel waarvoor het certificaat kan worden afgegeven, informatie die wordt gebruikt om het ondertekende certificaat te identificeren (zoals een domeinnaam in Onderwerp) en integriteitsbescherming (bijvoorbeeld een digitale handtekening).

### Q.Waar is het wachtwoord van de PKCS12?

A.Wanneer certificaten en sleutelparen naar een PKCS12-bestand worden geëxporteerd, wordt het wachtwoord gegeven in de opdracht Exporteren. Voor het importeren van een pkcs12bestand moet het wachtwoord worden geleverd door de eigenaar van de CA-server of de persoon die de PKCS12 heeft geëxporteerd van een ander apparaat.

### Q.Wat is het verschil tussen de wortel en de identiteit?

A. In cryptografie en computerbeveiliging is een basiscertificaat een publiek sleutelcertificaat dat een basiscertificeringsinstantie (CA) identificeert. De certificaten van de wortel zijn zelfondertekend (en het is mogelijk voor een certificaat om meerdere vertrouwenswegen te hebben, zeg als het certificaat door een wortel werd uitgegeven die) werd dwars-ondertekend en de basis van een op X.509-gebaseerde openbare zeer belangrijke infrastructuur (PKI) vormde. Een public key certificate, ook wel bekend als een digital certificate of Identity Certificate, is een elektronisch document dat gebruikt wordt om het eigendom van een publieke sleutel te bewijzen. Het certificaat bevat informatie over de sleutel, informatie over de identiteit van de eigenaar (het onderwerp genoemd), en de digitale handtekening van een entiteit die de inhoud van het certificaat heeft geverifieerd (de emittent genoemd). Als de handtekening geldig is, en de software die het certificaat onderzoekt de emittent vertrouwt, dan kan het die sleutel gebruiken om veilig met het onderwerp van het certificaat te communiceren.

Q.I installeerde de cert, waarom het niet werkt? A.Dit kan te wijten zijn aan vele redenen, bijvoorbeeld:

1. Het certificaat en trustpoint worden geconfigureerd, maar zijn niet gebonden aan het proces dat het moet gebruiken. Bijvoorbeeld, het te gebruiken trustpoint is niet gebonden aan de buiteninterface die AnyConnect-clients beëindigt.

2. Er wordt een PKCS12-bestand geïnstalleerd, maar dit bevat fouten als gevolg van het ontbreken van een tussentijds CA-certificaat in het PKCS12-bestand. De klanten die het tussenliggende CA-certificaat als betrouwbaar hebben, maar geen basiscertificaat van CA als betrouwbaar hebben, kunnen de gehele certificaatketen niet verifiëren en het server Identity Certificate niet als betrouwbaar rapporteren.

3. Een certificaat met onjuiste kenmerken kan installatiefouten of fouten aan de clientzijde veroorzaken. Bepaalde eigenschappen kunnen bijvoorbeeld met een verkeerd formaat worden gecodeerd. Een andere reden is dat het Identity Certificate ontbreekt. Alternatieve naam (SAN) ontbreekt, of dat de domeinnaam die gebruikt wordt om toegang te krijgen tot de server niet aanwezig is als SAN.

Q. Vereist een installatie van een nieuwe cert een onderhoudsvenster of veroorzaakt onderbreking?

A. De installatie van een nieuw certificaat (identiteit of CA) is niet opdringerig en zou geen onderbreking moeten veroorzaken of een onderhoudsvenster vereisen. Om een nieuw certificaat te kunnen gebruiken voor een service die bestaat, is een wijziging en vereist mogelijk een venster voor wijzigingsaanvraag/onderhoud.

Q.Kan het toevoegen of veranderen van een certificaat de verbonden gebruikers loskoppelen? A.No, de gebruikers die op dit moment verbonden zijn blijven verbonden. Het certificaat wordt gebruikt in de verbindingsinrichting. Wanneer de gebruikers opnieuw verbinding hebben gemaakt, wordt het nieuwe certificaat gebruikt.

Q.Hoe kan ik een MVO met een vervanging creëren? Of een alternatieve onderwerpnaam (SAN)?
A. Op dit moment kan de ASA/FTD geen CSR maken met wildcard; dit proces kan echter worden uitgevoerd met OpenSSL. U kunt de opdrachten uitvoeren om de CSR- en ID-toets te genereren: openssl genrsa - out id.key 2048

### openssl req -out id.csr -key id.key -nieuw

Wanneer een trustpoint is geconfigureerd met het FQDN-kenmerk (Fully Qualified Domain Name), bevat de door ASA/FTD gemaakte CSR de SAN met die waarde. Meer SAN-kenmerken kunnen door de CA worden toegevoegd wanneer deze de CSR ondertekent, of de CSR kan worden gemaakt met OpenSSL

Q.Worden certificaten onmiddellijk vervangen?

A. Het nieuwe server Identity Certificate wordt alleen gebruikt voor de nieuwe verbindingen. Het nieuwe certificaat is gereed om onmiddellijk na de wijziging gebruikt te worden, maar wordt daadwerkelijk gebruikt met nieuwe verbindingen.

V.Hoe kan ik controleren of de installatie werkte?

A.De CLI opdracht te verifiëren: toon crypto ca cert <trustpointname>

Q.Hoe te om PKCS12 van het Certificaat van de Identiteit, het certificaat van CA, en privé sleutel te produceren?

A. PKCS12 kan worden gemaakt met OpenSSL, met de opdracht: openssl pkcs12 -export -p12.pfx -inkey id.key -in id.crt -certfile ca.crt

Q. Hoe een certificaat uit te voeren om het in een nieuwe ASA te installeren? A.

- Met CLI: gebruik de opdracht: crypto kan <trustpointname> pkcs12 <password> exporteren
- Met ASDM:
  - a. Blader naar Configuratie > Apparaatbeheer > Certificaatbeheer > Identiteitscertificaten en kies het Identity Certificate. Klik op Exporteren.

File View Tools Wizards Windo	ow Help					Type topic to search	Go	ababa
Home 🖓 Configuration 🔯 Mon	iitoring 🔚 Save 🔇 Refre	esh 🔇 Back 🔘 Forwar	d 🧖 Help					CISCO
Bookmarks 🗗 म 🗡	Configuration > Device Ma	nagement > Certificate M	lanagement > Identity Ce	rtificates				
o bookmark a page, right-click 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 unstructuredName=risav	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			Evenet
								CAPOIT
								Install
								Re-Enrol
Device Management 🗗 🖗								
Management Access								
E-88 Licensing								
High Availability and Scalability								
E- Logging	Finds							
Smart Call-Home	1.00							
-24 Cloud Web Security	Certificate Expiration Alerts							
Users/AAA	Send the first alert befor	e: 60 (days) Set Def	ault					
Certificate Management     Jentity Certificates	Repeat Alert Interval :	7 (days)						
CA Certificates	Weak Crypto Configurations -							

b. Kies waar u het bestand wilt exporteren, geef het exportwachtwoord op en klik op Certificaat exporteren.

ssued To 1	Issued By	Expiry Date	Associated Trustpoints	Usage		Public Key Type	Add
nstructuredName=asav C	N=ca.example.com, OU	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023	General Pu	irpose	RSA (4096 bits)	Show Detai
nstructuredName=risav C	N=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Pu	rpose	RSA (2048 bits)	Show Deta
nstructuredName=FTD7 C	N=KrakowCA-sub1-1	04:44:00 CEST Dec 21 2024	SSL-Trustpoint-PKCS12	General Pu	rpose	RSA (2048 bits)	Delete
isa.vpn.example.com] N	lot Available	Pending	SSL-Trustpoint	Unknov	wn		Export
							Export
							Install
							Re-Enrol
ind: rtificate Expiration Alerts Send the first alert before : Repeat Alert Interval :	Image: Match Case       60     (days)       7     (days)	ult					
ind:	Image: Match Case       60     (days)       7     (days)       Export certificate	ult		×			
ind:	O Match Case      O (days) Set Defa      7 (days)     Export certificate      Ha	ult C: Wsers\cisco.DESKTOP4	R2CH8G5\Documents\ce Browse	×			
ind:	O Match Case     O     (days) Set Defa     (days)     Export certificate     Export to File:     Contificate Economia	ult C:\Users\cisco.DESKTOP4	R2CH8G5\Documents\ce Browse	×			
ind:	<ul> <li>Match Case</li> <li>(days) Set Defa</li> <li>(days)</li> <li>Export certificate</li> <li>Export to File: Certificate Format: alu</li> </ul>	C:\Users\cisco.DESKTOP4	R2CH8G5\Documents\ce	× .	a enerial n	omptional price for certificat	es and trial certificates
ind:	O Match Case     O (days) Set Defa     T (days)     Export certificate     Ha     Export to File:     Certificate Format:     pla	ult C:\Users\cisco.DESKTOP+ PKCS12 Format (Certif	R2CH8G5\Documents\ce Browse	. stomers a	a special pr	omotional price for certificat	tes and trial certificates
nd:	Match Case     Match Case     (days) Set Defa     Cays)     Export certificate     Export to File:     Certificate Format:     plie	Ult C:\Users\cisco.DESKTOP4 PKCS12 Format (Certificat PEM Format (Certificat	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	. stomers a	a special pr	omotional price for certificat	tes and trial certificates
ind:	O Match Case     Match Case     (days) Set Defa     (days)     Export certificate     Export to File:     Certificate Format:	ult C:\Users\cisco.DESKTOP4 @ PKCS 12 Format (Certificat O PEM Format (Certificat	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	· stomers a	a special pr	omotional price for certificat	tes and trial certificates
ind:	Match Case     Match Case     (days) Set Defa     (days)     Export certificate     Export to File:     Certificate Format:     pla	INIT C:\Users\cisco.DESKTOP4 PKCS 12 Format (Certificat PEM Format (Certificat an Passphrase	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	· stomers a	a special pr	omotional price for certificat	tes and trial certificates
ind:	Match Case     Match Case     (days) Set Defa     (days)     Export certificate     Export to File:     Certificate Format:     Dia     Configuration Encryption     Encryption Passphra	C:\Users\cisco.DESKTOP4 @ PKCS 12 Format (Certif O PEM Format (Certificat on Passphrase se:	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	· stomers a	a special pr	omotional price for certificat	tes and trial certificates

Het geëxporteerde certificaat kan op de computerschijf worden geplaatst. Let op het wachtwoord op een veilige plaats, het bestand is zonder het nutteloos.

Q.Als de sleutels ECDSA worden gebruikt, is het SSL proces van de certificaatgeneratie verschillend?

A.Het enige verschil in configuratie is de keypair generatiestap, waar een ECDSA keypair kan worden gegenereerd in plaats van een RSA keypair. De overige stappen zijn gelijk.

Q.Is het altijd vereist om een nieuw Zeer belangrijk paar te produceren?

A. De stap voor het genereren van het sleutelpaar is optioneel. Bestaand sleutelpaar kan worden gebruikt, of in het geval van PKCS12 wordt het sleutelpaar geïmporteerd met het certificaat. Zie de sectie Selecteer de Key pair Name voor het respectieve inschrijvings-/herinschrijvingstype.

Q.Is het veilig om een nieuw sleutelpaar te genereren voor een nieuw identiteitscertificaat? A.Het proces is veilig zolang een nieuwe naam van het Zeer belangrijke paar wordt gebruikt. In een dergelijk geval worden de oude Key Pairs niet gewijzigd.

Q.Is het vereist om sleutel opnieuw te produceren wanneer een firewall (zoals RMA) wordt vervangen?

A.De nieuwe firewall door ontwerp heeft geen Key Paren aanwezig op de oude firewall.

De back-up van de actieve configuratie bevat niet de sleutelparen.

De volledige back-up met ASDM kan de sleutelparen bevatten.

De Identity Certificates kunnen worden geëxporteerd van een ASA met ASDM of CLI voordat deze

faalt.

In het geval van een failover-paar worden de certificaten en sleutelparen gesynchroniseerd naar een stand-by-eenheid met de opdracht schrijfstand-by. In het geval van één knooppunt van failover-paar wordt vervangen is het voldoende om de basisfailover te configureren en de configuratie naar het nieuwe apparaat te duwen.

Als een sleutelpaar verloren gaat met het apparaat en er geen back-up is, moet een nieuw certificaat worden ondertekend met sleutelpaar aanwezig op het nieuwe apparaat.

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.