Installer et renouveler des certificats sur ASA géré par ASDM

Table des matières

Introduction Conditions préalables **Exigences** Composants utilisés Informations générales Demander et installer un nouveau certificat d'identité avec ASDM Demander et installer un nouveau certificat d'identité avec une demande de signature de certificat (CSR) Générer un CSR avec ASDM Créer un point de confiance avec un nom spécifique (Facultatif) Créer une nouvelle paire de clés Choisissez le nom de la paire de clés Configurer l'objet du certificat et le nom de domaine complet (FQDN) Générer et enregistrer le CSR Installer le certificat d'identité au format PEM avec ASDM Installer le certificat AC qui a signé le CSR Installer le certificat d'identité Lier le nouveau certificat à l'interface avec ASDM Installer un certificat d'identité reçu au format PKCS12 avec ASDM Installer les certificats d'identité et d'autorité de certification à partir d'un fichier PKCS12 Lier le nouveau certificat à l'interface avec ASDM Renouvellement du certificat Renouveler un certificat inscrit avec une demande de signature de certificat (CSR) avec ASDM Générer un CSR avec ASDM Créez un nouveau point de confiance avec un nom spécifique. (Facultatif) Créer une nouvelle paire de clés Sélectionnez le nom de la paire de clés Configurer l'objet du certificat et le nom de domaine complet (FQDN) Générer et enregistrer le CSR Installer le certificat d'identité au format PEM avec ASDM Installer le certificat AC qui a signé le CSR Installer le certificat d'identité Lier le nouveau certificat à l'interface avec ASDM Renouveler un certificat inscrit avec un fichier PKCS12 avec ASDM Installer le certificat d'identité renouvelé et les certificats CA à partir d'un fichier PKCS12 Lier le nouveau certificat à l'interface avec ASDM Vérifier Afficher les certificats installés via ASDM

Introduction

Ce document décrit comment demander, installer, approuver et renouveler certains types de certificats sur le logiciel Cisco ASA géré avec ASDM.

Conditions préalables

Exigences

- Avant de commencer, vérifiez que l'appliance ASA (Adaptive Security Appliance) dispose de l'heure, de la date et du fuseau horaire corrects. Avec l'authentification de certificat, il est recommandé d'utiliser un serveur NTP (Network Time Protocol) pour synchroniser l'heure sur l'ASA. Consultez Informations connexes pour référence.
- Pour demander un certificat qui utilise une demande de signature de certificat (CSR), il est nécessaire d'avoir accès à une autorité de certification (CA) interne ou tierce de confiance. Les exemples de fournisseurs CA tiers incluent, sans s'y limiter, Entrust, Geotrust, GoDaddy, Thawte et VeriSign.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASAv 9.18.1
- Pour la création de PKCS12, OpenSSL est utilisé.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les types de certificats auxquels ce document s'adresse sont les suivants :

- certificats auto-signés
- certificats signés par une autorité de certification tierce ou une autorité de certification interne

Les protocoles d'authentification SSL (Secure Socket Layer), TLS (Transport Layer Security) et IKEv2 rfc7296 pour EAP exigent que le serveur SSL/TLS/IKEv2 fournisse au client un certificat de serveur pour que le client effectue l'authentification du serveur. Il est recommandé d'utiliser des autorités de certification tierces de confiance pour émettre des certificats SSL à l'ASA à cette fin.

Cisco déconseille l'utilisation d'un certificat auto-signé, car un utilisateur peut configurer par inadvertance un navigateur pour faire confiance à un certificat provenant d'un serveur non autorisé. Il est également gênant pour les utilisateurs de devoir répondre à un avertissement de sécurité lorsqu'ils se connectent à la passerelle sécurisée.

Demander et installer un nouveau certificat d'identité avec ASDM

Un certificat peut être demandé à une autorité de certification (CA) et installé sur un ASA de deux manières :

- Utiliser la demande de signature de certificat (CSR). Générez une paire de clés, demandez un certificat d'identité à l'autorité de certification avec un CSR, installez le certificat d'identité signé obtenu auprès de l'autorité de certification.
- Utilisez le fichier PKCS12 obtenu d'une autorité de certification ou exporté à partir d'un autre périphérique. Le fichier PKCS12 contient la paire de clés, le certificat d'identité, le ou les certificats d'autorité de certification.

Demander et installer un nouveau certificat d'identité avec une demande de signature de certificat (CSR)

Un CSR est créé sur le périphérique qui a besoin d'un certificat d'identité, utilisez une paire de clés créée sur le périphérique.

Un CSR contient :

- informations sur la demande de certificat objet demandé et autres attributs, clé publique de la paire de clés,
- informations sur l'algorithme de signature,
- signature numérique des informations de demande de certificat, signée avec la clé privée de la paire de clés.

Le CSR est transmis à l'autorité de certification (CA), afin qu'elle le signe, dans un formulaire PKCS#10.

Le certificat signé est renvoyé par l'autorité de certification sous la forme d'un PEM.

Remarque : l'autorité de certification peut modifier les paramètres FQDN et Subject Name définis dans le point de confiance lorsqu'elle signe le CSR et crée un certificat d'identité signé.

Générer un CSR avec ASDM

- 1. Créer un point de confiance avec un nom spécifique
 - a. Accédez à Configuration > Device Management > Certificate Management > Identity

Certificates.



- b. Cliquez sur Add.
- c. Définissez un nom de point de confiance.

ssued To	Issued By	Expiry Date	Associated Trustpoints	^1	Usage	Public Key Type	Add
🔄 Add Identity (Certificate					×	Show Detai
Trustpoint Name	sSL-Trustpoint						Delete
O Import the id	dentity certificate from a file (PKCS12 format with Certificate(s)	+Private Key):				Export
Decryption P	assphrase:						Install
File to Impor	t From:	Browse					Re-Enroll
Add a new id	dentity certificate:						
Key Pair:	<default-rsa+< td=""><td>iey> v Show</td><td>New</td><td></td><td></td><td></td><td></td></default-rsa+<>	iey> v Show	New				
Certificate St	ubject DN: CN=asavpn.exa	mple.com Select					
Generate	e self-signed certificate						
Act a	as local certificate authority ar	d issue dynamic certificates to TL	S-Proxy				
			Advanced				
Enable C	A flag in basic constraints ext	ension	Hereiteen				
		Add Certificate	Cancel Help	1			

- d. Cliquez sur la case d'option Add a new identity certificate.
- 2. (Facultatif) Créer une nouvelle paire de clés

Remarque : par défaut, la clé RSA avec le nom Default-RSA-Key et une taille de 2048 est utilisée ; cependant, il est recommandé d'utiliser une paire de clés privée/publique unique pour chaque certificat d'identité.

a. Cliquez sur New pour générer une nouvelle paire de clés.

ssued To	Issued By	Expiry Da	te	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)+P	rivate Key):				Export
Decryption Pas	sphrase:	1						Install
File to Import F	From:		Browse					Re-Enro
Add a new ide	ntity certificate:							
Key Pair:	<default-rsa-< td=""><td>Key> v</td><td>Show</td><td>New</td><td></td><td></td><td></td><td></td></default-rsa-<>	Key> v	Show	New				
Certificate Sub	ject DN: CN=asavpn.ex	ample.com	Select					
Generate s	self-signed certificate							
Act as	local certificate authority a	nd issue dynamic ce	rtificates to TLS-F	roxy				
			_					
				Advanced				
Enable CA	flag in basic constraints ex	tension						

- b. Choisissez l'option Enter new Key Pair name et entrez un nom pour la nouvelle paire de clés.
- c. Sélectionnez le type de clé RSA ou ECDSA.
- d. Choisissez la Key Size ; pour RSA, choisissez General purpose for Usage.
- e. Cliquez sur Generate Now. La paire de clés est maintenant créée.

sued To	Issued By	Expiry Date	Associated Trustpoi	nts	Usage	Public Key Type	Add
🔤 Add Identity Certif	licate			×	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)	Show Deta
Trustpoint Name:	SSL-Trustpoint			a	our la contra por c		Delete
🔿 Impor <u></u> Add	Key Pair		×				Export
Decry	0.000	0.000					Install
File to	pe: () RSA	O ECDSA O E	DUSA				Re-Enro
Add a Name:	O Use default key	pair name					
Key Pa	Enter new key p	pair name: SSL-Keypair					
Certifi Size:	2048	~	N				
Ge Usage:	General purpose	Special	5				
				-			
	Generate Now	Cancel	Help				

3. Choisissez le nom de la paire de clés

Sélectionnez la paire de clés avec laquelle signer le CSR et à lier au nouveau certificat.

sued To	Issued By	Expiry Date	Associated Trust	points	Usage	Public Key Type	Add
Add Identity Certi	ificate			×	General Purpose	RSA (4096 bits)	Show Deta
				_	General Purpose	RSA (2048 bits)	Delete
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the identi	ty certificate from a file ((PKCS12 format with Certificate(s)+Private Key):				Export
Decryption Passp	hrase:						Install
File to Import Fro	im:	Browse					Re-Enro
Add a new identi	ty certificate:						
Key Pair:	SSL-Keypair	Show	New				
Certificate Subject	ct DN: CN=asavpn.ex	ample.com Select					
Generate self	f-signed certificate						
Act as loc	cal certificate authority a	nd issue dynamic certificates to T	TLS-Proxy				
			Advanced				
Enable CA fla	ig in basic constraints ex	tension					

4. Configurer l'objet du certificat et le nom de domaine complet (FQDN)

Attention : le paramètre FQDN doit correspondre au FQDN ou à l'adresse IP de l'interface ASA pour laquelle le certificat d'identité est utilisé. Ce paramètre définit l'extension de nom alternatif de sujet (SAN) demandée pour le certificat d'identité. L'extension SAN est utilisée par le client SSL/TLS/IKEv2 pour vérifier si le certificat correspond au nom de domaine complet auquel il se connecte.

a. Cliquez sur Sélectionner.

Issued To	Issued By	Expiry Date	Associated Trustpoints	^1	Usage	Public Key Type	Add
🛓 Add Identity Ce	rtificate	· ·				×	Show Deta
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the ider	ntity certificate from a file (P	KCS12 format with Certificate(s)	+Private Kev):				Export
Decryption Pas	sphrase:						Install
File to Import F	rom:	Browse					Re-Enrol
Add a new ider	ntity certificate:						
Key Pair:	SSL-Keypair	~ Show	New				
Certificate Subj	ject DN: CN=asavpn.exa	mple.com Select					
Generate s	elf-signed certificate						
Act as I	ocal certificate authority an	d issue dynamic certificates to TL	S-Proxy				
			Adversed			_	
	0		Advanced				
	fiag in basic constraints exte	ension					

b. Dans la fenêtre Certificate Subject DN, configurez les attributs de certificat - choisissez un attribut dans la liste déroulante, entrez la valeur, cliquez sur 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 b						

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

ssued To	Issued By	Expiry Date	Assoc	iated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Certificate	2						×	Show Detai
Trustpoint Name:	SSL-Trustpoint							Delete
O Import the identity ce	Cartificate Subi	ect DN				×		Export
Decryption Passphrase	Certificate Subj	eccon				~		Install
File to Import From:				Attribute	Value			Re-Enrol
 Add a new identity cer Key Pair: Certificate Subject DN Generate self-sign Act as local cer 	DN Attribute to Attribute: Value: C S S Li	o be Added Country (C) common Name (CN) lepartment (OU) country (C) tate (St) ocation (L) mail Address (EA)	Add>> Delete	Common Name (CN)	asa.vpn.e	xam		
Enable CA flag in t		ОК	Cancel	Help				

Attribut	Description
CN	Nom par lequel le pare-feu est accessible (généralement le nom de domaine
	complet, par exemple, vpn.example.com).
OU	Nom de votre service au sein de l'organisation
0	Le nom enregistré légalement de votre organisation/société
С	Code du pays (code de 2 lettres sans ponctuation)
ST	État dans lequel se trouve votre organisation.
L	Ville dans laquelle se trouve votre entreprise.
CE	Adresse électronique

Remarque : aucune des valeurs des champs précédents ne peut dépasser une limite de 64 caractères. Une valeur plus longue peut entraîner des problèmes avec l'installation du certificat d'identité. En outre, il n'est pas nécessaire de définir tous les attributs DN.

Cliquez sur OK après avoir ajouté tous les attributs.

c. Configurez le nom de domaine complet du périphérique - cliquez sur Avancé.

sued to	Issued By	Expiry (Date	Associated Trustpoints	^1	Usage	Public Key Type		Add
Add Identity Certificat	te						×		Show Detai
Trustpoint Name:	SSL-Trustpoint								Delete
Import the identity ce	rtificate from a file (PKCS	12 format wit	h Certificate(s)+Pri	vate Kev):				1	Export
Decryption Passphras	e:								Install
File to Import From:			Browse						Re-Enrol
Add a new identity ce	rtificate:								
Key Pair:	SSL-Keypair	~	Show	New					
Certificate Subject DN	I: CN=asa.vpn.example	e.com	Select						
Generate self-sigr	ned certificate								
Act as local ce	rtificate authority and iss	ue dynamic ce	ertificates to TLS-Pr	оху			-		
							-		
-				Advanced					
Enable CA flag in	basic constraints extensio	n							

d. Dans le champ FQDN, saisissez le nom de domaine complet par lequel le périphérique est accessible à partir d'Internet. Click OK.

Issued To	Issund D.	Evoiry Data	Acceptated Trustasiate	A 1 Ukana	Public Key Type	Add
Add Identity Ce	rtificate Advanced	d Options		×	×	Show Deta
Trustnoint Name:	Enrollment mo	de parameters and SCEP cha	lenge password are not available for se	If-signed certificates.		Delete
Import the iden	Certifica	arameters Enrollment Mode	SCEP Challenge Password			Export
Decryption Pas	sphrase: FQDN:	asavpn.example.com				Install
File to Import F	rom: E-mail:					Re-Enro
Add a new ider	IP Address:					
Kev Pair:	S Include	serial number of the device				
Certificate Subj	ject DN: C					
Generate s	elf-signed ce					
Act as I	ocal certifica					
Enable CA	flag in basic (
	100		·····	10		

- 5. Générer et enregistrer le CSR
 - a. Cliquez sur Ajouter un certificat.

sued To	Issued By	Expiry (Date	Associated Trustpoints	^1	Usage	Public Key Type	e	Add
Add Identity Certifi	cate						· · · ·	×	Show Detai
Trustpoint Name:	SSL-Trustpoint								Delete
Import the identity	certificate from a file (PKC	CS12 format wit	h Certificate(s)+Pr	ivate Kev):					Export
Decryption Passoh	rase:								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.exam	ple.com	Select						
Generate self-	signed certificate								
Act as local	certificate authority and i	issue dynamic ce	ertificates to TLS-P	roxy					
				Advanced					
Enable CA flag	in basic constraints exten	sion							

b. Une invite s'affiche afin d'enregistrer le CSR dans un fichier sur la machine locale.

ssued To	Issued By	Expiry Date	Associated Trustpoints	~1	Usage	Public Key Type	Add
Add Identity Certi	ficate					×	Show Details
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the identit	ty certificate from a file (PKCS12 format with Certificate(s)	+Private Key):				Export
Decryption Passp	hrase:						Install
File to Import Fro	m:	Identity Certificate Request		×			Re-Enroll
Certificate Subjec	t DN: CN=asa.vp	You will then need to install the ce clicking the Install button in the Ide Save CSR to File:	rtificate that is returned from the C entity Certificates panel.	wse			
Act as loc	al certificate author	ОК	Cancel Help				
			Advanced				
Enable CA fla	g in basic constraints ext	tension					

Cliquez sur Browse, choisissez un emplacement dans lequel enregistrer la CSR, puis enregistrez le fichier avec l'extension .txt.

Remarque : lorsque le fichier est enregistré avec une extension .txt, la demande PKCS#10 peut être ouverte et affichée à l'aide d'un éditeur de texte (tel que le Bloc-notes).

c. Le nouveau point de confiance est maintenant affiché à l'état En attente.

isued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
sa.vpn.example.com]	Not Available	Pending	SSL-Trustpoint	Unknown		Show Detail
						Delete
						Export
						Install

Installer le certificat d'identité au format PEM avec ASDM

Les étapes d'installation supposent que l'autorité de certification a signé le CSR et fourni un certificat d'identité codé PEM (.pem, .cer, .crt) et un ensemble de certificats d'autorité de certification.

- 1. Installer le certificat AC qui a signé le CSR
 - a. Accédez à Configuration > Device Management > Certificate Management > , et choisissez CA Certificates. Cliquez sur Add.

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

b. Entrez le nom du point de confiance et sélectionnez Installer à partir du fichier, cliquez sur le bouton Parcourir, puis sélectionnez le certificat intermédiaire. Vous pouvez également coller le certificat CA codé PEM d'un fichier texte dans le champ texte.

issued To	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	
Install Certificate			×			Show Deta
						Request CF
Trustpoint Name:	SSL-Trustpoint					Delete
Install from a file:		Browse				
Paste certificate in	PEM format:					

Remarque : installez le certificat d'autorité de certification qui a signé le CSR et utilisez le même nom de point de confiance que le certificat d'identité. Les autres certificats d'autorité de certification situés plus haut dans la hiérarchie PKI peuvent être installés dans des points de confiance distincts.

c. Cliquez sur Install Certificate.

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	E dis
uoVadis Root CA 2	CN=QuoVadis Root CA 2,	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	Edit
Install Certificate					×	Show Details
Trustagiat Name	1 Tructuoint	1				Request CRI
Traspoint Name. 55	c-mospoinc					Delete
O Install from a file:		Browse				
Paste certificate in PEN	4 format:					
9ILFV52L47em9UXaM cGqeyDMRhsRsk/wD2 z8qaqRsk/wD2 z8qaqRsk/s153y//L88 QRyjaH56BFladAvc7k gW8YnhOvM08syrD2 dcVcovO/PAxmAJ+N END CERTIFICATE O Use EST: Specify source Interfate EST URL: https:// Certificate Subject DN:	AGGCSqGSIb 3DQEBC/NUAA4IB SM2/MAF4AY2HgN9gK9/CK +H SM2/MAF4AY2HgN9gK9/CK +H RddtVxYB9sfEbFh [2]yWFN3MXW2O [2]yWFN3MXW2O [2] ce:None [] co: (N-risavpn3]	AQArsXIPwK3JNBwQsrh5mgT wodrMQ2y4X,Uhj65NDU70Ff6f te wait Please wait while ASDM is deliv device	X Information INFO: Certificate has the Fingerprint: e9ad165c 265 Trustpoint CA certificate a	following attributes: 73424c 6e7e0c5f b30b4 iccepted.	402	
allow-untrusted-co	nnection					
0				ж		
O Use SCEP:	ce: None	~				
O Use SCEP: Specify source Interfac						
O Use SCEP: Specify source Interface SCEP URL: http://						
O Use SCEP: Specify source Interface SCEP URL: http:// Retry Period:	1	minutes				

- 2. Installer le certificat d'identité
 - a. Sélectionnez le certificat d'identité créé précédemment lors de la génération CSR. Cliquez sur Install.

onfiguration	n > Rem	ote Ac	cess VPN > Certific	ate Management > Ident	ity Certificates			
Issued To		^1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
[vpn.examp	le.com]		Not Available	Pending	SSL-Trustpoint	Unknown		Show Details
								Delete
								Export
								Install

Remarque : le champ Émis par peut avoir la valeur Non disponible et le champ Date d'expiration la valeur En attente.

b. Choisissez un fichier qui contient le certificat d'identité codé PEM reçu de l'autorité de certification, ou ouvrez le certificat codé PEM dans un éditeur de texte et copiez et collez le certificat d'identité fourni par l'autorité de certification dans le champ de texte.

sued To	^1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
n.example.com]		Not Available	Pending	SSL-Trustpoint	Unknown		Show Detai
Install Islands				~	General Purpose	RSA (2048 bits)	
install identity	centric	ate		tpoint	General Purpose	RSA (2048 bits)	Delete
entity Certificate							Export
Install from a	fler [Browse			Export
 Install from a 	file:			Browse			Export
 Install from a Paste the cert 	file:	data in base-64 forma	t:	Browse			Export Install
Install from a Paste the cert	file:	data in base-64 forma	t	Browse			Export Install Re-Enroll
Install from a Paste the cert	file:	data in base-64 forma	tı	Browse			Export Install Re-Enroll
Install from a Paste the cert	file:	data in base-64 forma	tı	Browse			Export Install Re-Enroll
Install from a Paste the cert	file:	data in base-64 forma	t:	Browse			Export Install Re-Enroll
Install from a Paste the cert	file:	data in base-64 forma	t:	Browse			Export Install Re-Enroll
Install from a Paste the cert	file:	data in base-64 forma	tı	Browse			Export Install Re-Enroll

Remarque : le certificat d'identité peut être au format .pem, .cer, .crt à installer.

c. Cliquez sur Install Certificate.

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 Detail
Install Identity certificate		×	General Purpose	RSA (2048 bits)	
a mistal identity certificate		tpoint	General Purpose	RSA (2048 bits)	Delete
Jentity Certificate	🔁 Please wait	×			Export
Install from a file:		Information	×		Install
Paste the certificate data in ba	Please wait while ASDM is de	elivering th			
LnNBJz6XgDmVuQjfBEMVxR2K	device				Re-Enroll
Gyer3x2GXML7MAiHBptyMcHD		(1) Certificate im	port succeeded.		
KdNgiEbUr6VW9NTuE2DowH3					
END CERTIFICATE					
		OK			
<		i			

3. Lier le nouveau certificat à l'interface avec ASDM

L'ASA doit être configuré pour utiliser le nouveau certificat d'identité pour les sessions WebVPN qui se terminent sur l'interface spécifiée.

- a. Accédez à Configuration > Remote Access VPN > Advanced > SSL Settings.
- b. Sous Certificates, choisissez l'interface utilisée pour terminer les sessions WebVPN. Dans cet exemple, l'interface externe est utilisée.

Cliquez sur Edit.

c. Dans la liste déroulante Certificate, sélectionnez le nouveau certificat installé.

- Comon		eer meere		Edit
				Delete
	Select SSL Certificate	×		
	Specify enrolled trustpoints to be used for SSL authen OUTSIDE-direct interface. To enroll a trustpoint, go to Management > Identity Certificates.	tication and VPN load balancing on the Device Management > Certificate		
rtificates Specify which certificates, if ar	Interface: OUTSIDE-direct		es not associated with a certificate of their own.	
Interface	Primary Enrolled Certificate: SSL-Trustpoint:u Load Balancing Enrolled Certificate: None	nstructuredName =asavpn.exampl v	Кеу-Туре	Edit
inside	OK Cancel	Help		
management				
allback Certificate:	None	×		
Forced Certification Authenticat	n Timeout:	2 minutes		

- d. Click OK.
- e. Cliquez sur Apply.

Interface	Primary Certificate	Load Balancing Certificate	Кеу-Туре	Edit
OUTSIDE-direct	SSL-Trustpoint:unstructuredNan	ne=	Primary: RSA (2048 bits), Load Balancing:	
inside				
inside-vlan				
management				

Le nouveau certificat d'identité est maintenant utilisé.

Installer un certificat d'identité reçu au format PKCS12 avec ASDM

Le fichier PKCS12 (format .p12 ou .pfx) contient un certificat d'identité, une paire de clés et un ou plusieurs certificats d'autorité de certification. Il est créé par l'autorité de certification, par exemple en cas de certificat générique, ou exporté à partir d'un autre périphérique. Il s'agit d'un fichier binaire qui ne peut pas être affiché avec l'éditeur de texte.

1. Installer les certificats d'identité et d'autorité de certification à partir d'un fichier PKCS12

Le certificat d'identité, le ou les certificats d'autorité de certification et la paire de clés doivent être regroupés dans un fichier PKCS12 unique.

- a. Accédez à Configuration > Device Management > Certificate Management, et choisissez Identity Certificates.
- b. Cliquez sur Add.
- c. Spécifiez un nom de point de confiance.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
			103			Show Detail
🔤 Add Identity Ce	ertificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-F	PKCS12				Export
Import the ide	ntity certificate from a file (F	PKCS12 format with Certificate	(s) +Private Key):			Install
Decryption Pas	sphrase:					Re-Enrol
File to Import F	From:	Browse.				
O Add a new ide	ntity certificate:					
Key Pair:	<default-rsa-k< td=""><td>iey> v Show</td><td>. New</td><td></td><td></td><td></td></default-rsa-k<>	iey> v Show	. New			
Certificate Sub	ject DN: CN=risavpn31	Select				
Generate s	self-signed certificate					
Act as	local certificate authority an	nd issue dynamic certificates to	TLS-Proxy			
			Advanced			
NEnable CA	flag in basic constraints ext	ension				
4,3						

d. Activez la case d'option Importer le certificat d'identité à partir d'un fichier.

	Issued By	Expiry	Date	Associated	Trustpoints	Usage	Publi	с Кеу Туре	1	Add
										Show Detai
🔁 Add Identity Certifi	cate		and the second s		×				-	Delete
Trustpoint Name:	SSL-Trustpoint-PI	CS12]		import ID certi	ficate file				
Import the identity	certificate from a file (P	CS12 format w	ith Certificate(s)+P	rivate Key):	Look in:	Document	ts	~	🥬 📂 🛄 •	
Decryption Passphr	ase:		1		Co.	CSR.txt				
File to Import From	:		Browse		Recent Items	🥦 vpn.exan	ple.com.pfx			
Add a new identity	certificate:									
Key Pair:	<default-rsa-ke< td=""><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					
Certificate Subject	DN: CN=risavpn31		Select							
Generate self-s	signed certificate				Documents					
Act as local	certificate authority and	l issue dynamic	certificates to TLS-f	roxy						
				Advanced	This PC F	ile name:	vpn.example.com.pf	¢	Import ID o	ertificate file
	in basic constraints outs	ocion		Advanced	- 🥌 F	iles of type:	All Files	~	Ca	ncel
	in basic consulaints exte	13011			L					

e. Entrez la phrase de passe utilisée pour créer le fichier PKCS12.

ssued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
							Show Detail
add Identity Certif	ficate			×			Delete
Trustpoint Name:	SSL-Trustpoint-Pi	KCS12					Export
 Import the identit 	y certificate from a file (P	KCS12 format with C	Certificate(s)+Pri	vate Key):			Install
Decryption Passpl	hrase: ••••						Re-Enroll
File to Import From	m: C:\Users\cisco.D	ESKTOP-R2CH8G	Browse				
O Add a new identit	y certificate:						
Key Pair:	<default-rsa-ke< td=""><td>ey> ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-ke<>	ey> ~	Show	New			
Certificate Subject	t DN: CN=risavpn31		Select				
Generate self	-signed certificate						
Act as loc	al certificate authority and	d issue dynamic certi	ficates to TLS-P	oxy			
				Idvanced			
Enable CA flag	n in basic constraints exte	ension					
	g						

f. Cliquez sur Add Certificate.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Detail
🔁 Add Identity Co	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	ssphrase: •••••					Re-Enrol
File to Import	From: C:\Users\cisco.E	DESKTOP-R2CH8G Browse.				
🔿 Add 🔤 Ple	ase wait					
Keyl	Disess with this ACDM	in delivering the second of the				
Certi 🖘	device	is delivering the command(s) to		6		
]			s for CAs higher in the hie	rarchy as the CA certificate was not s	elf-signed.
			WARNING: CA cer	tificates can be used to va	alidate VPN connections.by default. Ple	ease adjust
			the validation-usa	ge of this trustpoint to limi	t the validation scope, if necessary	
Enable CA	flag in basic constraints ext	tension	Import PKCS 12 op	eration completed success	fully.	
_						
	Add Certificate	Cancel Help		OK		

Remarque : lorsque vous importez une chaîne de certificats PKCS12 avec CA, l'ASDM crée automatiquement les points de confiance CA en amont avec des noms avec le suffixe -number aiouté.

			• • • • • • • • •	
Configura	tion > Ren	note Access VPN >	Certificate Managem	ent > CA Certificates

Issued To V	¹ 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. Lier le nouveau certificat à l'interface avec ASDM

L'ASA doit être configuré pour utiliser le nouveau certificat d'identité pour les sessions WebVPN qui se terminent sur l'interface spécifiée.

a. Accédez à Configuration > Remote Access VPN > Advanced > SSL Settings.

b. Sous Certificates, sélectionnez l'interface utilisée pour terminer les sessions WebVPN. Dans cet exemple, l'interface externe est utilisée.

Cliquez sur Edit.

c. Dans la liste déroulante Certificate, sélectionnez le nouveau certificat installé.

Unit		er mene		Edit
rtificates Specify which certificates, if ar Interface OUTSIDE-direct inside-vlan management	Select SSL Certificate Specify enrolled trustpoints to be OUTSIDE-dret interface. Primary Enrolled Certificate: Load Balancing Enrolled Certificate	X used for SSL authentication and VPN load balancing on the all a trustpoint, go to Device Management > Certificate es. OUTSIDE-direct SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u v :: None v K Cancel Help	es not associated with a certificate of their own. Key-Type	Edt
Fallback Certificate: Forced Certification Authenticat	None	2 minutes		

- d. Click OK.
- e. Cliquez sur Apply.

Certif Spe	ficates ecify which certificates, if any, should be	e used for SSL authentication on each interface. Th	ne 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	

Le nouveau certificat d'identité est maintenant utilisé.

Renouvellement du certificat

Renouveler un certificat inscrit avec une demande de signature de certificat (CSR) avec ASDM

Le renouvellement de certificat du certificat inscrit CSR nécessite la création et l'inscription d'un nouveau point de confiance. Il doit avoir un nom différent (par exemple, ancien nom avec suffixe de l'année d'inscription). Il peut utiliser les mêmes paramètres et la même paire de clés que l'ancien certificat, ou peut utiliser des paramètres différents.

Générer un CSR avec ASDM

- 1. Créez un nouveau point de confiance avec un nom spécifique.
 - a. Accédez à Configuration > Device Management > Certificate Management > Identity

Certificates.



- b. Cliquez sur Add.
- c. Définissez un nom de point de confiance.

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

- d. Cliquez sur la case d'option Add a new identity certificate.
- 2. (Facultatif) Créer une nouvelle paire de clés

Remarque : par défaut, la clé RSA avec le nom Default-RSA-Key et une taille de 2048 est utilisée ; cependant, il est recommandé d'utiliser une paire de clés privée/publique unique pour chaque certificat d'identité.

a. Cliquez sur New pour générer une nouvelle paire de clés.

sueu to issued	d By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
structuredName= CN=ca	a.example.com, OU	15:10:00 CEST F	Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
add Identity Certificate	e			×			Delete
Trustpoint Name:	SSL-Trustpoint-202	23					Export
O Import the identity cer	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 cer	tificate:						
Key Pair:	<default-rsa-key< td=""><td>/></td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-key<>	/>	Show	New			
Certificate Subject DN	: CN=asavpn.exam	ple.com	Select				
Generate self-sign	ed certificate						
Act as local cer	tificate authority and	issue dynamic cer	tificates to TL	S-Proxy			
				Advanced			
	asic constraints exten	sion		Autoriceant			

- b. Choisissez l'option Saisir le nom de la nouvelle paire de clés et entrez un nom pour la nouvelle paire de clés.
- c. Sélectionnez le type de clé : RSA ou ECDSA.
- d. Choisissez la taille de clé ; pour RSA, choisissez Fonction générale pour Utilisation.
- e. Cliquez sur Generate Now. La paire de clés est maintenant créée.

Show Detai Delete Export
Delete
Export
Install
Re-Enroll

3. Sélectionnez le nom de la paire de clés

Sélectionnez la paire de clés avec laquelle signer le CSR et à lier au nouveau certificat.

33000 10 133000	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
🔄 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	- v	Show	New			
Certificate Subject DN:	CN=asavpn.exam	nple.com	Select				
Generate self-signe	d certificate			-			
Act as local cert	ificate aut prity and	issue dynamic ce	rtificates to TL	S-Proxy			
				Advanced			
Enable CA flag in ba	sic constraints exter	nsion					

4. Configurer l'objet du certificat et le nom de domaine complet (FQDN)

Attention : le paramètre FQDN doit correspondre au nom de domaine complet ou à l'adresse IP de l'interface ASA pour laquelle le certificat est utilisé. Ce paramètre définit le nom alternatif du sujet (SAN) pour le certificat. Le champ SAN est utilisé par le client SSL/TLS/IKEv2 pour vérifier si le certificat correspond au nom de domaine complet auquel il est connecté.

Remarque : l'autorité de certification peut modifier les paramètres FQDN et Subject Name définis dans le point de confiance lorsqu'elle signe le CSR et crée un certificat d'identité signé.

a. Cliquez sur Sélectionner.

- ca avample com OU							
-catexample.com, OU	15:10:00 CEST F	eb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Deta
ate			×	<			Delete
SSI -Trustnoint-202	23						Export
certificate from a file (PKG	CS12 format with	Certificate(s)+	Private Key):				Install
ase:							Re-Enrol
		Browse	í				
certificate:							
SSL-KeyPair-2023	~	Show	New				
DN: CN=asavpn.examp	de.com	Select					
gned certificate				-			
certificate authority and i	ssue dynamic cer	tificates to TLS	-Proxy	-			
		[Advanced				
n basic constraints exten	sion	L					
	ste SSL-Trustpoint-202 certificate from a file (PKC see: SSL-KeyPair-2023 N: (CN=asavpn.examp gned certificate certificate balaic constraints exten balaic constraints exte	ate SSL-Trustpoint-2023 certificate from a file (PKCS 12 format with use: SSL-KeyPair-2023 SSL-KeyPair-202 SSL-KeyPair-2023 S	ate SSL-Trustpoint-2023 certificate from a file (PKCS12 format with Certificate(s) + use: Browse Browse Browse Browse SSL-KeyPair-2023 ✓ Show N1: CN=asavpn.example.com Select gned certificate certificate basic constraints extension	ate SSL-Trustpoint-2023 SSL-Trustpoint-2023 certificate from a file (PKCS12 format with Certificate(s) +Private Key): use: Browse Bro	ate X SSL-Trustpoint-2023 Startificate (s) +Private Key): set: Browse set: Browse certificate: Startificate: startificate: Startificate: yn: ON=asavpn.example.com Select Select gned certificate Advanced	Ate X SSL-Trustpoint-2023 certificate from a file (PKCS12 format with Certificate(s) +Private Key): use: Browse Browse Browse Browse Browse Advanced	Advanced

b. Dans la fenêtre Certificate Subject DN, configurez les attributs du certificat - sélectionnez l'attribut dans la liste déroulante, entrez la valeur, cliquez sur Add.

Issued To	Issued By	Expiry	Date	Associated Trustpoints		Usage	Public Key Type	Add
instructuredName	CN=ca.example.com	, OU 15:10:	00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detai
🔄 Add Identity	Certificate			×				Delete
Trustpoint Nam	e: SSL-Trustp	oint-2023						Export
ertificate Subject	t DN				×			Install
			-					Re-Enroll
			Attribute	Value				
DN Attribute to Attribute: Co	e Added	Add>>	Company Name (O) example inc				
Value: US		Delete						
	ОК	Cance	el Help		- 1			
	CA flag in basic constraint	s extension						
	CA flag in basic constraint	s extension						

Attribut	Description
CN	Nom par lequel le pare-feu est accessible (généralement le nom de domaine complet, par exemple, vpn.example.com).
ου	Nom de votre service au sein de l'organisation
0	Le nom enregistré légalement de votre organisation/société
С	Code du pays (code de 2 lettres sans ponctuation)
ST	État dans lequel se trouve votre organisation.
L	Ville dans laquelle se trouve votre entreprise.
CE	Adresse électronique

Remarque : aucun des champs précédents ne peut dépasser une limite de 64 caractères. Une valeur plus longue peut entraîner des problèmes avec l'installation du certificat d'identité. En outre, il n'est pas nécessaire de définir tous les attributs DN.

Cliquez sur OK après avoir ajouté tous les attributs.

c. Pour configurer le nom de domaine complet du périphérique, cliquez sur Avancé.

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
🔄 Add Identity (Certificate			×			Delete
Trustpoint Name	SSI -Trustnoint-20	123					Export
O Import the id	dentity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption P	assphrase:						Re-Enroll
File to Import	t From:		Browse				
Add a new id	dentity certificate:						
Key Pair:	SSL-KeyPair-2023	۰ V	Show	New			
Certificate Su	ubject DN: /pn.example.com	,O=example inc	Select				
Generate	e self-signed certificate						
Act a	as local certificate authority and	issue dynamic ce	rtificates to TL	S-Proxy			
				- Adversed			
				Advanceu			
	A hag in basic constraints exter	nsion					

d. Dans le champ FQDN, saisissez le nom de domaine complet par lequel le périphérique est accessible à partir d'Internet. Click OK.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
Advanced (Ontions	OU ISHOOD OSET SAKE 2	024 SSI Tructoriat	General Purpose	RSA (2048 bits)	Show Details
Auvanceu						Delete
Certificate Para	ameters Enrollment Mode	SCEP Challenge Password	e for self-signed certificates.			Export
						Install
FQDN:	asavpn.example.com					Re-Enrol
E-mail:						
IF Address:	arial number of the device					
	and number of the device					
		N				
		43				
	OY	Canad				

- 5. Générer et enregistrer le CSR
 - a. Cliquez sur Ajouter un certificat.

Issued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName= (CN=ca.example.com, OU	15: 10:00 CEST Fe	eb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🔄 Add Identity Cert	lificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
O Import the ident	ity certificate from a file (PK	CS12 format with C	Certificate(s)+	Private Key):			Install
Decryption Pass	phrase:						Re-Enroll
File to Import Fre	om:		Browse				
Add a new ident	ity certificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate Subje	ect DN: /pn.example.com,	O=example inc	Select				
Generate sel	If-signed certificate						
Act as lo	cal certificate authority and	issue dynamic certi	ficates to TLS	-Proxy			
			Г	Advanced			
Enable CA fi	ag in hasic constraints exter	nsion					
		131011					

b. Une invite s'affiche pour enregistrer le CSR dans un fichier sur l'ordinateur local.

sueu ru	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
Trustopiot Name	SSL Tructopint-20	22				Export
Import the id	dentity certificate from a file (PK	CS12 format with Certificate(s)+Private Key):			Install
(martine	in California Barran					Re-Enroll
F	ity Certificate Request		^			
To com reques	plete the enrollment process, pl t (CSR) and send it to the CA.	lease save the PKCS 10 enrollm	ent			
K You wil clicking C	then need to install the certification the Install button in the Identity	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			
	OK C	ancel Help				
		ince				
			Advanced			
	A first in basely and shall be automatically	nsion				

Cliquez sur Browse. Choisissez un emplacement dans lequel enregistrer le CSR, et enregistrez le fichier avec l'extension .txt.

Remarque : lorsque le fichier est enregistré avec une extension .txt, la demande PKCS#10 peut être ouverte et affichée à l'aide d'un éditeur de texte (tel que le Bloc-notes).

c. Le nouveau point de confiance est maintenant affiché à l'état En attente.

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
instructuredName=	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

Installer le certificat d'identité au format PEM avec ASDM

Les étapes d'installation supposent que l'autorité de certification a signé le CSR et fourni un nouveau certificat d'identité codé PEM (.pem, .cer, .crt) et un ensemble de certificats d'autorité de certification.

1. Installer le certificat AC qui a signé le CSR

Le certificat d'autorité de certification qui a signé le certificat d'identité peut être installé dans le point de confiance créé pour le certificat d'identité. Si le certificat d'identité est signé par une autorité de certification intermédiaire, ce certificat peut être installé dans le point de confiance du certificat d'identité. Tous les certificats d'autorité de certification en amont dans la hiérarchie peuvent être installés dans des points de confiance d'autorité de certification distincts.

a. Accédez à Configuration > Device Management > Certificate Management >, et choisissez CA Certificates. Cliquez sur Add.

Inducation > Device Mana	igement > Certificate Man	<u>agement</u> > <u>CA Certificates</u>				
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
uoVadis Root CA 2	CN=QuoVadis Root CA 2,	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	Luit
enTrust Commercial Root	CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Show Details

b. Entrez le nom du point de confiance et choisissez Install From File, cliquez sur Browse button, et choisissez le certificat intermédiaire. Vous pouvez également coller le certificat CA codé PEM d'un fichier texte dans le champ texte.

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				Request C
Install from a flou		Browse				Delete

Remarque : installez le certificat intermédiaire avec le même nom de point de confiance que le nom de point de confiance du certificat d'identité, si le certificat d'identité est signé par le certificat d'autorité de certification intermédiaire.

c. Cliquez sur Install Certificate.

ssued To	Issued By ^1	Expiry Date	Associated Trustpoints	Usage	Active		Add
.example.com	CN=ca.example.com, OU=I	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes		Edit
🧧 Install Certificate						×	Show Details
Trustpoint Name:	SSL-Trustpoint-2023]				Î	Request CRI
O Install from a file:		Browse				1	Delete
Paste certificate in	PEM format:						
OjskinYCbPfg3p2 VROOBVEFESK25 9EEV52147em9XL cGqeyDMRhs3Rs/m 25kqafixs153jW1 9Ky3H56BFlackN gW87HOvM08svy dcVcovO/Axmr4J END CERTIFIC Use EST: Specify source Inter EST URL: https:// Certificate Subject I allow-untrusted Use SCEP:	dH7W3h1K3prAgMBAAGJUDBOMU bragb9BLFV52U47emsUvAHB6GA D25M2wkAF4AY2H0M9K BC5M2wkAF4AY2H0M9K BKEPSAUtaN470fX0vH75 :/RRddfuxYf9seftbFHN8oc TXSUJf0UCdmAY4H60gdh H0g2rWFN3MXW2O4S3C ATE face:None	WGA LUGEWQFMAMBAf8wHQY UdIwQFMBaAFESSL2bra9b VArxXFwk3INBwOsYh5mgT formation INFO: Certificate ha Fingerprint: e9ad 165 Trustpoint CA certific	D s the following attributes: Sc 2673424c 6e7e0c5f b30b4a02 cate accepted.	×		v	
Specify source Inter	face: None	\sim					
SCEP URL: http://							
Date: Date:	4	minuter					

Dans l'exemple, le nouveau certificat est signé avec le même certificat CA que l'ancien. Le même certificat CA est désormais associé à deux Trustpoints.

Configuration > Device Management > Certificate Management > CA Certificates

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-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 Detai
						Request C
						Delete

- 2. Installer le certificat d'identité
 - a. Sélectionnez le certificat d'identité créé précédemment avec la génération CSR. Cliquez sur Install.

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 Detai
asavpn.example.com]	Not Available	Pending	SSL-Trustpoint-2023		Unknown		
							Delete
							Export
							Instal

Remarque : le champ Émis par du certificat d'identité peut avoir la valeur Non disponible, et le champ Date d'expiration la valeur En attente.

b. Choisissez un fichier qui contient le certificat d'identité codé PEM reçu de l'autorité de certification, ou ouvrez le certificat codé PEM dans un éditeur de texte, puis copiez et collez le certificat d'identité fourni par l'autorité de certification dans le champ de texte.

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.	com] Not Available	Pending	SSL-Trustpoint-2023		Unknown		Delete
							Delete
							Export
linstall Ident	ity certificate		×				Install
lentity Certifica	te						Re-Enrol
Install free	n a filos		Province				-
	ind nic.		browse				
O Paste the	certificate data in base-64 format						

Remarque : le certificat d'identité peut être au format .pem, .cer, .crt à installer.

c. Cliquez sur Install Certificate.

ssued 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.com	nj Not Available	Pending	SSL-1rustpoint-2023		Unknown		Delete
							Export
Install Identity	certificate		×				Install
entity Certificate							Re-Enrol
	e wait						
PIPAS							
Pieas	Informa	ation	×				
Preas	Please wait wf	ation	×				
Pre F G r: Preas	Please wait wf device	ation Certificate import succeede	x .d.				
Pre Pre Pre V	Please wait wi device	tion Certificate import succeede	.d.				
Preas	Please wait wir device	Certificate import succeede	d.				

Après l'installation, des certificats d'identité anciens et nouveaux sont présents.

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

3. Lier le nouveau certificat à l'interface avec ASDM

L'ASA doit être configuré pour utiliser le nouveau certificat d'identité pour les sessions

WebVPN qui se terminent sur l'interface spécifiée.

- a. Accédez à Configuration > Remote Access VPN > Advanced > SSL Settings.
- b. Sous Certificates, choisissez l'interface utilisée pour terminer les sessions WebVPN. Dans cet exemple, l'interface externe est utilisée.

Cliquez sur Edit.

c. Dans la liste déroulante Certificate, sélectionnez le nouveau certificat installé.

					Edit	
ſ	select SSL Certificate		×		Delete	
tificates	Specify enrolled trustpoints to be us OUTSIDE-direct interface. To enroll Management > Identity Certificates	ed for SSL authentication and VPN load balancing on the a trustpoint, go to Device Management > Certificate				
pecify which certificates, if an	Interface:	OUTSIDE-direct		ces not associated with a certificate of their own.		
Interface	Primary Enrolled Certificate:	SSL-Trustpoint-2023:unstructuredName=asavpn.exampl	~	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. Click OK.
- e. Cliquez sur Apply. Le nouveau certificat d'identité est maintenant utilisé.

	ss VPN > Advanced > <u>SSL Settings</u>			
				Edit Delete
ficates				-
ficates ecify which certificates, if a	ny, should be used for SSL authentication on eac	h interface. The fallback certificate will be us	sed on interfaces not associated with a certificate of their own.	Edt 1
ficates ecify which certificates, if a Interface	ny, should be used for SSL authentication on eac Primary Certificate	h interface. The fallback certificate will be us Load Balancing Certificate	sed on interfaces not associated with a certificate of their own. Key-Type	Edit
ficates ecify which certificates, if a Interface OUTSIDE-direct	ny, should be used for SSL authentication on eac Primary Certificate SSL=Trustpoint=2023:unstructure	h 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 ecify which certificates, if ar Interface OUTSIDE-direct inside	ny, should be used for SSL authentication on eac Primary Certificate SSL-Trustpoint-2023:unstructure	h 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-Vian	ny, should be used for SSL authentication on eac Primary Certificate SSL-Trustpoint-2023;unstructure	h 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

Renouveler un certificat inscrit avec un fichier PKCS12 avec ASDM

Le renouvellement du certificat inscrit PKCS12 nécessite la création et l'inscription d'un nouveau point de confiance. Il doit avoir un nom différent (par exemple, ancien nom avec suffixe de l'année d'inscription).

Le fichier PKCS12 (format .p12 ou .pfx) contient un certificat d'identité, une paire de clés et un ou plusieurs certificats d'autorité de certification. Il est créé par l'autorité de certification, par exemple, en cas de certificat générique, ou exporté à partir d'un autre périphérique. Il s'agit d'un fichier binaire qui ne peut pas être affiché avec l'éditeur de texte.

1. Installer le certificat d'identité renouvelé et les certificats CA à partir d'un fichier PKCS12

Le certificat d'identité, le ou les certificats d'autorité de certification et la paire de clés doivent être regroupés dans un fichier PKCS12 unique.

- a. Accédez à Configuration > Device Management > Certificate Management, et choisissez Identity Certificates.
- b. Cliquez sur Add.
- c. Spécifiez un nouveau nom de point de confiance.

ssued To	Issued By	Expiry Da	te	Associated Trustpoints	Usage	Public Key Type	Add
	1			1			Show Detai
🔤 Add Identity Ce	rtificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-	PKCS12					Export
Import the iden	ntity certificate from a file (PKCS12 format with	Certificate(s)+P	rivate Key):			Install
Decryption Pas	sphrase:						Re-Enrol
File to Import F	rom:		Browse				
O Add a new ider	ntity certificate:						
Key Pair:	<default-rsa+< td=""><td><ey> <</ey></td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa+<>	<ey> <</ey>	Show	New			
Certificate Sub	ject DN: CN=risavpn31		Select				
Generate s	elf-signed certificate						
Act as l	ocal certificate authority a	nd issue dynamic ce	rtificates to TLS-f	roxy			
				Advanted			
The Franklas CA	One in hereis ersetheinte ers	handland		Advanceu			
C Shaple CA	nag in basic constraints ex	lension					

d. Activez la case d'option Importer le certificat d'identité à partir d'un fichier.

Issued To	Issued By	Expiry Da	ate	Associated	Trustpoints	Usage	Pub	іс Кеу Туре		Add
										Show Detai
📴 Add Identity Cei	rtificate		D	(×					Delete
Trustnoint Name:	SSI -Trustpoint-i	WCS12	~		import ID certif	icate file				
Import the iden	tity certificate from a file (PKCS12 format wit	h Certificate(s)+P	rivate Kev)	Look in:	Document	ts	~	🥬 📂 🛄	
Decruption Page	robrace:	recore rormat ma	in cer uncate (a) in	indie neyj.	0	CSR.txt				
Eile to Import E	sprilase.		Brawaa			눩 vpn.exam	ple.com.pfx			
			Drowse		Recent Items					
Add a new iden	itity certificate:			_						
Key Pair:	<default-rsa-k< td=""><td>iey> 🗸</td><td>Show</td><td>New</td><td>Desktop</td><td></td><td></td><td></td><td></td><td></td></default-rsa-k<>	iey> 🗸	Show	New	Desktop					
Certificate Subj	ect DN: CN=risavpn31		Select							
Generate se	elf-signed certificate				Documents					
Act as k	ocal certificate authority ar	nd issue dynamic ce	ertificates to TLS-	Proxy						
					This PC F	ile name:	vpn.example.com.pf	x	Import ID (certificate file
				Advanced	- 🙈 F	iles of type:	All Files	~	Cr	ancel
Enable CA f	flag in basic constraints ext	ension								

e. Entrez la phrase de passe utilisée pour créer le fichier PKCS12.

ssued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
							Show Detail
add Identity Certif	ficate			×			Delete
Trustpoint Name:	SSL-Trustpoint-Pi	KCS12					Export
 Import the identit 	y certificate from a file (P	KCS12 format with C	Certificate(s)+Pri	vate Key):			Install
Decryption Passpl	hrase: ••••						Re-Enroll
File to Import From	m: C:\Users\cisco.D	ESKTOP-R2CH8G	Browse				
O Add a new identit	y certificate:						
Key Pair:	<default-rsa-ke< td=""><td>ey> ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-ke<>	ey> ~	Show	New			
Certificate Subject	t DN: CN=risavpn31		Select				
Generate self	-signed certificate						
Act as loc	al certificate authority and	d issue dynamic certi	ficates to TLS-P	oxy			
				Idvanced			
Enable CA flag	n in basic constraints exte	ension					
	g						

f. Cliquez sur Add Certificate.

issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
🔁 Add Identity Ce	ertificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-I	PKCS12				Export
Import the ide	ntity certificate from a file (PKCS12 format with Certificate	(s) +Private Key):			Install
Decryption Pas	ssphrase: ••••					Re-Enroll
File to Import F	From: C:\Users\cisco.0	DESKTOP-R2CH8G Browse.				
🔿 Add 🗧 Ple	ase wait		X Information			
Key F	Please wait while ACDM	is delivering the command(s) to	a the			^
Certi TD	device	is derivering the communication	G Created trustmint	s for CAs bigher in the big	ararchy as the CA certificate was not s	elf-cioned
¢	J			a for CAShigher in the file	and ty as the CA cel theate was not a	en agrico.
0			WARNING: CA cer	tificates can be used to va	alidate VPN connections,by default. Ple	ase adjust
			the validation-usa	ge of this trustpoint to limi	it the validation scope, if necessary	
			Import PKCS12 op	eration completed success	sfully.	
Enable CA	flag in basic constraints ext	tension			i cii și	

Remarque : lorsqu'une chaîne PKCS12 avec certificats d'autorités de certification est importée, l'ASDM crée automatiquement les points de confiance des autorités de certification en amont avec des noms avec le suffixe -number ajouté.

Configuration > Remote Access VPN > Certificate Management > CA Certificates

Issued To	√ 1	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. Lier le nouveau certificat à l'interface avec ASDM

L'ASA doit être configuré pour utiliser le nouveau certificat d'identité pour les sessions WebVPN qui se terminent sur l'interface spécifiée.

a. Accédez à Configuration > Remote Access VPN > Advanced > SSL Settings.

b. Sous Certificates, choisissez l'interface utilisée pour terminer les sessions WebVPN. Dans cet exemple, l'interface externe est utilisée.

Cliquez sur Edit.

c. Dans la liste déroulante Certificate, sélectionnez le nouveau certificat installé.

		Let autore		Edit
rtificates	Select SSL Certificate Specify enrolled trustpoints to be use OUTSIDE-direct interface. To enrol a Management > Identity Certificates. Interface: Primary Enrolled Certificate:	ed for SSL authentication and VPN load balancing on the strustpoint, go to Device Management > Certificate OUTSIDE-direct SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u	es not associated with a certificate of their own.	
Interface OUTSIDE-direct inside inside-vlan management	Load Balancing Enrolled Certificate:	Cancel Help	Кеу-Туре	Edit
Fallback Certificate: Forced Certification Authentica	None	2 minutes		

- d. Click OK.
- e. Cliquez sur Apply.

Certif	Certificates									
Spe	Specify which certificates, if any, should be used for SSL authentication on each interface. The failback 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						

Le nouveau certificat d'identité est maintenant utilisé.

Vérifier

Suivez ces étapes afin de vérifier que l'installation du Certificat du Fournisseur tiers est réussie et que les connexions VPN SSL sont utilisées.

Afficher les certificats installés via ASDM

- 1. Accédez à Configuration > Remote Access VPN > Certificate Management, et choisissez Identity Certificates.
- 2. Le certificat d'identité émis par le fournisseur tiers peut s'afficher.

Certi Sp	rtificates							
	Interface	Primary Certificate	Load Balancing Certificate	Кеу-Туре	Edit			
	OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName =F		Primary: RSA (2048 bits), Load Balan				

Dépannage

Cette commande debug doit être collectée sur l'interface de ligne de commande en cas d'échec de l'installation du certificat SSL.

• debug crypto ca 14

Forum aux questions

Q.Qu'est-ce qu'un PKCS12 ?

R.Dans le domaine de la cryptographie, PKCS12 définit un format de fichier d'archive créé pour stocker de nombreux objets de cryptographie sous la forme d'un fichier unique. Il est couramment utilisé pour regrouper une clé privée avec son certificat X.509 ou pour regrouper tous les membres d'une chaîne de confiance.

Q.Qu'est-ce qu'une RSE ?

R. Dans les systèmes d'infrastructure à clé publique (ICP), une demande de signature de certificat (également une demande de CSR ou de certification) est un message envoyé par un demandeur à une autorité d'enregistrement de l'infrastructure à clé publique afin de demander un certificat d'identité numérique. Il contient généralement la clé publique pour laquelle le certificat peut être émis, les informations utilisées pour identifier le certificat signé (par exemple, un nom de domaine dans Subject) et la protection de l'intégrité (par exemple, une signature numérique).

Q. Où se trouve le mot de passe de PKCS12 ?

R. Lorsque les certificats et les paires de clés sont exportés vers un fichier PKCS12, le mot de passe est indiqué dans la commande export. Pour importer un fichier pkcs12, le mot de passe doit être fourni par le propriétaire du serveur AC ou par la personne qui a exporté le PKCS12 à partir d'un autre périphérique.

Q. Quelle est la différence entre la racine et l'identité ?

R.Dans le domaine de la cryptographie et de la sécurité informatique, un certificat racine est un certificat à clé publique qui identifie une autorité de certification racine. Les certificats racine sont auto-signés (et il est possible qu'un certificat ait plusieurs chemins d'accès d'approbation, par exemple si le certificat a été émis par un racine qui a été signé de manière croisée) et forment la base d'une infrastructure de clé publique (PKI) basée sur X.509. Un certificat de clé publique, également appelé certificat numérique ou certificat d'identité, est un document électronique utilisé pour prouver la propriété d'une clé publique. Le certificat comprend des informations sur la clé, des informations sur l'identité de son propriétaire (appelée objet) et la signature numérique d'une entité qui a vérifié le contenu du certificat (appelée émetteur). Si la signature est valide et que le logiciel qui examine le certificat fait confiance à l'émetteur, il peut utiliser cette clé pour communiquer en toute sécurité avec l'objet du certificat.

Q.J'ai installé le certificat, pourquoi il ne fonctionne pas ?

R. Cela pourrait être dû à de nombreuses raisons, par exemple :

1. Le certificat et le point de confiance sont configurés, mais ils n'ont pas été liés au processus qui

devrait l'utiliser. Par exemple, le point de confiance à utiliser n'est pas lié à l'interface externe qui termine les clients Anyconnect.

2. Un fichier PKCS12 est installé, mais présente des erreurs en raison de l'absence du certificat d'autorité de certification intermédiaire dans le fichier PKCS12. Les clients dont le certificat d'autorité de certification intermédiaire est approuvé, mais dont le certificat d'autorité de certification racine n'est pas approuvé, ne sont pas en mesure de vérifier l'ensemble de la chaîne de certificats et de signaler le certificat d'identité du serveur comme n'étant pas approuvé.

3. Un certificat renseigné avec des attributs incorrects peut entraîner un échec de l'installation ou des erreurs côté client. Par exemple, certains attributs peuvent être codés avec un format incorrect. Une autre raison est que le certificat d'identité ne contient pas de nom alternatif de sujet (SAN) ou que le nom de domaine utilisé pour accéder au serveur n'est pas présent en tant que SAN.

Q. L'installation d'un nouveau certificat nécessite-t-elle une fenêtre de maintenance ou entraîne-telle des temps d'arrêt ?

R. L'installation d'un nouveau certificat (identité ou autorité de certification) n'est pas intrusive et ne devrait pas entraîner d'interruption ou nécessiter une fenêtre de maintenance. L'activation d'un nouveau certificat pour un service existant est une modification et peut nécessiter une demande de modification / une fenêtre de maintenance.

Q. L'ajout ou la modification d'un certificat peut-il déconnecter les utilisateurs connectés ? R.Non, les utilisateurs actuellement connectés restent connectés. Le certificat est utilisé lors de l'établissement de la connexion. Une fois les utilisateurs reconnectés, le nouveau certificat est utilisé.

Q. Comment créer une demande de service client avec un caractère générique ? Ou un autre nom de sujet (SAN) ?

R. Actuellement, l'ASA/FTD ne peut pas créer de CSR avec un caractère générique ; cependant, ce processus peut être effectué avec OpenSSL. Pour générer la clé CSR et ID, vous pouvez exécuter les commandes suivantes :

openssl genrsa -out id.key 2048

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

Lorsqu'un point de confiance est configuré avec l'attribut FQDN (Fully Qualified Domain Name), le CSR créé par ASA/FTD contient le SAN avec cette valeur. L'autorité de certification peut ajouter d'autres attributs SAN lorsqu'elle signe le CSR, ou le CSR peut être créé avec OpenSSL

Q. Le remplacement du certificat prend-il effet immédiatement ?

R. Le nouveau certificat d'identité du serveur est utilisé uniquement pour les nouvelles connexions. Le nouveau certificat est prêt à être utilisé immédiatement après la modification, mais il est en fait utilisé avec les nouvelles connexions.

Q.Comment puis-je vérifier si l'installation a fonctionné ?

A.La commande CLI pour vérifier : show crypto ca cert <trustpointname>

Q.Comment générer PKCS12 à partir d'un certificat d'identité, d'un certificat d'autorité de certification et d'une clé privée ?

R. PKCS12 peut être créé avec OpenSSL, avec la commande : openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt

Q. Comment exporter un certificat pour l'installer dans un nouvel ASA ? A.

- Avec l'interface de ligne de commande : utilisez la commande : crypto ca export <trustpointname> pkcs12 <password>
- Avec ASDM :
 - a. Accédez à Configuration > Device Management > Certificate Management > Identity Certificates et choisissez Identity Certificate. Cliquez sur Exporter.

File View Tools Wizards Wind	low Help					Type topic to search	Go	ahaha
Home 🆓 Configuration 🔯 Me	onitoring 🔚 Save 🔇 Refre	esh 🔇 Back 🔘 Forwar	d 🦻 Help					cisco
Bookmarks 🗗 🗘 🗙	Configuration > Device Ma	nagement > Certificate N	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 unstructuredName =risav unstructuredName =risav [asa.vpn.example.com]	[CN=ca.example.com, OU CN=ca.example.com, OU CN=KrakowCA-sub1-1 Not Available	16:10:00 CEDT Apr 6 2024 15:10:00 CEST Feb 6 2024 04:44:00 CEST Dec 21 2024 Pending	SSL-Trustpoint-2023 SSL-Trustpoint SSL-Trustpoint-PKCS12 SSL-Trustpoint	General Purpose General Purpose General Purpose Unknown	RSA (4096 bits) RSA (2048 bits) RSA (2048 bits)		Show Details Delete Export Instal Re-Enroll
Device Management 2 4	Finds	A Match Case						
Smart Call-Home Goud Web Security Service Module Settings GU Sers/AAA Cortificate Management An Identity Certificates	Certificate Expiration Alerts Send the first alert befor Repeat Alert Interval :	e : 60 (days) Set Def 7 (days)	ault					

b. Choisissez où exporter le fichier, spécifiez le mot de passe d'exportation, cliquez sur Export Certificate.

ssued To I	ssued By	Expiry Date	Associated Trustpoints	Usa	age	Public Key Type	Add
nstructuredName=asav C	N=ca.example.com, OU	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023		General Purpose	RSA (4096 bits)	Show Detail
nstructuredName=risav C	N=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detail
nstructuredName=FTD7 C	N=KrakowCA-sub1-1	04:44:00 CEST Dec 21 2024	SSL-Trustpoint-PKCS12		General Purpose	RSA (2048 bits)	Delete
sa.vpn.example.com] N	ot Available	Pending	SSL-Trustpoint		Unknown		Export
							Export
							Install
							Re-Enroll
nd:	🕥 🗋 Match Case						
nd: (🕤 🙆 🗌 Match Case						
nd: () (rtificate Expiration Alerts —	🕤 🔘 🗌 Match Case						
nd:	O Match Case O (days) Set Defa	ult					
nd:	Match Case 60 (days) Set Defa 7 (days)	ult					
nd: () () () () () () () () () () () () ()	 Match Case (days) Set Defa (days) Export certificate 	ut		×	_		
nd:	 Match Case (days) Set Defa (days) Export certificate 	ut		×)		
nd: () () () () () () () () () () () () ()	 Match Case (days) Set Defa (days) Export certificate Export to File: 	ult C: (Users/cisco.DESKTOP4	R2CH8G5\Documents\ce Browse.	×	1		
nd: () tificate Expiration Alerts	O Match Case Match Case (days) Set Defa (days) Export certificate Export to File: Certificate Format	ult C:\Users\disco.DESKTOP4	R2CH8G5\Documents\ce	×	1		
nd: () tificate Expiration Alerts — Send the first alert before : Repeat Alert Interval : Crypto Configurations — Permit Weak key sizes and I CA Enrollment — CA Enrollment — Sec Cross A&C sec vity to be	 Match Case (days) Set Defa (days) Export certificate Export to File: Certificate Format: 	ult C:\Users\cisco.DESKTOP4	R2CH8G5\Documents\ce Browse.	×		populational price for partificat	
nd:	Match Case Match Case (days) Set Defa Case Export certificate Export to File: Certificate Format:	C:\Users\cisco.DESKTOP4	R2CH8G5\Documents\ce Browse.	×	stomers a special	promotional price for certificat	es and trial certificates
nd: () () () () () () () () () () () () ()	O Match Case Match Case (days) Set Defa (days) Export certificate Export to File: Certificate Format:	C: Users\cisco.DESKTOP4 PKCS12 Format (Certified)	R2CH8G5\Documents\ce Browse.	×	stomers a special	promotional price for certificat	es and trial certificates
nd: () tificate Expiration Alerts	Match Case Match Case (days) Set Defa (days) Export certificate Export to File: Certificate Format:	Ult C:\Users\cisco.DESKTOP+ @ PKCS12 Format (Certificat _ PEM Format (Certificat	R2CH8G5\Documents\ce Browse. ficate(s) + Private Key) te Orly)	×	stomers a special	promotional price for certificat	es and trial certificates
nd: (tificate Expiration Alerts Send the first alert before : Repeat Alert Interval : Crypto Configurations Permit Weak key sizes and I CA Enrollment ; your Cisco ASA security app ting.	O Match Case O (days) Set Defa (days) Export certificate Export to File: Certificate Format:	Ult C:\Users\disco.DESKTOP+ @ PKCS12 Format (Certificat PEM Format (Certificat	R2CH8G5\Documents\ce Browse. ficate(s) + Private Key) te Only)	× 	stomers a special	promotional price for certificat	es and trial certificates
nd: () () () () () () () () () () () () ()	O Match Case Match Case (days) Set Defa 7 (days) Export certificate Export to File: Certificate Format: dat Configuration Encryptic	Ult C: \Users\cisco.DESKTOP4 @ PKCS 12 Format (Certificat O PEM Format (Certificat in Passphrase	R2CH8G5\Documents\ce Browse. ficate(s) + Private Key) te Only)	× 	stomers a special	promotional price for certificat	es and trial certificates
nd: () tificate Expiration Alerts — Send the first alert before : Repeat Alert Interval : Crypto Configurations — Permit Weak key sizes and t CA Enrollment — : your Cisco ASA security app ting. ng a previously saved certifi	Match Case Match Case Match Case (days) Set Defa Cays) Export certificate Export to File: Certificate Format:	ult C:\Users\oisco.DESKTOP+ @ PKCS 12 Format (Certif O PEM Format (Certificat in Passphrase se:	R2CH8G5\Documents\ce Browse. ficate(s) + Private Key) te Only)	× 	stomers a special	promotional price for certificat	es and trial certificates
nd: (tificate Expiration Alerts Send the first alert before : Repeat Alert Interval : Crypto Configurations Permit Weak key sizes and I CA Enrollment your Cisco ASA security app ting. ng a previously saved certifi Identity Certificate Wizard	Match Case Match Case (days) Set Defa (days) Export certificate Export to File: Certificate Format:	elt C:\Users\disco.DESKTOP+ @ PKCS12 Format (Certificat	R2CH8G5\Documents\ce Browse. ficate(s) + Private Key) te Only)	× 	stomers a special	promotional price for certificat	es and trial certificates t
hd:	Match Case Match Case (days) Set Defa (days) Export certificate Export to File: Certificate Format: Certificate Format: Certificate Format: Configuration Encryption Encryption Passphrase: Confirm passphrase:	ult C:\Users\disco.DESKTOP4 @ PKCS 12 Format (Certif O PEM Format (Certificat in Passphrase se: •••••	R2CH8G5\Documents\ce Browse. ficate(s) + Private Key) te Only)	× :	stomers a special cher.	promotional price for certificat	es and trial certificates t

Le certificat exporté peut se trouver sur le disque de l'ordinateur. Veuillez prendre note de la phrase de passe dans un endroit sûr, le fichier est inutile sans elle.

Q. Si des clés ECDSA sont utilisées, le processus de génération de certificat SSL est-il différent ? R. La seule différence de configuration est l'étape de génération de paire de clés, où une paire de clés ECDSA peut être générée à la place d'une paire de clés RSA. Le reste des étapes reste le même.

Q. Est-il toujours nécessaire de générer une nouvelle paire de clés ?

R. L'étape de génération de la paire de clés est facultative. La paire de clés existante peut être utilisée ou, dans le cas de PKCS12, la paire de clés est importée avec le certificat. Reportez-vous à la section Sélectionner le nom de la paire de clés pour le type d'inscription/réinscription correspondant.

Q. Est-il sûr de générer une nouvelle paire de clés pour un nouveau certificat d'identité ? R.Le processus est sûr tant qu'un nouveau nom de paire de clés est utilisé. Dans ce cas, les anciennes paires de clés ne sont pas modifiées.

Q. Faut-il générer à nouveau une clé lorsqu'un pare-feu est remplacé (comme RMA) ?
R.Le nouveau pare-feu n'a pas de paires de clés sur l'ancien pare-feu.
La sauvegarde de la configuration en cours ne contient pas les paires de clés.
La sauvegarde complète effectuée avec ASDM peut contenir les paires de clés.
Les certificats d'identité peuvent être exportés à partir d'un ASA avec ASDM ou CLI, avant qu'il

n'échoue.

En cas de paire de basculement, les certificats et les paires de clés sont synchronisés sur une unité en veille avec la commande write standby. En cas de remplacement d'un noeud de la paire de basculement, il suffit de configurer le basculement de base et de transmettre la configuration au nouveau périphérique.

Si une paire de clés est perdue avec le périphérique et qu'il n'y a pas de sauvegarde, un nouveau certificat doit être signé avec la paire de clés présente sur le nouveau périphérique.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.