Installazione e rinnovo dei certificati su un'appliance ASA gestita da ASDM

Sommario

Introduzione **Prerequisiti Requisiti** Componenti usati Premesse Richiedere e installare un nuovo certificato di identità con ASDM Richiedere e installare un nuovo certificato di identità con richiesta di firma del certificato (CSR) Generare un CSR con ASDM Creazione di un trust point con un nome specifico (Facoltativo) Creare una nuova coppia di chiavi Scegliere il nome della coppia di chiavi Configurare il soggetto del certificato e il nome di dominio completo (FQDN) Generare e salvare il CSR Installare il certificato di identità in formato PEM con ASDM Installa certificato CA con firma CSR Installa certificato di identità Associare il nuovo certificato all'interfaccia con ASDM Installare un certificato di identità ricevuto nel formato PKCS12 con ASDM Installare i certificati di identità e CA da un file PKCS12 Associare il nuovo certificato all'interfaccia con ASDM **Rinnovo certificato** Rinnova un certificato registrato con Richiesta di firma del certificato (CSR) con ASDM Generare un CSR con ASDM Creare un nuovo trust point con un nome specifico. (Facoltativo) Creare una nuova coppia di chiavi Selezionare il nome della coppia di chiavi Configurare il soggetto del certificato e il nome di dominio completo (FQDN) Generare e salvare il CSR Installare il certificato di identità in formato PEM con ASDM Installa certificato CA con firma CSR Installa certificato di identità Associare il nuovo certificato all'interfaccia con ASDM Rinnova un certificato registrato con un file PKCS12 con ASDM Installare il certificato di identità e i certificati CA rinnovati da un file PKCS12 Associare il nuovo certificato all'interfaccia con ASDM Verifica Visualizza certificati installati tramite ASDM Risoluzione dei problemi

Introduzione

Questo documento descrive come richiedere, installare, considerare attendibili e rinnovare alcuni tipi di certificati su software Cisco ASA gestito con ASDM.

Prerequisiti

Requisiti

- Prima di iniziare, verificare che l'ora, la data e il fuso orario di Adaptive Security Appliance (ASA) siano corretti. Con l'autenticazione dei certificati, si consiglia di usare un server Network Time Protocol (NTP) per sincronizzare l'ora sull'appliance ASA. Consultare Informazioni correlate per riferimento.
- Per richiedere un certificato che utilizza la richiesta di firma del certificato (CSR), è
 necessario disporre dell'accesso a un'Autorità di certificazione (CA) interna o di terze parti
 attendibile. Esempi di fornitori di CA di terze parti includono, tra gli altri, Entrust, Geotrust,
 GoDaddy, Thawte e VeriSign.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASAv 9.18.1
- Per la creazione di PKCS12, viene utilizzato OpenSSL.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I tipi di certificati a cui si riferisce il documento sono:

- certificati autofirmati
- · certificati firmati da un'autorità di certificazione di terze parti o da una CA interna

SSL (Secure Sockets Layer), TLS (Transport Layer Security) e IKEv2 rfc7296 per i protocolli di autenticazione EAP richiedono che il server SSL/TLS/IKEv2 fornisca al client un certificato server per eseguire l'autenticazione del server. A tale scopo, è consigliabile utilizzare CA di terze parti attendibili per rilasciare certificati SSL all'appliance ASA.

Cisco sconsiglia di utilizzare un certificato autofirmato perché potrebbe essere impossibile

configurare inavvertitamente un browser per considerare attendibile un certificato rilasciato da un server non autorizzato. Vi è inoltre l'inconveniente per gli utenti di dover rispondere a un avviso di sicurezza quando si connette al gateway sicuro.

Richiedere e installare un nuovo certificato di identità con ASDM

È possibile richiedere un certificato a un'Autorità di certificazione (CA) e installarlo su un'appliance ASA in due modi:

- Utilizzare la richiesta di firma del certificato (CSR). Generare una coppia di chiavi, richiedere un certificato di identità a una CA con un CSR, installare il certificato di identità firmato ottenuto dalla CA.
- Utilizzare un file PKCS12 ottenuto da una CA o esportato da un dispositivo diverso. Il file PKCS12 contiene la coppia di chiavi, il certificato di identità e i certificati CA.

Richiedere e installare un nuovo certificato di identità con richiesta di firma del certificato (CSR)

Sul dispositivo viene creato un CSR che richiede un certificato di identità. Utilizzare una coppia di chiavi creata sul dispositivo.

Un CSR contiene:

- informazioni sulla richiesta di certificato oggetto richiesto e altri attributi, chiave pubblica dalla coppia di chiavi,
- informazioni sull'algoritmo della firma,
- firma digitale delle informazioni della richiesta di certificato, firmata con la chiave privata dalla coppia di chiavi.

Il CSR viene passato all'Autorità di certificazione (CA), in modo che lo firmi, in un formato PKCS#10.

Il certificato firmato viene restituito dalla CA in un modulo PEM.

Nota: quando firma il CSR e crea un certificato di identità firmato, CA può modificare i parametri FQDN e Nome soggetto definiti nel Trustpoint.

Generare un CSR con ASDM

- 1. Creazione di un trust point con un nome specifico
 - a. Passare a Configurazione > Gestione dispositivi > Gestione certificati > Certificati di identità.



- b. Fare clic su Add.
- c. Definire un nome di trust.

sued To Issued	By Expiry	Date	Associated Trustpoints	^1 Usage	Public Key Type	Add
Add Identity Certificate					×	Show Deta
Trustpoint Name:	L-Trustpoint	1				Delete
Import the identity certificate	e from a file (PKCS12 format	with Certificate(s)+Pr	ivate Key):			Export
Decryption Passphrase:						Install
File to Import From:		Browse				Re-Enrol
Add a new identity certificate	21					
Key Pair: <	Default-RSA-Key>	/ Show	New			
Certificate Subject DN: CN	=asavpn.example.com	Select				
Generate self-signed cer	tificate					
Act as local certificate	e authority and issue dynami	certificates to TLS-P	roxy		_	
		_	Advanced		-	
Enable CA flag in basic co	onstraints extension		Harancean			

- d. Fare clic sul pulsante di opzione Aggiungi nuovo certificato di identità.
- 2. (Facoltativo) Creare una nuova coppia di chiavi

Nota: per impostazione predefinita, viene utilizzata la chiave RSA con il nome Default-RSA-Key e una dimensione di 2048; tuttavia, si consiglia di utilizzare una coppia di chiavi pubblica/privata univoca per ciascun certificato di identità.

a. Fare clic su Nuovo per generare una nuova coppia di chiavi.

sued To	Issued By	Expiry Date	Associated Trust	points	Usage	Public Key Type	Add
Add Identity Cert	ificate			×	General Purpose	RSA (4096 bits)	Show Detail
				_	General Purpose	RSA (2048 bits)	Delete
Trustpoint Name:	SSL-Trustpoint						
O Import the ident	ity certificate from a file ((PKCS12 format with Certificate	(s)+Private Key):				Export
Decryption Pass	phrase:						Install
File to Import Fre	om:	Browse					Re-Enrol
Add a new ident	ity certificate:						
Key Pair:	<default-rsa-< td=""><td>Key> ~ 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	lf-signed certificate						
Act as lo	cal certificate authority a	nd issue dynamic certificates to	TLS-Proxy				
			Advanced				
Enable CA fl	ag in basic constraints ex	tension					

- b. Scegliere l'opzione Immettere il nome della nuova coppia di chiavi e immettere un nome per la nuova coppia di chiavi.
- c. Scegliere il tipo di chiave: RSA o ECDSA.
- d. Scegliere le dimensioni della chiave; per RSA, scegliere Uso generico.
- e. Fare clic su Genera ora. La coppia di chiavi è stata creata.

	Issued by	Expiry Date	Associated Trustpoin	nts	Usage	Public Key Type	Add
🔄 Add Identity Cert	ificate			×	General Purpose	RSA (4096 bits) RSA (2048 bits)	Show Deta
Trustpoint Name:	SSL-Trustpoint			2.	deneral rapose		Delete
🔿 Impor 🔂 Add	Key Pair		×				Export
Decry		0.50004 0.5	2224				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	e O Special	63				
	Generate Now	Cancel	Help				

3. Scegliere il nome della coppia di chiavi

Scegliere la coppia di chiavi con cui firmare il CSR e da associare al nuovo certificato.

ssued To	Issued By	Expiry Date	Associated Trust	points	Usage	Public Key Type	Add
Add Identity C	ertificate			×	General Purpose	RSA (4096 bits)	Show Detail
				_	General Purpose	RSA (2048 bits)	Delete
Trustpoint Name:	SSL-Trustpoint						Export
O Import the ide	entity certificate from a file ((PKCS12 format with Certificate	:(s)+Private Key):				Export
Decryption Pa	assphrase:						Install
File to Import	From:	Browse					Re-Enrol
Add a new ide	entity certificate:						
Key Pair:	SSL-Keypair	Show	New				
Certificate Sul	bject DN: CN=asavpn.ex	ample.com Select.	••				
Generate	self-signed certificate						
Act as	s local certificate authority a	nd issue dynamic certificates to	TLS-Proxy				
			Advanced				
Enable CA	A flag in basic constraints ex	tension					
Enable CA	A flag in basic constraints ex	tension	Advanced				

4. Configurare il soggetto del certificato e il nome di dominio completo (FQDN)

Attenzione: il parametro FQDN deve corrispondere all'FQDN o all'indirizzo IP dell'interfaccia ASA per cui viene utilizzato il certificato di identità. Questo parametro imposta l'estensione SAN (Subject Alternative Name) richiesta per il certificato di identità. L'estensione SAN viene utilizzata dal client SSL/TLS/IKEv2 per verificare se il certificato corrisponde all'FQDN a cui si connette.

a. Fare clic su Seleziona.

Issued To	Issued By	Expiry Date	Associated Trustpoints	∧¹ Usa	ge Public Key Type	e	Add
🛓 Add Identity Ce	rtificate	· · · ·				×	Show Detail
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the iden	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 l	ocal certificate authority an	d issue dynamic certificates to TL	S-Proxy			-	
			Advanted				
	0		Advanced				
	nag in basic constraints exte	ension					

b. Nella finestra DN soggetto certificato, configurare gli attributi del certificato - scegliere l'attributo dall'elenco a discesa, immettere il valore e fare clic su Aggiungi.

sued To	Issued By	Expiry Date	Associated Trustpoints	^1 Us	age	Public Key Type	Add
Add Identity Certificat	e					×	Show Detai
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the identity ce	Cartificata Subject	DN			×		Export
Decryption Passphrase	Certificate Subject				^		Install
File to Import From:			Attribute	Value			Re-Enrol
Add a new identity cer Key Pair: Certificate Subject DN	DN Attribute to b Attribute: Con Value: asa.	e Added moon Name (CN) v	Add>>				
Generate self-sign		~	Cancel Hole				
🔄 Enable CA flag in t		UK	Cancel hep				

ssued To	Issued By	Expiry Date	Assoc	iated Trustpoints	~1	Usage	Public Key Type	Add
Add Identity Certificat	e).	×	Show Detai
Trustpoint Name:	SSL-Trustpoint							Delete
O Import the identity ce	Certificate Subi	ect DN				×		Export
Decryption Passphras	Certificate Subj					~		Install
File to Import From:				Attribute	Value			Re-Enrol
Add a new identity ce	DN Attribute to	o be Added		Common Name (C	N) asa.vpn.e	exam		
Key Pair:	Attribute: C	Country (C) V	Add>>					
Certificate Subject DN	Value: D	epartment (OU)	Delete					
Generate self-sign	C	Company Name (O)						
Act as local ce	s	tate (St)						
	E	mail Address (EA)						
		ОК	Cancel	Help				

Attributo	Descrizione
CN	Il nome attraverso il quale è possibile accedere al firewall (in genere il nome di dominio completo, ad esempio vpn.example.com).
UO	Il nome del reparto all'interno dell'organizzazione
0	La ragione sociale legalmente registrata dell'azienda
С	Codice paese (codice a 2 lettere senza punteggiatura)
ST	Stato in cui si trova l'organizzazione.
L	Città in cui si trova l'organizzazione.
EA	Indirizzo email

Nota: nessuno dei valori dei campi precedenti può superare il limite di 64 caratteri. Un valore più lungo può causare problemi con l'installazione del certificato di identità. Inoltre, non è necessario definire tutti gli attributi DN.

Dopo aver aggiunto tutti gli attributi, fare clic su OK.

c. Configurare l'FQDN del dispositivo - fare clic su Avanzate.

ssued To	Issued By	Expiry Date	Associated Trustpoin	ts ^1	Usage	Public Key Type	Add
Add Identity Ce	ertificate					×	Show Detai
Trustpoint Name:	SSL-Trustpoint						Delete
○ Import the ide	entity certificate from a file (P	KCS12 format with Certi	ficate(s)+Private Kev):				Export
Decryption Pa	ssphrase:						Install
File to Import i	From:	Bro	owse				Re-Enrol
Add a new ide	entity certificate:		<u></u>				
Key Pair:	SSL-Keypair	√ Sł	New				
Certificate Sub	oject DN: CN=asa.vpn.exa	mple.com Se	lect				
Generate :	self-signed certificate						
Act as	local certificate authority and	d issue dynamic certificat	es to TLS-Proxy				
_			Advanced				
Enable CA	flag in basic constraints exte	nsion					
		-					
		Add Certificate	Cancel He	lo de			

d. Nel campo FQDN immettere il nome di dominio completo tramite il quale il dispositivo è accessibile da Internet. Fare clic su OK.

Issued To	Issund D.	Evolet Data	Associated Trustasiate	A 1 Unan	Public Key Type	Add
Add Identity Ce	rtificate Advanced	Options		×	×	Show Detai
Trustnoint Name:	Enrollment mode	e parameters and SCEP challen	ge password are not available for se	If-signed certificates.		Delete
Import the ider	ertifica	ameters Enrollment Mode S	CEP Challenge Password			Export
Decryption Pas	sphrase: FQDN:	asavpn.example.com				Install
File to Import F	From: E-mail:					Re-Enrol
Add a new ider	IP Address:					
Key Pair:	S Include s	erial 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			1.1		

- 5. Generare e salvare il CSR
 - a. Fare clic su Aggiungi certificato.

sued To	Issued By	Expiry D	ate	Associated Trustpoints	^1	Usage	Public Key T	ype	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)+Pr	ivate Kev):					Export
Decryption Passphi	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.exar	nple.com	Select						
Generate self-	signed certificate								
Act as local	certificate authority and	issue dynamic ce	rtificates to TLS-P	roxy				-	
			_						
				Advanced					
Enable CA flag	in basic constraints exter	ISION							

b. Viene visualizzato un prompt per salvare il CSR in un file sul computer locale.

ssued To	Issued By	Expiry Date	Associated Trustpoints	^1	Usage	Public Key Type	Add
🔄 Add Identity Ce	ertificate					×	Show Details
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the ider	ntity certificate from a file (PK	CS12 format with Certificate(s)	+Private Kev):				Export
Decryption Pas	ssphrase:						Install
File to Import F	From:	dentity Certificate Request		×			Re-Enroll
Add a new ider	ntity certificate: To	complete the enrollment proces	s, please save the PKCS10 enrollmen	t			
Key Pair:	SSL-Keypa	u will then need to install the ce	rtificate that is returned from the CA	v			
Certificate Sub	oject DN: CN=asa.vp clic	king the Install button in the Id	entity Certificates panel.	.,			
Generate s	self-signed certificate Sa	ve CSR to File:	Brow	se			
Act as	local certificate author		Course La Links				
		UK	Cancel Help				
			Advanced				
Enable CA	flag in basic constraints exter	ision					
				-			
		Add Certificate	Cancel Help				

Fare clic su Sfoglia, scegliere il percorso in cui salvare il CSR e salvare il file con estensione txt.

Nota: quando il file viene salvato con estensione .txt, è possibile aprire e visualizzare la richiesta PKCS#10 con un editor di testo, ad esempio Blocco note.

c. A questo punto il nuovo trust point viene visualizzato in stato In sospeso.

sued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
a.vpn.example.com]	Not Available	Pending	SSL-Trustpoint	Unknown		Show Deta
						Delete
						Export

Installare il certificato di identità in formato PEM con ASDM

Nelle procedure di installazione si presuppone che l'autorità di certificazione abbia firmato il CSR e abbia fornito un certificato di identità con codifica PEM (.pem, .cer, .crt) e un bundle di certificati CA.

- 1. Installa certificato CA con firma CSR
 - a. Passare a Configurazione > Gestione dispositivi > Gestione certificati > e scegliere Certificati CA. Fare clic su Add.

Configuration > Remote Acc	cess VPN > Certificate Mana	igement > <u>CA Certificates</u>				
A.						
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	Luit

b. Immettere il nome del Trustpoint e selezionare Installa da file, fare clic sul pulsante Sfoglia e selezionare il certificato intermedio. In alternativa, incollare il certificato CA con codifica PEM da un file di testo nel campo di testo.

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 C
Trustpoint Name:	SSL-Trustpoint					Delete
Install from a file:		Browse				
O Paste certificate in	PEM format:					

Nota: installare il certificato CA che ha firmato il CSR e utilizzare lo stesso nome del trust point del certificato di identità. Gli altri certificati CA di livello superiore nella gerarchia PKI possono essere installati in punti di attendibilità separati.

c. Fare clic su Installa certificato.

ssueu ro	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	C.da
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	Cl. Trustaniat	1				Request CRI
Trusquine Name.	SSE-Traspoint					Delete
O Install from a file:		Browse				
Paste certificate in PE	EM format:					
CGGeyCMRIns3Rs/wD 29kqaRijsx153)/ML0 QRxy3la1568FlacAkc7 gW8YnHOvM08xyT dcCrovD(PAxnrAl) + END CERTIFICAT O Use EST: Specify source Interfi EST URL: https:// Certificate Subject DV	22M2wkAF4AY2Hgn9gK9VCK+ Be9oAIaba/fQfKv NRddtvxY89ftbFhh XSLJfUUCdmAY+IG0 Ng2tvVFN3MXVZ0 TE ace:None	ModeMQ2Y4X,Uhj6SNDU70Ff6f Exceedeseuts.commun. Please wait while ASDM is delive device	X Information INFO: Certificate has the Fingerprint: e9ad165c 26 Trustpoint CA certificate	following attributes: 73424c 6e7e0c5f b30b- accepted.	4a02	
allow-untrusted-c	connection					
Use SCEP:				ОК		
	ace: None	~	L			
Specify source Interfe						
Specify source Interfa						
Specify source Interfa SCEP URL: http:// Retry Period:	1	minutes				

- 2. Installa certificato di identità
 - a. Scegliere il certificato di identità creato in precedenza durante la generazione di CSR. Fare clic su Install (Installa).

nfiguration > Remo	ote Ad	cess VPN > Certifica	ate Management > Ident	ity Certificates			
Issued To	^1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
vpn.example.com]		Not Available	Pending	SSL-Trustpoint	Unknown		Show Details
							Delete
							Export
							Install

Nota: il campo Rilasciato da del certificato di identità può essere Non disponibile e il campo Data scadenza può essere impostato su In sospeso.

b. Scegliere un file contenente il certificato di identità con codifica PEM ricevuto dalla CA oppure aprire il certificato con codifica PEM in un editor di testo e copiare e incollare il certificato di identità fornito dalla CA nel campo di testo.

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				~	General Purpose	RSA (2048 bits)	
install identity	centific	ate		↑ tpoint	General Purpose	RSA (2048 bits)	Delete
entity Certificate	_						Export
Install from a t	file:			Browse			Export
entity Certificate Install from a 	file:			Browse			Export
 entity Certificate Install from a formation 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
entity Certificate Install from a Paste the cert	file:	lata in base-64 forma	t:	Browse			Export Install Re-Enroll
Install from a Paste the cert	file:	lata in base-64 forma	t:	Browse			Export Instal Re-Enroll
entity Certificate 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	tı	Browse			Export Install Re-Enroll

Nota: il certificato di identità può essere in formato .pem, .cer, .crt da installare.

c. Fare clic su Installa certificato.

Show Detail: Delete
Delete
Delete
Export
Install
De Ferel
Re-Enroll

3. Associare il nuovo certificato all'interfaccia con ASDM

È necessario configurare l'ASA in modo che usi il nuovo certificato di identità per le sessioni WebVPN che terminano sull'interfaccia specificata.

- a. Selezionare Configurazione > VPN ad accesso remoto > Avanzate > Impostazioni SSL.
- b. In Certificati scegliere l'interfaccia utilizzata per terminare le sessioni WebVPN. nell'esempio viene usata l'interfaccia esterna.

Fare clic su Modifica.

c. Nell'elenco a discesa Certificato scegliere il certificato appena installato.

o omoin	Cer uncave				
					Edit
					Delete
	🔤 Select SSL Certificate	×	1		
	Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate				
	Management > Identity Certificates.				
specify which certificates, if ar	Interface: OUTSIDE-direct	_	es not	t associated with a certificate of	their own.
Interface	Primary Enrolled Certificate: SSL-Trustpoint:unstructuredName =asavpn.exampl	~		Key-Type	Edit
OLITSIDE-direct	Load Balancing Enrolled Certificate: None	\sim		Ney-1ype	
inside					
inside-vlan	OK Cancel Help				

- d. Fare clic su OK.
- e. Fare clic su Apply (Applica).

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

A questo punto il nuovo certificato di identità è in uso.

Installare un certificato di identità ricevuto nel formato PKCS12 con ASDM

Il file PKCS12 (formato .p12 o .pfx) contiene il certificato di identità, la coppia di chiavi e i certificati CA. Viene creata dalla CA, ad esempio in caso di certificato con caratteri jolly, o esportata da un dispositivo diverso. Si tratta di un file binario, che non può essere visualizzato con un editor di testo.

1. Installare i certificati di identità e CA da un file PKCS12

Il certificato di identità, i certificati CA e la coppia di chiavi devono essere raggruppati in un unico file PKCS12.

- a. Passare a Configurazione > Gestione dispositivi > Gestione certificati e scegliere Certificati di identità.
- b. Fare clic su Add.
- c. Specificare il nome di un Trustpoint.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Detai
Add Identity Certi	ficate		×			Delete
Trustpoint Name:	SSL-Trustpoint-P	PKCS12				Export
 Import the identit 	ty certificate from a file (F	PKCS12 format with Certificate	(s) +Private Key):			Install
Decryption Passp	hrase:					Re-Enrol
File to Import Fro	m:	Browse.				
O Add a new identit	ty 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 Subject	t DN: CN=risavpn31	Select.				
Generate self	-signed certificate					
Act as loc	al certificate authority an	nd issue dynamic certificates to	TLS-Proxy			
			Advanced			
Enable CA fla	g in basic constraints ext	ension				
List doit on the	y in obsic const dints ext					

d. Fare clic sul pulsante di opzione Importa il certificato di identità da un file.

	Issued By	Expiry D	ate	Associated	Trustpoints	Usage	Public	Кеу Туре	Add
									Show Det
🧧 Add Identity Cert	ificate		A.	(×				Delete
Trustpoint Name:	SSL-Trustpoint-P	(CS12	-0		import ID cer	tificate file			
Import the identi	ity certificate from a file (Pi	KCS12 format wit	h Certificate(s)+P	rivate Kev):	Look in:	Document	s	× 6	• 💷 🔊
Decryption Pass	ohrase:				0.	CSR.txt			
File to Import Fro	om:		Browse		Recent Items	ypn.exam	ple.com.pfx		
O Add a new identi	ity 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></default-rsa-ke<>	y> ~	Show	New	Desktop				
Certificate Subje	ct DN: CN=risavpn31		Select						
Generate sel	f-signed certificate				Documents				
Act as loo	cal certificate authority and	l issue dynamic c	ertificates to TLS-f	roxy					
				Advanced	This PC	File name:	vpn.example.com.pfx		Import ID certificate fi
	an in hasic constraints exte	nsion		Advanceu	1	Files of type:	All Files	~	Cancel
Enable (1) ft:	ay in basic consulaints exte	13011							

e. Immettere la passphrase utilizzata per creare il file 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. Fare clic su Aggiungi certificato.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
		,			,	Show Details
🔁 Add Identity C	Certificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-	PKCS12				Export
Import the id	entity certificate from a file (PKCS12 format with Certificate((s) +Private Key):			Install
Decryption Pa	assphrase: ••••		100000			Re-Enroll
File to Import	t From: C:\Users\cisco.0	DESKTOP-R2CH8G Browse.				
🔿 Add 🔚 Pl	ease wait		Information			×
Certi	Please wait while ASDM device	is delivering the command(s) to	the Created trustpoint WARNING: CA cert the validation-usage	s for CAs higher in the hie tificates can be used to va je of this trustpoint to limi	erarchy as the CA certificate was not s alidate VPN connections, by default. Ple t the validation scope, if necessary	elf-signed.
Enable C/	A flag in basic constraints ext	tension	Import PKCS12 opt	eration completed success	sfully.	

Nota: quando si importa un PKCS12 con una catena di certificati CA, ASDM crea automaticamente i trust CA a monte con nomi con suffisso -number aggiunto.

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. Associare il nuovo certificato all'interfaccia con ASDM

È necessario configurare l'ASA in modo che usi il nuovo certificato di identità per le sessioni WebVPN che terminano sull'interfaccia specificata.

a. Selezionare Configurazione > VPN ad accesso remoto > Avanzate > Impostazioni SSL.

b. In Certificati selezionare l'interfaccia utilizzata per terminare le sessioni WebVPN. nell'esempio viene usata l'interfaccia esterna.

Fare clic su Modifica.

c. Nell'elenco a discesa Certificato scegliere il certificato appena installato.

o onder		E	Edit elete
	Select SSL Certificate		
rtificates	Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate Management > Identity Certificates. Interface: OUTSIDE-direct Primary Enrolled Certificate: SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u v	ies not associated with a certificate of their own.	
Interface OUTSIDE-direct inside inside-vlan management	Load Balancing Enrolled Certificate: None V	Key-Type Edi	t
Fallback Certificate:	None 🗸		

- d. Fare clic su OK.
- e. Fare clic su Apply (Applica).

Certi Sp	ificates ecify which certificates, if any, should be	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	

A questo punto il nuovo certificato di identità è in uso.

Rinnovo certificato

Rinnova un certificato registrato con Richiesta di firma del certificato (CSR) con ASDM

Il rinnovo del certificato del certificato registrato CSR richiede la creazione e la registrazione di un nuovo punto di attendibilità. Deve avere un nome diverso, ad esempio vecchio con suffisso anno di registrazione. Può utilizzare gli stessi parametri e la stessa coppia di chiavi del certificato precedente oppure diversi.

Generare un CSR con ASDM

- 1. Creare un nuovo trust point con un nome specifico.
 - a. Passare a Configurazione > Gestione dispositivi > Gestione certificati > Certificati di

identità.



- b. Fare clic su Add.
- c. Definire un nome di trust.

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 Deta
Add Identity Certificate						×	Delete
Trustpoint Name:	ASDM_TrustPoint0						Export
 Import the identity certif 	icate from a file (PKC	S12 format with Certificate(s)+Priva	te Key):				Install
Decryption Passphrase:							Re-Enrol
File to Import From:		Browse					
O Add a new identity certif	icate:						
Key Pair:	<default-rsa-key< td=""><td>> V Show</td><td>New</td><td></td><td></td><td></td><td></td></default-rsa-key<>	> V Show	New				
Certificate Subject DN:	CN=risavpn31	Select					
Generate self-signed	certificate						
Act as local certif	icate authority and is	sue dynamic certificates to TLS-Prox	у				
		Adv	vanced				
Enable CA flag in bas	ic constraints extens	ion					

- d. Fare clic sul pulsante di opzione Aggiungi nuovo certificato di identità.
- 2. (Facoltativo) Creare una nuova coppia di chiavi

Nota: per impostazione predefinita, viene utilizzata la chiave RSA con il nome Default-RSA-Key e una dimensione di 2048; tuttavia, si consiglia di utilizzare una coppia di chiavi pubblica/privata univoca per ciascun certificato di identità.

a. Fare clic su Nuovo per generare una nuova coppia di chiavi.

Issued 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 Cer	rtificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
O Import the iden	ntity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Pass	sphrase:						Re-Enroll
File to Import Fi	rom:		Browse				
Add a new iden	ntity certificate:						
Key Pair:	<default-rsa-key< td=""><td>y> ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-key<>	y> ~	Show	New			
Certificate Subj	ject DN: CN=asavpn.exam	ple.com	Select				
Generate se	elf-signed certificate						
Act as lo	ocal certificate authority and	issue dynamic cer	rtificates to TL	S-Proxy			
				Advanced			
Enable CA f	flag in basic constraints exter	nsion		Advanced			
	nag in basic constraints exter	131011					

- b. Scegliere l'opzione Immettere il nuovo nome della coppia di chiavi e immettere un nome per la nuova coppia di chiavi.
- c. Scegliere il tipo di chiave: RSA o ECDSA.
- d. Scegliere le dimensioni della chiave; per RSA, scegliere Uso generico.
- e. Fare clic su Genera ora. La coppia di chiavi è stata creata.

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 Deta
add Identity	Certificate		×			Delete
Trustopint Name	ssi -Trustnoint-20	23				Export
C To Add Ke	ey Pair		× Key):			Install
Key Type	: • RSA		A			Re-Enrol
Name:	O Use default key pair name					
Size.	Enter new Key pair name	SSL-KeyPair-2023	ew			
Usage:	General purpose	Special				
	Generate Now Cance	el Help	iced			
THE PARTY OF THE P	in may in public consulants exter	131011				

3. Selezionare il nome della coppia di chiavi

Scegliere la coppia di chiavi con cui firmare il CSR e da associare al nuovo certificato.

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 Cert	tificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23				Export
O Import the ident	tity certificate from a file (PK	CS12 format with Certificate	(s) +Private Key):			Install
Decryption Pass	phrase:					Re-Enroll
File to Import Fro	om:	Browse				
Add a new ident	tity certificate:					
Key Pair:	SSL-KeyPair-2023	✓ Show	. New			
Certificate Subje	ect DN: CN=asavpn.exam	ple.com Select.	• 11			
Generate sel	If-signed certificate					
Act as lo	cal certificate aut grity and	issue dynamic certificates to	TLS-Proxy			
			Advanced			
-	ag in basic constraints exten	sion				

4. Configurare il soggetto del certificato e il nome di dominio completo (FQDN)

Attenzione: il parametro FQDN deve corrispondere all'FQDN o all'indirizzo IP dell'interfaccia ASA per cui viene utilizzato il certificato. Questo parametro imposta il nome alternativo del soggetto (SAN) per il certificato. Il campo SAN viene utilizzato dal client SSL/TLS/IKEv2 per verificare se il certificato corrisponde all'FQDN a cui si connette.

Nota: quando firma il CSR e crea un certificato di identità firmato, CA può modificare i parametri FQDN e Nome soggetto definiti nel trust point.

a. Fare clic su Seleziona.

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
Trustopint Name	e. SSI .Trustmoint.20	23					Export
O Import the i	identity certificate from a file (PK	CS12 format with	n Certificate(s)	+Private Key):			Install
Decryption F	Passphrase:						Re-Enrol
File to Impor	rt From:		Browse				
Add a new i	identity certificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate S	Subject DN: CN=asavpn.exam	ple.com	Select				
Generat	te self-signed certificate			_			
Act	as local certificate authority and	issue dynamic ce	rtificates to TL	S-Proxy			
				Advanced			
Enable (CA flag in basic constraints exter	nsion					
	CA flag in basic constraints exter	nsion		_			

b. Nella finestra DN soggetto certificato, configurare gli attributi del certificato selezionare l'attributo dall'elenco a discesa, immettere il valore e fare clic su Aggiungi.

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						

Attributo	Descrizione
CN	Il nome attraverso il quale è possibile accedere al firewall (in genere il nome di dominio completo, ad esempio vpn.example.com).
UO	Il nome del reparto all'interno dell'organizzazione
0	La ragione sociale legalmente registrata dell'azienda
с	Codice paese (codice a 2 lettere senza punteggiatura)
ST	Stato in cui si trova l'organizzazione.
L	Città in cui si trova l'organizzazione.
EA	Indirizzo email

Nota: nessuno dei campi precedenti può superare il limite di 64 caratteri. Un valore più lungo può causare problemi con l'installazione del certificato di identità. Inoltre, non è necessario definire tutti gli attributi DN.

Dopo aver aggiunto tutti gli attributi, fare clic su OK.

c. Per configurare l'FQDN del dispositivo, fare clic su Avanzate.

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	e: SSL-Trustpoint-20	23					Export
O Import the i	identity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption I	Passphrase:						Re-Enroll
File to Impo	rt From:		Browse				
Add a new i	identity certificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate S	Subject DN: /pn.example.com,	O=example inc	Select				
Generat	te self-signed certificate						
Act	as local certificate authority and	issue dynamic cer	tificates to TL	S-Proxy			
				Advanced			
Enable (CA flag in basic constraints exter	nsion		Advanced			
	CA hag in basic constraints exter	151011					

d. Nel campo FQDN immettere il nome di dominio completo tramite il quale il dispositivo è accessibile da Internet. Fare clic su OK.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
	Ontions	- OLI - 115-10-00 CEST Solv 6 20	24 CEL Trustosist	General Purpose	RSA (2048 bits)	Show Details
Auvanceuv						Delete
Certificate Para	parameters and SCEP cha	allenge password are not available	for self-signed certificates.			Export
						Install
FQDN:	asavpn.example.com					Re-Enroll
E-mail:						
IP Address:						
	rial number of the device					
		G				

- 5. Generare e salvare il CSR
 - a. Fare clic su Aggiungi certificato.

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. Viene visualizzato un prompt per salvare il CSR in un file sul computer locale.

	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
Trustnoint Nam	e: SSI -Trustnoint-20	123				Export
O Import the	identity certificate from a file (PF	KCS12 format with Certificate(s)+Private Key):			Install
C Con Laboratoria	tite Contificate Research		×			Re-Enroll
F	inty connecte nequest					
To cor reque	nplete the enrollment process, p st (CSR) and send it to the CA.	lease save the PKCS10 enrollm	ent			
K You w clicking	ill then need to install the certific g the Install button in the Identit	ate that is returned from the C ty Certificates panel.	A by			
Save	CSR to File: C:\Users\cisco.DES	KTOP-R2CH8G5\Docun Br	owse			
		ancol Holp				
		ancer				
			Advanced			
	CA flag in basic constraints exter	nsion				

Scegliere Sfoglia. Scegliere un percorso in cui salvare il CSR e salvare il file con estensione .txt.

Nota: quando il file viene salvato con estensione .txt, è possibile aprire e visualizzare la richiesta PKCS#10 con un editor di testo, ad esempio Blocco note.

c. A questo punto il nuovo trust point viene visualizzato in stato In sospeso.

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

Installare il certificato di identità in formato PEM con ASDM

Nelle procedure di installazione si presuppone che l'autorità di certificazione abbia firmato il CSR e abbia fornito un nuovo certificato di identità e un bundle di certificati CA codificati PEM (.pem, .cer, .crt).

1. Installa certificato CA con firma CSR

Il certificato CA che ha firmato il certificato di identità può essere installato nel punto di fiducia creato per il certificato di identità. Se il certificato di identità è firmato da un'autorità di certificazione intermedia, è possibile installare tale certificato nel punto di fiducia del certificato di identità. Tutti i certificati CA a monte nella gerarchia possono essere installati in punti di trust CA distinti.

a. Passare a Configurazione > Gestione dispositivi >Gestione certificati > e scegliere Certificati CA. Fare clic su Add.

	igement > Certificate Plan	agement > CA Certificates				
issued 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
denTrust Commercial Root	CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Show Details

 b. Immettere il nome del Trustpoint e scegliere Installa da file, fare clic su Pulsante Sfoglia, quindi scegliere il certificato intermedio. In alternativa, incollare il certificato CA con codifica PEM da un file di testo nel campo di testo.

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

Nota: installare il certificato intermedio con lo stesso nome del trust point del

certificato di identità, se il certificato di identità è firmato da un certificato CA intermedio.

c. Fare clic su Installa certificato.

sued 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: St	SL-Trustpoint-2023						Request CR
O Install from a file:		Browse					Delete
Paste certificate in PE	M format:						
Ojskkn/CP/Fg3p2Fd/ VROOBYPEFSS/ZDW 9tLFV52U47em9uXaM cGqeyDMRh3Rs/W/LK8 0JRyjaH568FladAkC7 gW8YnHO-MM0SavyT/ dK/covOj/PAxmrAJ+H END CERTIFICAT Use EST: Specify source Interfa EST URL: https:// Certificate Subject DN	17WJh 11KSprAgMBAAGJUDEOL 999LIPS2J47em9UXdMBSG A0GCSqStb 3DCEBC-WLAAH 159WJAAF4AY27ByB9gK ESDAIJathA/FQfX6V4h7 RddTVX7B5rEbFINBoc SLIFOUCGMY44Gogdh Ig2jrWFN3MXWZO453C E ce:None .: CN=risavpn31 proection	AwGA 1UdEwQPMANBAR9wHQ 1UdEwQVMBARFEStX2sbra9b BAOArsxIEwK3llNBwOsYhSmgT Information INFO: Certificate ha Fingerprint: e9ad 16 Trustpoint CA certifi	D as the following attributes: 5c 2673424c 6e7e0c5f b30b4a02 icate accepted.	×		~	
Use SCEP:							
Specify source Interfa	ce: None	~					
SCEP URL: http://							
Retry Period:	1	minutes					

Nell'esempio il nuovo certificato è firmato con lo stesso certificato CA del precedente. Lo stesso certificato CA è ora associato a due Trustpoint.

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

- 2. Installa certificato di identità
 - a. Scegliere il certificato di identità creato in precedenza con la generazione di CSR. Fare clic su Install (Installa).

nfiguration > Device	<u>e Management > Certifica</u>	ate Management > Identit	y 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

Nota: il campo Rilasciato da del certificato di identità può essere Non disponibile e il campo Data scadenza può essere impostato su In sospeso.

b. Scegliere un file contenente il certificato di identità con codifica PEM ricevuto dalla CA oppure aprire il certificato con codifica PEM in un editor di testo e copiare e incollare il certificato di identità fornito dalla CA nel campo di testo.

sued To	Issued By	Expiry Date	Associated Trustpoints	~1	Usage	Public Key Type	Add
structuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detai
savpn.example.com]	Not Available	Pending	SSL-Trustpoint-2023		Unknown		
							Delete
							Export
a Install Identity o	ertificate		×				Install
dentity Certificate							Re-Enroll
Certificate	N						
 Install from a f 	ie:	L	browse				
O Paste the certi	ficate data in base-64 format:						

Nota: il certificato di identità può essere in formato .pem, .cer, .crt da installare.

c. Fare clic su Installa certificato.

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.co	omj Not Available	Pending	SSL-Trustpoint-2023		Unknown		Delete
							Export
Install Identit	y certificate		×				Install
entity Certificat							Re-Enrol
church ceruncau	e						1
O In 🔂 Plea	ase wait						
O In To Plea	ase wait	ation	×				
O In Plea	ase wait Please wait wf device	ation	×				
O In Plex	e ase wait Please wait wf device	ation Certificate import succeede	×				
In Pre P	ase wait Please wait wf device	stion Certificate import succeede	d.				

Dopo l'installazione, sono presenti certificati di identità vecchi e nuovi.

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 Deta
instructuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Deta
							Delete
							Export
							Install
							Re-Enrol

3. Associare il nuovo certificato all'interfaccia con ASDM

È necessario configurare l'ASA in modo che usi il nuovo certificato di identità per le sessioni

WebVPN che terminano sull'interfaccia specificata.

- a. Selezionare Configurazione > VPN ad accesso remoto > Avanzate > Impostazioni SSL.
- b. In Certificati scegliere l'interfaccia utilizzata per terminare le sessioni WebVPN. nell'esempio viene usata l'interfaccia esterna.

Fare clic su Modifica.

c. Nell'elenco a discesa Certificato scegliere il certificato appena installato.

quiation > Remote Access	With > Advanced > 35c Sectings	<u>2</u>			
	_			Edit Delete	
	Select SSL Certificate	2	×	-	
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: Load Balancing Enrolled Certificate:	SSL-Trustpoint-2023:unstructuredName=asavpn.exampl v	Кеу-Туре	Edit	
inside	-		Primary: RSA (2048 bits), Load Balancing: n	1	
inside-vlan	OK	Cancel Help			
management					

- d. Fare clic su OK.
- e. Fare clic su Apply (Applica). A questo punto il nuovo certificato di identità è in uso.

uration > Remote Acce	ss VPN > Advanced > SSL Settings			
				Edit
ificates				
ificates	1y, should be used for SSL authentication on eac	ch interface. The fallback certificate will be us	sed on interfaces not associated with a certificate of their own.	Edit
ificates ecify which certificates, if ar Interface	1y, should be used for SSL authentication on eac Primary Certificate	ch interface. The failback certificate will be us Load Balancing Certificate	sed on interfaces not associated with a certificate of their own. Key-Type	Edit
ificates ecify which certificates, if ar Interface OUTSIDE-direct	1y, should be used for SSL authentication on eac Primary Certificate SSL-Trustpoint-2023:unstructure	ch 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
ificates ecify which certificates, if ar Interface OUTSIDE-drect inside	ny, should be used for SSL authentication on eac Primary Certificate SSL-Trustpoint-2023;unstructure	ch 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
ificates — 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	ch 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

Rinnova un certificato registrato con un file PKCS12 con ASDM

Il rinnovo del certificato di un certificato registrato PKCS12 richiede la creazione e la registrazione di un nuovo trust point. Deve avere un nome diverso, ad esempio vecchio con suffisso anno di registrazione.

Il file PKCS12 (formato .p12 o .pfx) contiene il certificato di identità, la coppia di chiavi e i certificati CA. Viene creata dalla CA, ad esempio in caso di certificato con caratteri jolly, oppure esportata da un dispositivo diverso. Si tratta di un file binario e non può essere visualizzato con un editor di testo.

1. Installare il certificato di identità e i certificati CA rinnovati da un file PKCS12

Il certificato di identità, i certificati CA e la coppia di chiavi devono essere raggruppati in un unico file PKCS12.

- a. Passare a Configurazione > Gestione dispositivi > Gestione certificati e scegliere Certificati identità.
- b. Fare clic su Add.
- c. Specificare un nuovo nome per il punto di trust.

ssued To	Issued By	Expiry Date	2	Associated Trustpoints	Usage	Public Key Type	Add
							Show Detai
add Identity (ertificate			×			Delete
Trustpoint Name	SSL-Trustpoint-	PKCS12					Export
 Import the id 	entity certificate from a file (PKCS12 format with (Certificate(s)+Pr	ivate Key):			Install
Decryption P	assphrase:						Re-Enrol
File to Import	From:		Browse				
O Add a new id	entity 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 Su	bject DN: CN=risavpn31		Select				
Generate	self-signed certificate						
Act a	s local certificate authority a	nd issue dynamic cert	ificates to TLS-P	roxy			
				Advanced			
CR Fachla C	And in basis constraints out	topping		Auvanceu			
	A hag in basic consulants exi	LETISION;					

d. Fare clic sul pulsante di opzione Importa il certificato di identità da un file.

ssued To	Issued By	Expiry Da	te	Associated 1	rustpoints	Usage	Public	Кеу Туре	Add
									Show Deta
Add Identity Certificat	te			>	<u></u>				Delete
Trustpoint Name:	SSL-Trustpoint-PKCS1	12	-0		Import ID certif	icate file			
Import the identity ce	rtificate from a file (PKCS)	12 format with	Certificate(s)+P	rivate Kev):	Look in:	😫 Document	3	× 🤌	· 📂 🛄 -
Decryption Passphras	e:				6.	CSR.txt			
File to Import From:			Browse		Recent Items	🖄 vpn.exam	ple.com.pfx		
O Add a new identity ce	rtificate:								
Key Pair:	<default-rsa-key></default-rsa-key>	\sim	Show	New	Desktop				
Certificate Subject DN	CN=risavpn31		Select						
Generate self-sign	ned certificate				Documents				
Act as local ce	rtificate authority and issu	ue dynamic ce	rtificates to TLS-F	roxy					
					This PC F	le name:	vpn.example.com.pfx	I	mport ID certificate file
				Advanced	- 🗳 F	les of type:	All Files	~	Cancel
Enable CA flag in t	basic constraints extension	n			L				

e. Immettere la passphrase utilizzata per creare il file 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. Fare clic su Aggiungi certificato.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
			· · · · · · · · · · · · · · · · · · ·			Show Details
Add Identity Co	ertificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-F	PKCS12				Export
Import the ide	entity certificate from a file (PKCS12 format with Certificate((s) +Private Key):			Install
Decryption Pa	ssphrase: ••••					Re-Enroll
File to Import	From: C:\Users\cisco.E	DESKTOP-R2CH8G Browse.				
Add Pre	Please wait while ASDM device	is delivering the command(s) to	the			×
			Created trustpoint WARNING: CA cer the validation-usa	s for CAs higher in the hie tificates can be used to va ge of this trustpoint to limi	rarchy as the CA certificate was not s alidate VPN connections,by default. Ple t the validation scope, if necessary	elf-signed.
Enable CA	flag in basic constraints ext	tension	Import PKCS 12 op	eration completed success	fully.	

Nota: quando si importa una catena di certificati PKCS12 con CA, ASDM crea automaticamente i trust CA a monte con nomi con suffisso -number aggiunto.

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. Associare il nuovo certificato all'interfaccia con ASDM

È necessario configurare l'ASA in modo che usi il nuovo certificato di identità per le sessioni WebVPN che terminano sull'interfaccia specificata.

a. Selezionare Configurazione > VPN ad accesso remoto > Avanzate > Impostazioni SSL.

b. In Certificati scegliere l'interfaccia utilizzata per terminare le sessioni WebVPN. nell'esempio viene usata l'interfaccia esterna.

Fare clic su Modifica.

c. Nell'elenco a discesa Certificato scegliere il certificato appena installato.

	ULT UTION L	
ertificates	Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface: Interface: OUTSIDE-direct Primary Enrolled Certificate: SSL-Trustpoint-PKCS 12:unstructuredName=FTD72-ek, u v	Edit Delete
Interface OUTSIDE-direct inside inside-vlan management	Load Balancing Enrolled Certificate: None V Key-Type	Edit
Fallback Certificate: Forced Certification Authentica	tion Timeout: 2 minutes	

- d. Fare clic su OK.
- e. Fare clic su Apply (Applica).

Certi Sp	ficates	e used for SSL authentication on each interface. Ti	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	SSL-Trustpoint-PKCS12:unstructuredName=F		Primary: RSA (2048 bits), Load Balan	

A questo punto il nuovo certificato di identità è in uso.

Verifica

Utilizzare questa procedura per verificare la corretta installazione del certificato del fornitore di terze parti e utilizzarlo per le connessioni VPN SSL.

Visualizza certificati installati tramite ASDM

- 1. Passare a Configurazione > VPN ad accesso remoto > Gestione certificati e scegliere Certificati di identità.
- 2. È possibile visualizzare il certificato di identità rilasciato dal fornitore di terze parti.

C	ertificates				
	Specify which certificates, if any, should be	e used for SSL authentication on each interface. The	he fallback certificate will be used on interfaces not assoc	iated with a certificate of their own.	
					5 .11
	Interface	Primary Certificate	Load Balancing Certificate	Key-Type	Edit
	OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName=F		Primary: RSA (2048 bits), Load Balan	

Risoluzione dei problemi

Questo comando debug deve essere raccolto nella CLI in caso di errore durante l'installazione di un certificato SSL.

• debug crypto ca 14

Domande frequenti

D. Che cos'è un PKCS12?

A.In crittografia, PKCS12 definisce un formato di file di archivio creato per archiviare molti oggetti di crittografia come un unico file. Viene in genere utilizzato per includere una chiave privata nel relativo certificato X.509 o per includere tutti i membri di una catena di attendibilità.

D. Che cos'è un CSR?

A. Nei sistemi con infrastruttura a chiave pubblica (PKI), una richiesta di firma del certificato (anche CSR o richiesta di certificazione) è un messaggio inviato da un richiedente a un'autorità di registrazione dell'infrastruttura a chiave pubblica per richiedere un certificato di identità digitale. In genere contiene la chiave pubblica per la quale è possibile rilasciare il certificato, le informazioni utilizzate per identificare il certificato firmato (ad esempio un nome di dominio in Oggetto) e la protezione dell'integrità (ad esempio, una firma digitale).

D. Dov'è la password di PKCS12?

A.Quando i certificati e le coppie di chiavi vengono esportati in un file PKCS12, la password viene specificata nel comando di esportazione. Per importare un file pkcs12, la password deve essere recapitata dal proprietario del server CA o dalla persona che ha esportato il PKCS12 da un altro dispositivo.

D.Qual è la differenza tra la radice e l'identità?

A.Nella crittografia e nella protezione del computer, un certificato radice è un certificato a chiave pubblica che identifica un'Autorità di certificazione (CA) radice. I certificati radice sono autofirmati (ed è possibile che un certificato abbia più percorsi di attendibilità, ad esempio se è stato rilasciato da una radice con firma incrociata) e costituiscono la base di un'infrastruttura a chiave pubblica (PKI) basata su X.509. Un certificato a chiave pubblica, noto anche come certificato digitale o certificato di identità, è un documento elettronico utilizzato per provare la proprietà di una chiave pubblica. Il certificato include informazioni sulla chiave, informazioni sull'identità del proprietario (denominato soggetto) e la firma digitale di un'entità che ha verificato il contenuto del certificato (denominata emittente). Se la firma è valida e il software che esamina il certificato considera attendibile l'emittente, può utilizzare tale chiave per comunicare in modo sicuro con il soggetto del certificato.

D.Ho installato il certificato. Perché non funziona? R.Ciò può essere dovuto a diversi motivi, ad esempio:

1. Il certificato e il trust point sono configurati, ma non sono stati associati al processo che deve utilizzarli. Ad esempio, il trust point da utilizzare non è associato all'interfaccia esterna che

termina i client Anyconnect.

2. È installato un file PKCS12, ma vengono restituiti errori dovuti alla mancanza del certificato CA intermedio nel file PKCS12. I client in cui il certificato CA intermedio è considerato attendibile, ma il certificato CA radice non è considerato attendibile, non sono in grado di verificare l'intera catena di certificati e segnalare il certificato di identità del server come non attendibile.

3. Un certificato contenente attributi non corretti può causare errori di installazione o errori sul lato client. Alcuni attributi, ad esempio, potrebbero essere codificati utilizzando un formato non corretto. Un altro motivo è che nel certificato di identità manca il nome alternativo del soggetto (SAN) oppure il nome di dominio utilizzato per accedere al server non è presente come SAN.

D. L'installazione di un nuovo certificato richiede una finestra di manutenzione o causa tempi di inattività?

R. L'installazione di un nuovo certificato (identità o CA) non è intrusiva e non deve causare tempi di inattività o richiedere un intervento di manutenzione. L'abilitazione di un nuovo certificato da utilizzare per un servizio esistente è una modifica e potrebbe richiedere una finestra di richiesta di modifica o di manutenzione.

D. È possibile aggiungere o modificare un certificato per disconnettere gli utenti connessi? A.No, gli utenti attualmente connessi rimangono connessi. Il certificato viene utilizzato al momento della connessione. Una volta riconnessi gli utenti, verrà utilizzato il nuovo certificato.

D.Come creare un CSR con un carattere jolly? O un nome alternativo del soggetto (SAN)? R.Al momento, l'ASA/FTD non può creare un CSR con caratteri jolly; tuttavia, questa procedura può essere eseguita con OpenSSL. Per generare la chiave CSR e ID, è possibile eseguire i comandi seguenti:

openssl genrsa -out id.key 2048

openssl req -out id.csr -key id.key -new Quando un trust point è configurato con l'attributo FQDN (Fully Qualified Domain Name), il CSR creato da ASA/FTD contiene la SAN con tale valore. La CA può aggiungere altri attributi SAN quando firma il CSR oppure è possibile creare il CSR con OpenSSL

Q. La sostituzione del certificato è immediata?

R. Il nuovo certificato di identità del server viene utilizzato solo per le nuove connessioni. Il nuovo certificato è pronto per essere utilizzato subito dopo la modifica, ma viene utilizzato con le nuove connessioni.

D.Come posso verificare se l'installazione ha funzionato?

A.II comando CLI da verificare: show crypto ca cert <trustpointname>

D.Come generare PKCS12 da un certificato di identità, un certificato CA e una chiave privata?

A. PKCS12 può essere creato con OpenSSL, con il comando: openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt D. Come esportare un certificato per installarlo in una nuova appliance ASA? R.

- Con CLI: utilizzare il comando crypto ca export <nometrust> pkcs12 <password>
- Con ASDM:
 - a. Passare a Configurazione > Gestione dispositivi > Gestione certificati > Certificati di identità e scegliere il certificato di identità. Fare clic su Esporta.

File View Tools Wizards Windo	ow Help					Type topic to search	Go	ahaha
Home 🎭 Configuration 🔯 Mor	iitoring 🔚 Save 🔇 Refre	esh 🔇 Back 🔘 Forwar	d 🦻 Help					cisco
Bookmarks 급 무 ×	Configuration > Device Ma	inagement > Certificate M	tanagement > 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	CN=ca.example.com, OU CN=ca.example.com, OU	15:10:00 CEDT Apr 6 2024 15:10:00 CEST Feb 6 2024	SSL-Trustpoint-2023 SSL-Trustpoint	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)		Show Details
	unstructuredName=FTD7 [asa.vpn.example.com]	CN=KrakowCA-sub1-1 Not Available	04:44:00 CEST Dec 21 2024 Pending	SSL-Trustpoint-PKCS12 SSL-Trustpoint	General Purpose Unknown	RSA (2048 bits)		Delete
								Export
							- 17	Re-Enrol
								Realition
Management Access								
Gensing System Image/Configuration								
High Availability and Scalability								
- I Smart Call-Home	Find:	Match Case						
-2 Cloud Web Security	Certificate Expiration Alerts							
Service Module Settings Users/AAA	Send the first alert before	e: 60 (days) Set Def	ault					
Certificate Management Certificates	Repeat Alert Interval :	7 (days)						
-2 CA Certificates	Weak Crypto Configurations -							

b. Scegliere dove esportare il file, specificare la password di esportazione e fare clic su Esporta certificato.

sued to	Issued By	Expiry Date	Associated Trustpoints	Usa	ge	Public Key Type	Add
nstructuredName=asav	CN=ca.example.com, OU	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023		General Purpose	RSA (4096 bits)	Show Details
nstructuredName=risav	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show De tails
nstructuredName=FTD7	CN=KrakowCA-sub1-1	04:44:00 CEST Dec 21 2024	SSL-Trustpoint-PKCS12		General Purpose	RSA (2048 bits)	Delete
sa.vpn.example.com]	Not Available	Pending	SSL-Trustpoint		Unknown		Export
							Laport
							Install
							Re-Enrol
nd: rtificate Expiration Alerts Send the first alert befor Repeat Alert Interval :	re : 60 (days) Set Defa 7 (days)	sult					
ind: rtificate Expiration Alerts Send the first alert befor Repeat Alert Interval : k Crypto Configurations -	re : 60 (days) Set Defa 7 (days) 8 Export certificate	sult		×			
nd: tificate Expiration Alerts Send the first alert befor Repeat Alert Interval : : Crypto Configurations – Permit Weak key sizes ai	Image: Match Case re : 60 (days) Image: Comparison of the second secon	suit		×	}		
nd: tificate Expiration Alerts Send the first alert befor Repeat Alert Interval : c Crypto Configurations -) Permit Weak key sizes an	Image: Set Defa 7 (days) Set Defa 7 (days) Image: Set Defa 7 (days)	ult C:\Users\disco.DESKTOP4	R2CH8G5\Documents\ce Browse	×	1		
nd: tificate Expiration Alerts Send the first alert befor Repeat Alert Interval : : Crypto Configurations - Permit Weak key sizes an : CA Enrollment -	Image: Set Defa 7 (days) Set Defa 7 (days) Image: Set Defa 8 Export to File: 10 Certificate Format:	ult C:\Users\disco.DESKTOP4	R2CH8G5\Documents\ce Browse	×			
nd: tificate Expiration Alerts Send the first alert befor Repeat Alert Interval : : Crypto Configurations – Permit Weak key sizes ar : CA Enrollment tyour Cisco ASA security tio.	Image: Set Defa 7 (days) Set Defa 7 (days) Image: Set Defa 8 Export certificate 9 Image: Set Defa 9 Image: Set Defa 9 Image: Set Defa 10 Image: Set Defa 11 Image: Set Defa 12 Image: Set Defa 13 Image: Set Defa 14 Image: Set Defa 14 Image: Set Defa 15 Image: Set Defa 16 Image: Set Defa 17 Image: Set Defa 16 Image: Set Defa 17 Image: Set Defa	eult C:\Users\disco.DESKTOP4 PKCS12 Format (Cerbif	R2CH8G5\Documents\ce} Browse	×	stomers a special	promotional price for certificate	es and trial certificates f
nd: tificate Expiration Alerts Send the first alert befor Repeat Alert Interval : c Crypto Configurations – Permit Weak key sizes and c A Enrollment – tyour Cisco ASA security ting.	Image: Set Defa 7 (days) Set Defa 7 (days) Image: Set Defa 8 Export certificate 10 Export to File: Certificate Format: appliz	C:\Users\cisco.DESKTOP4 PKCS12 Format (Certif PEM Format (Certificat	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	×	stomers a special	promotional price for certificate	es and trial certificates f
nd: tificate Expiration Alerts Send the first alert befor Repeat Alert Interval : : Crypto Configurations - Permit Weak key sizes and : CA Enrollment	Image: Set Defa 7 (days) 8 Export certificate nd Ha Export to File: Certificate Format: appliz	eult C:\Users\cisco.DESKTOP4 PKCS12 Format (Certificat) PEM Format (Certificat)	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	× 	stomers a special	promotional price for certificate	es and trial certificates f
nd: trificate Expiration Alerts Send the first alert befor Repeat Alert Interval : c Crypto Configurations -] Permit Weak key sizes an : CA Enrollment	O Match Case re : 60 (days) Set Defa 7 (days) Export certificate nd Ha Export to File: Certificate Format: applic rtifica Configuration Encryption	C:\Users\cisco.DESKTOP4 OPKCS 12 Format (Certif OPEM Format (Certificat on Passphrase	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	× 	stomers a special	promotional price for certificate	es and trial certificates f
ind: trificate Expiration Alerts Send the first alert befor Repeat Alert Interval : k Crypto Configurations] Permit Weak key sizes an c CA Enrollment	Image: Set Defa 7 (days) 8 Export certificate 1 Export to File: Certificate Format: Certificate Format: applix Encryption Passphra	C: Users \cisco.DESKTOP 4 PKCS 12 Format (Certificat PEM Format (Certificat on Passphrase se:	R2CH8G5\Documents\ce Browse ficate(s) + Private Key) te Only)	× 	stomers a special	promotional price for certificate	es and trial certificates fo

Il certificato esportato può trovarsi sul disco del computer. Prendere nota della

passphrase in un luogo sicuro, il file è inutile senza di essa.

D.Se vengono utilizzate chiavi ECDSA, il processo di generazione del certificato SSL è diverso? A.L'unica differenza di configurazione è rappresentata dalla fase di generazione della coppia di chiavi, in cui è possibile generare una coppia di chiavi ECDSA anziché una coppia di chiavi RSA. Il resto dei gradini rimane lo stesso.

D.È sempre necessario generare una nuova coppia di chiavi?

A. Il passo di generazione della coppia di chiavi è facoltativo. È possibile utilizzare una coppia di chiavi esistente oppure, nel caso di PKCS12, tale coppia viene importata con il certificato. Vedere la sezione Selezionare il nome della coppia di chiavi per il rispettivo tipo di registrazione/ri-registrazione.

D.È sicuro generare una nuova coppia di chiavi per un nuovo certificato di identità? A. Il processo è sicuro se si utilizza un nuovo nome di coppia di chiavi. In questo caso, le vecchie coppie di chiavi non vengono modificate.

D.È necessario generare nuovamente la chiave quando si sostituisce un firewall (come RMA)? A.Il nuovo firewall non dispone per impostazione predefinita di una coppia di chiavi sul firewall precedente.

Il backup della configurazione corrente non contiene le coppie di chiavi.

Il backup completo eseguito con ASDM può contenere le coppie di chiavi.

È possibile esportare i certificati di identità da un'appliance ASA con ASDM o CLI prima che si verifichi un errore.

In caso di coppia di failover, i certificati e le coppie di chiavi vengono sincronizzati su un'unità in standby con il comando write standby. In caso di sostituzione di un nodo di coppia di failover, è sufficiente configurare il failover di base ed eseguire il push della configurazione sul nuovo dispositivo.

Se una coppia di chiavi viene persa con il dispositivo e non è disponibile alcun backup, è necessario firmare un nuovo certificato con la coppia di chiavi presente nel nuovo dispositivo.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).