Instalación y renovación de certificados en ASA administrados por ASDM

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Solicitud e instalación de un nuevo certificado de identidad con ASDM
<u>Solicitar e instalar un nuevo certificado de identidad con solicitud de firma de</u> certificado (CSR)
Generación de un CSR con ASDM
Crear un punto de confianza con un nombre específico
(Opcional) Creación de un nuevo par de claves
Elija el nombre del par de claves
Configure el asunto del certificado y el nombre de dominio completamente calificado (FQDN)
<u>Generar y guardar el CSR</u>
Instalación del Certificado de Identidad en formato PEM con ASDM
Instalar el certificado de CA que firmó el CSR
Instalar certificado de identidad
Enlace del Nuevo Certificado a la Interfaz con ASDM
Instalación de un Certificado de Identidad Recibido en Formato PKCS12 con ASDM
Instalar la identidad y los certificados de CA desde un archivo PKCS12
Enlace del Nuevo Certificado a la Interfaz con ASDM
Renovación de certificados
Renovación de un certificado inscrito con solicitud de firma de certificado (CSR) con ASDM
Generación de un CSR con ASDM
Cree un nuevo punto de confianza con un nombre específico.
(Opcional) Creación de un nuevo par de claves
Seleccione el nombre del par de claves
Configure el asunto del certificado y el nombre de dominio completamente calificado (FQDN)
<u>Generar y guardar el CSR</u>
Instalación del Certificado de Identidad en Formato PEM con ASDM
Instalar el certificado de CA que firmó el CSR
Instalar certificado de identidad
Enlace del Nuevo Certificado a la Interfaz con ASDM
Renovación de un Certificado Inscrito con el Archivo PKCS12 con ASDM
Instalación del certificado de identidad renovado y los certificados de CA desde un archivo PKCS12
Enlace del Nuevo Certificado a la Interfaz con ASDM
<u>Verificación</u>
Ver certificados instalados mediante ASDM

Troubleshoot

Introducción

Este documento describe cómo solicitar, instalar, confiar y renovar ciertos tipos de certificados en el software Cisco ASA administrado con ASDM.

Prerequisites

Requirements

- Antes de comenzar, compruebe que el dispositivo de seguridad adaptable (ASA) tiene la hora, fecha y zona horaria del reloj correctas. Con la autenticación de certificados, se recomienda utilizar un servidor de protocolo de tiempo de la red (NTP) para sincronizar la hora en el ASA. Marque Información relacionada para referencia.
- Para solicitar un certificado que utilice la Solicitud de firma de certificado (CSR), es necesario tener acceso a una Autoridad de certificación (CA) interna o de terceros de confianza. Algunos ejemplos de proveedores de CA de terceros son, entre otros, Entrust, Geotrust, GoDaddy, Thawte y VeriSign.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASAv 9.18.1
- Para la creación de PKCS12, se utiliza OpenSSL.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Los tipos de certificados a los que se dirige este documento son:

- · Certificados con firma automática
- · Certificados firmados por una autoridad de certificación externa o una CA interna

Los protocolos de autenticación Secure Socket Layer (SSL), Transport Layer Security (TLS) e IKEv2 rfc7296 para EAP exigen que el servidor SSL/TLS/IKEv2 proporcione al cliente un certificado de servidor para que el cliente realice la autenticación del servidor. Se recomienda utilizar CA de terceros de confianza para emitir certificados SSL al ASA con este fin.

Cisco no recomienda el uso de un certificado autofirmado debido a la posibilidad de que un

usuario pueda configurar inadvertidamente un navegador para confiar en un certificado de un servidor no autorizado. También existe la molestia para los usuarios de tener que responder a una advertencia de seguridad cuando se conecta al gateway seguro.

Solicitud e instalación de un nuevo certificado de identidad con ASDM

Se puede solicitar un certificado a una autoridad de certificación (CA) e instalarlo en un ASA de dos maneras:

- Utilizar la solicitud de firma de certificado (CSR). Genere un par de claves, solicite un certificado de identidad de CA con una CSR e instale el certificado de identidad firmado obtenido de CA.
- Utilice el archivo PKCS12 obtenido de una CA o exportado desde un dispositivo diferente. El archivo PKCS12 contiene pares de claves, certificados de identidad y certificados de CA.

Solicitar e instalar un nuevo certificado de identidad con solicitud de firma de certificado (CSR)

Se crea una CSR en el dispositivo que necesita un certificado de identidad; utilice un par de claves creado en el dispositivo.

Una CSR contiene:

- información de solicitud de certificado: asunto solicitado y otros atributos, clave pública del par de claves,
- información del algoritmo de firma,
- firma digital de la información de solicitud de certificado, firmada con la clave privada del par de claves.

La CSR se pasa a la Autoridad de Certificación (CA), para que la firme, en un formulario PKCS#10.

El certificado firmado se devuelve desde la CA en un formulario PEM.

Nota: CA puede modificar los parámetros FQDN y nombre de sujeto definidos en el punto de confianza cuando firma el CSR y crea un certificado de identidad firmado.

Generación de un CSR con ASDM

- 1. Crear un punto de confianza con un nombre específico
 - a. Vaya a Configuración > Administración de dispositivos > Administración de certificados
 > Certificados de identidad.



- b. Haga clic en Add (Agregar).
- c. Defina un nombre de punto de confianza.

sued To	Issued By	Expiry Date	Associated Trustpoints	∧ ¹ Usage	Public Key Type	Add
🔄 Add Identity Certi	ficate				×	Show Detail
Trustpoint Name:	SSL-Trustpoint					Delete
O Import the identit	ty certificate from a file (PKCS12 format with Certificat	te(s)+Private Key):			Export
Decryption Passp	hrase:					Install
File to Import Fro	m:	Brows	e			Re-Enrol
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=asavpn.exa	mple.com Select	t			
Generate self	-signed certificate					
Act as loc	al certificate authority ar	d issue dynamic certificates	to TLS-Proxy			
			Advanced			
Enable CA fla	g in basic constraints ext	ension				

- d. Haga clic en el botón de opción Add a New Identity Certificate .
- 2. (Opcional) Creación de un nuevo par de claves

Nota: De forma predeterminada, se utiliza la clave RSA con el nombre Default-RSA-Key y un tamaño de 2048. Sin embargo, se recomienda utilizar un único par de claves pública y privada para cada certificado de identidad.

a. Haga clic en Nuevo para generar un nuevo par de claves.

isued To	Issued By	Expiry Da	te	Associated Trustp	points	Usage	Public Key Type	Add
Add Identity Ce	rtificate				×	General Purpose	RSA (4096 bits)	Show Detai
					-	General Purpose	RSA (2048 bits)	Delete
Trustpoint Name:	SSL-Trustpoint							
O Import the ider	ntity certificate from a file (PKCS12 format with	Certificate(s)+P	rivate Key):				Export
Decryption Pas	sphrase:	Į.						Install
File to Import F	rom:		Browse					Re-Enrol
Add a new ider	ntity certificate:							
Key Pair:	<default-rsa-< td=""><td>⟨ey> ∨</td><td>Show</td><td>New</td><td></td><td></td><td></td><td></td></default-rsa-<>	⟨ey> ∨	Show	New				
Certificate Sub	ject DN: CN=asavpn.ex	ample.com	Select					
Generate s	elf-signed certificate							
Act as	ocal certificate authority a	nd issue dynamic ce	rtificates to TLS-f	гоху				
			_					
				Advanced				
Enable CA	flag in basic constraints ex	tension						

- b. Elija la opción Enter new Key Pair name e ingrese un nombre para el nuevo Key Pair.
- c. Elija el Tipo de clave: RSA o ECDSA.
- d. Elija el tamaño de clave; para RSA, elija propósito general para uso.
- e. Haga clic en Generar ahora. Ya se ha creado el par de claves.

1000000	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
Add Identity Certificate		×	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)	Show Detai
Trustpoint Name: SSL-Trustpoint					Delete
O Impor 🔁 Add Key Pair		×			Export
Decry	0.000				Install
File to	O ECDSA O EDD	5A			Re-Enrol
Add a Name: ① Use default key pa	air name				
Key Pa	ir name: SSL-Keypair				
Certifi Size: 2048					
Ge Usage: General purpose	() Special	3			
Generate Now	Cancel He	elp			

3. Elija el nombre del par de claves

Elija el par de claves con el que firmar el CSR y al que se vinculará con el nuevo certificado.

isued To Is	sued By	Expiry Date	Associated Trustp	oints	Usage	Public Key Type	Add
Add Identity Certificate				×	General Purpose	RSA (4096 bits)	Show Deta
					General Purpose	RSA (2048 bits)	Delete
Trustpoint Name:	SSL-Trustpoint						Event
 Import the identity certi 	ficate from a file (PKC	512 format with Certi	ficate(s)+Private Key):				Export
Decryption Passphrase:							Install
File to Import From:		Br	owse				Re-Enrol
Add a new identity certi	ficate:						
Key Pair:	SSL-Keypair	S	how New				
Certificate Subject DN:	CN=asavpn.example	e.com S	elect				
Generate self-signed	d certificate						
Act as local certi	ficate authority and is	sue dynamic certifica	tes to TLS-Proxy				
			Advanced	-			
Act as local certi	ficate authority and is:	sue dynamic certifica	Advanced				

4. Configure el asunto del certificado y el nombre de dominio completamente calificado (FQDN)

Precaución: el parámetro FQDN debe coincidir con el FQDN o la dirección IP de la interfaz ASA para la que se utiliza el certificado de identidad. Este parámetro establece la extensión de nombre alternativo de sujeto (SAN) solicitada para el certificado de identidad. El cliente SSL/TLS/IKEv2 utiliza la extensión SAN para verificar si el certificado coincide con el FQDN al que se conecta.

a. Haga clic en Seleccionar.

Issued To	Issued By	Expiry Date	Associated Trustpoints	∧ ¹ Usage	Public Key Type	Add
Add Identity C	ertificate				×	Show Detail
Trustpoint Name:	SSL-Trustpoint					Delete
○ Import the ide	entity certificate from a file (F	PKCS12 format with Certificate(s)	+Private Kev):			Export
Decryption Pa	assphrase:					Install
File to Import	From:	Browse				Re-Enroll
Add a new ide	entity certificate:		-			
Key Pair:	SSL-Keypair	~ Show	New			
Certificate Sul	bject DN: CN=asavpn.exa	mple.com Select				
Generate	self-signed certificate					
Act as	s local certificate authority an	d issue dynamic certificates to TL	S-Proxy			
_			Advanced			
Enable CA	A flag in basic constraints ext	ension				
		Add Cart Carts	Coursel Units	-		
		Add Certificate	Cancel Help			

b. En la ventana Certificate Subject DN, configure certificate attributes - choose attribute from drop-down list, ingrese el valor, haga clic en 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

Issued To	Issued By	Expiry Date	Associ	ated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Certific	ate						×	Show Detail
Trustpoint Name:	SSL-Trustpoint							Delete
O Import the identity	e 🕞 Cartificata Subi	act DN				×		Export
Decryption Passphra	ist	ecton				^		Install
File to Import From:				Attribute	Value			Re-Enroll
Add a new identity	DN Attribute to	o be Added		Common Name (CN) asa.vpn.e	xam		
Key Pair:	Attribute:	Country (C) 🗸 🗸	Add>>					
Certificate Subject	N Value: D	epartment (OU)	Delete					
Generate self-si	gn C	Company Name (O)						
Act as local	sei S	itate (St)						
	6	imail Address (EA)						
		ОК	Cancel	Help				
						_		
		Add Certificate	Cancel	Help				

Atributo	Descripción
CN	El nombre a través del cual se puede acceder al firewall (normalmente el nombre de dominio completo, por ejemplo, vpn.example.com).
OU	El nombre de su departamento dentro de la organización
0	El nombre registrado legalmente de su organización/empresa
С	Código de país (código de 2 letras sin puntuación)
ST	El estado en el que se encuentra la organización.
L	La ciudad en la que se encuentra su organización.
EA	Dirección de correo

Nota: ninguno de los valores de campos anteriores puede superar un límite de 64 caracteres. Un valor mayor podría causar problemas con la instalación del certificado de identidad. Además, no es necesario definir todos los atributos DN.

Haga clic en Aceptar después de agregar todos los atributos.

c. Configure el FQDN del dispositivo: haga clic en Advanced.

ssued To	Issued By	Expiry Dat	e	Associated Trustpoints	^1	Usage	Public Key Ty	/pe	Add
Add Identity Certi	ficate	Ne oriente de la companya de la comp						×	Show Deta
Trustpoint Name:	SSL-Trustpoint								Delete
Import the identit	ty certificate from a file (Pi	CS12 format with C	Certificate(s)+Priva	ate Kev):					Export
Decryption Passo	hrase:								Install
File to Import Fro	m:		Browse						Re-Enro
Add a new identit	ty certificate:								
Key Pair:	SSL-Keypair	~	Show	New					
Certificate Subject	ct DN: CN=asa.vpn.exa	mple.com	Select						
Generate self	f-signed certificate								
Act as loc	al certificate authority and	issue dynamic certi	ficates to TLS-Pro:	ку				-	
								_	
			Ad	vanced					
Enable CA fla	ig in basic constraints exte	nsion							

d. En el campo FQDN, introduzca el nombre de dominio completo a través del cual se puede acceder al dispositivo desde Internet. Click OK.

Issued To	ISSUED Data Accepted Trustaniata	1 10000	Public Key Type	Add
Add Identity Ce	ertificate	×	×	Show Detail
	Enrollment mode parameters and SCEP challenge password are not available for self-signed	certificates.		Delete
Trustpoint Name:	S Certificate Parameters Enrollment Mode SCEP Challenge Password			Export
 Import the ider 	ntity certifica			Install
Decryption Pas	ssphrase:			2 in Secon
File to Import F	From:			Re-Enrol
Add a new ider	ntity certifica			
Key Pair:	S			
Certificate Subj	ject DN: C			
Generate s	self-signed ce			
Act as I	local certifica			
Enable CA	flag in basic (
		12		

- 5. Generar y guardar el CSR
 - a. Haga clic en Agregar certificado.

sued To	Issued By	Expiry	Date	Associated Trustpoints	^1	Usage	Public Key Type		Add
Add Identity Certifie	cate						×	<	Show Detai
Trustpoint Name:	SSL-Trustpoint	1							Delete
Import the identity	certificate from a file (PK	CS12 format wit	h Certificate(s)+Pr	ivate Key):					Export
Decryption Passphr	ase:								Install
File to Import From	:		Browse						Re-Enrol
Add a new identity	certificate:								
Key Pair:	SSL-Keypair	~	Show	New					
Certificate Subject	DN: CN=asa.vpn.exam	ple.com	Select						
Generate self-s	igned certificate								
Act as local	certificate authority and i	ssue dynamic o	ertificates to TLS-Pi	roxy				-	
				Advanced					
Enable CA flag	in basic constraints exten	sion							

b. Se muestra un mensaje para guardar el CSR en un archivo en la máquina local.

ssued To	Issued By	Expiry Date	Associated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Certific	ate					×	Show Detail
Trustpoint Name:	SSL-Trustpoin	itl					Delete
Import the identity of th	certificate from a file	e (PKCS12 format with Certificate(s)+Private Key):				Export
Decryption Passphra	ise:						Install
File to Import From:		Identity Certificate Request		×			Re-Enroll
Add a new identity of Key Pair: Certificate Subject D	SSL-Keypa SSL-Keypa N: CN=asa.vr gned certificate	You will then need to install the or clicking the Install button in the Io Save CSR to File:	ertificate that is returned from the C lentity Certificates panel.	A by			
Act as local o	certificate author	ОК	Cancel Help Advanced				
Enable CA flag ir	n basic constraints e	extension					

Haga clic en Browse, elija una ubicación en la que guardar el CSR, y guarde el archivo con la extensión .txt.

Nota: Cuando el archivo se guarda con una extensión .txt, la solicitud PKCS#10 se puede abrir y ver con un editor de texto (como el Bloc de notas).

c. Ahora el nuevo punto de confianza se muestra en un estado Pendiente.

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

Instalación del Certificado de Identidad en formato PEM con ASDM

En los pasos de instalación, se supone que la CA firmó el CSR y proporcionó un paquete de certificados de CA y un certificado de identidad codificados por PEM (.pem, .cer, .crt).

- 1. Instalar el certificado de CA que firmó el CSR
 - a. Vaya a Configuration > Device Management >Certificate Management > y elija CA Certificates. Haga clic en Add (Agregar).

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

b. Introduzca el nombre del punto de confianza y seleccione Install From File (Instalar desde archivo), haga clic en el botón Browse (Examinar) y seleccione el certificado intermedio. También puede pegar el certificado de CA codificado PEM de un archivo de texto en el campo de texto.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active	Add
enTrust Commercial Root	CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Edit
ioVadis Root CA 2	CN=QuoVadis Root CA 2,	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	
Install Certificate			×			Show Detai
						Request CF
Trustpoint Name:	SSL-Trustpoint					Delete
Install from a file:		Browse				
O Paste certificate in	PEM format:					

- Nota: instale el certificado de CA que firmó el CSR. Utilice el mismo nombre de punto de confianza que el certificado de identidad. Los otros certificados de CA superiores en la jerarquía PKI se pueden instalar en puntos de confianza independientes.
- c. Haga clic en Install Certificate.

		Expiry Date	Associated Trustpoints	Usage	Active	Add
denTrust Commercial Roo	ot 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	COIL
Install Certificate					×	Show Details
Trustpoint Name:	SSL-Trustpoint	1				Request CRI
○ Install from a file:		Browse				Delete
Paste certificate in	DEM format:					
9tt FV52U47em5U CGqeVMRhsRs/ 2skqaRijsx153W/ OR yajH58Plad gW8YnHOvM08sy dc/covO/PAurnAl BND CERTIFIC Use EST: Specify source Int EST URL: https:// Certificate Subject allow-untruste Use SCEP: Specify source Int SCEP URL: http://	caMaGocSqGSID=DQEBCWUAA4BP Lo2Sm2wka47a/bgNgKvQC+H UKBE90Alatha/fQfKvU+15*Km2#E Lo2RddtVXYB9sfEbFn IC/RcddtVXYB9sfEbFn I=Ng2WFN3WKWZ0- ATE DN: CN=risavpn31 DN: CN=risavpn31 d-connection erface: None	AQArs/HPWK3/NEWOSY/h5mgT doc/MQ2y4X/ub/5SNDU70Ff6f separate wait Please wait while ASDM is delive device	X INFO: Certificate has the Fingerprint: e9ad165c 267 Trustpoint CA certificate a	following attributes: 73424c 6e7e0c5f b30b iccepted. Ж	4402	

- 2. Instalar certificado de identidad
 - a. Elija el certificado de identidad creado anteriormente durante la generación de CSR. Haga clic en Instale.

Configuration > Re	mote A	ccess VPN > Certific	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: El certificado de identidad puede tener el campo Emitido por como No disponible y el campo Fecha de vencimiento como Pendiente.

 b. Elija un archivo que contenga el certificado de identidad con codificación PEM recibido de la CA, o abra el certificado con codificación PEM en un editor de texto y copie y pegue el certificado de identidad proporcionado por la CA en el campo de texto.

Jed To	^1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
n.example.com]		Not Available	Pending	SSL-Trustpoint	Unknown		Show Detail
Install Islanding				~	General Purpose	RSA (2048 bits)	
Install identity	centifica	te		tpoint t	General Purpose	RSA (2048 bits)	Delete
ntity Certificate							Export
Install from a	file:			Browse			Install
O Paste the cert	tificate d	ata in base-64 format	ti				Re-Forol
O Paste the cert	tificate d	ata in base-64 format	t:				Re-Enroll
O Paste the cert	tificate d	ata in base-64 format	tı				Re-Enroll
O Paste the cert	tificate d	ata in base-64 formal	t:				Re-Enroll
O Paste the cert	tificate d	ata in base-64 formal	t:				Re-Enroll
O Paste the ceri	tificate d	ata in base-64 formal	t:				Re-Enroll

Nota: el certificado de identidad puede tener el formato .pem, .cer o .crt para su instalación.

c. Haga clic en Install Certificate.

sued To ^1 Issued E	by Ex	piry Date	Associated Trustpoints	Usage	Public Key Type	Add
on.example.com] Not Avai	able Per	nding	SSL-Trustpoint	Unknown		Show Details
Install Identify antificate			~	General Purpose	RSA (2048 bits)	
Install Identity certificate			tpoint	General Purpose	RSA (2048 bits)	Delete
dentity Certificate	🧧 Please wait		×			Export
Install from a file:			Information	×		Install
 Paste the certificate data in be LinNB J26XgDmVuQjHEMVXR2K Gyer3x2GML7MAHBEMVXR2K KdVqFbUM4W9NTuF2DowH3 END CERTIFICATE 	device	t while ASUM is delivering	Certificate impor	t succeeded.		Re-Enroll

3. Enlace del Nuevo Certificado a la Interfaz con ASDM

El ASA debe configurarse para utilizar el nuevo certificado de identidad para las sesiones WebVPN que terminan en la interfaz especificada.

- a. Vaya a Configuration > Remote Access VPN > Advanced > SSL Settings.
- b. En Certificados, elija la interfaz que se utiliza para terminar las sesiones WebVPN. En este ejemplo, se utiliza la interfaz externa.

Haga clic en Editar.

c. En la lista desplegable Certificado, seleccione el certificado recién instalado.

Specify enrolled trustpoints to be used for SSL au OUTSIDE-direct interface. To enroll a trustpoint, r	Delete
Specify enrolled trustpoints to be used for SSL au OUTSIDE-direct interface. To enroll a trustpoint,	X with an interview and VDN load halancing on the
Specify enrolled trustpoints to be used for SSL au OUTSIDE-direct interface. To enroll a trustpoint, a	uthantication and VDN load balancing on the
Management > Identity (entiticates	go to Device Management > Certificate
ertificates Outputs to	
Specify which certificates, if an Interface: 001510E-dire	ecc es not associated with a certificate of their own.
Interface SSL-Truspo	Key-Type Edit
OUTSIDE-direct Load Balancing Enrolled Certificate: None	
inside	
inside-vlan	ancel Hep
management	

- d. Click OK.
- e. Haga clic en Apply (Aplicar).

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

Ahora el nuevo certificado de identidad está en uso.

Instalación de un Certificado de Identidad Recibido en Formato PKCS12 con ASDM

El archivo PKCS12 (formato .p12 o .pfx) contiene el certificado de identidad, el par de claves y los certificados de CA. Es creado por la CA, por ejemplo, en el caso de un certificado comodín, o exportado desde un dispositivo diferente. Es un archivo binario, no se puede ver con el editor de texto.

1. Instalar la identidad y los certificados de CA desde un archivo PKCS12

El certificado de identidad, los certificados de CA y el par de claves deben incluirse en un único archivo PKCS12.

- a. Navegue hasta Configuration > Device Management > Certificate Management, y elija Identity Certificates.
- b. Haga clic en Add (Agregar).
- c. Especifique un nombre de punto de confianza.

					Show Detai
		×			Delete
SSL-Trustpoint-PKCS1	2				Export
ficate from a file (PKCS1	2 format with Certificate(s)+Pr	rivate Key):			Install
					Re-Enrol
	Browse				
ificate:					
<default-rsa-key></default-rsa-key>	Show	New			
CN=risavpn31	Select				
d certificate					
ificate authority and issu	e dynamic certificates to TLS-P	roxy			
		Advanced			
sic constraints extension	i				
	SSL-Trustpoint-PKCS1 frate from a file (PKCS1 frate: CDefault-RSA-Key> CN=risavpn31 d certificate ficate authority and issu	SSL-Trustpoint-PKCS12 frate from a file (PKCS12 format with Certificate(s) +Pr Browse frate:	SSL-Trustpoint-PKCS12 SSL-Trustpoint-PKCS12 facate from a file (PKCS12 format with Certificate(s) +Private Key): Browse Browse Browse CN=risavpn31 Select d certificate facate authority and issue dynamic certificates to TLS-Proxy Advanced Browse Browse Advanced Browse Browse	SSL-Trustpoint-PKCS12 fcate from a file (PKCS12 format with Certificate(s)+Private Key): Browse Browse fcate: Obefault-RSA-Key> Show New Otertificate fcate authority and issue dynamic certificates to TLS-Proxy Advanced	SSL-Trustpoint-PKCS12 fcate from a file (PKCS12 format with Certificate(s)+Private Key): Browse Browse fcate: Obefault-RSA-Key> Show New Otertificate fcate authority and issue dynamic certificates to TLS-Proxy Advanced

d. Haga clic en el botón de opción Import The Identity Certificate from a File .

	Issued By	Expiry D	Date	Associated	Trustpoints	Usage	Public Key	Туре	Add
									Show Detai
🔁 Add Identity Certifi	icate			()	×				Delete
Trustpoint Name:	SSL-Trustpoint-PI	KCS12]		import ID cert	tificate file			
Import the identity	certificate from a file (P	KCS12 format wi	th Certificate(s)+P	rivate Key):	Look in:	Document	5	 Image: state of the state of th	
Decryption Passph	rase:]		0.	CSR.txt			
File to Import From	1:		Browse		Recent Items	🖄 vpn.exan	ple.com.pfx		
O 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></default-rsa-ke<>	:y> ~	Show	New	Desktop				
Certificate Subject	DN: CN=risavpn31		Select						
Generate self-	signed certificate				Documents				
Act as loca	l certificate authority and	d issue dynamic c	certificates to TLS-f	roxy					
				Advanced	This PC	File name:	vpn.example.com.pfx	Import	ID certificate file
	in basic constraints outs	uncion.		Advanced	S	Files of type:	All Files	~	Cancel
Enable CA flag	In Dasic Consulaints exte	nsion							

e. Introduzca la frase de paso utilizada para crear el archivo 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. Haga clic en Agregar certificado.

sued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
		, ,				Show Details
🗧 Add Identity C	ertificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-F	PKCS12				Export
 Import the ide 	entity certificate from a file (F	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 🛄 Ple	ase wait		Information			×
Certi 😰	device	is derivering une command(s) to	Created trustpoint WARNING: CA cer the validation-usag	is for CAs higher in the hie tificates can be used to va ge of this trustpoint to limit	erarchy as the CA certificate was not s alidate VPN connections,by default. Pli t the validation scope, if necessary	elf-signed.
			Import PKCS 12 opt	eration completed success	sfully.	

Nota: Al importar un PKCS12 con la cadena de certificados de CA, el ASDM crea automáticamente los puntos de confianza de CA ascendentes con nombres con el sufijo -number agregado

nfiguration > Remote /	Access VPN > Certificate N	lanagement > <u>CA Certificates</u>			
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. Enlace del Nuevo Certificado a la Interfaz con ASDM

El ASA debe configurarse para utilizar el nuevo certificado de identidad para las sesiones WebVPN que terminan en la interfaz especificada.

a. Vaya a Configuration > Remote Access VPN > Advanced > SSL Settings.

b. En Certificados, seleccione la interfaz que se utiliza para terminar las sesiones WebVPN. En este ejemplo, se utiliza la interfaz externa.

Haga clic en Editar.

c. En la lista desplegable Certificado, seleccione el certificado recién instalado.

	Constructor	Edit
rtificates Specify which certificates, if ar Interface OUTSIDE-direct inside inside-vlan management	Select SSL Certificate × Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate Management > Identity Certificates. Interface: OUTSIDE-direct Primary Enrolled Certificate: SSL-Trustpoint-PKCS 12:unstructuredName=FTD72-ek, u v Load Balancing Enrolled Certificate: None OK Cancel Help	sted with a certificate of their own.
Fallback Certificate: Forced Certification Authentica	None V	

- d. Click OK.
- e. Haga clic en Apply (Aplicar).

Certi	ficates	a used for SSL suthentication on each interface. Th	a fallback cartificate will be used on interfaces not accord	isted with a cartificate of their own	
spi	Tabafaaa	Diagona Castificate	le raiback ceruncate will be used on interfaces not assoc	dated with a certificate of their own.	Edit
	Interface	Primary Certificate	Load Balancing Certificate	key-Type	Luc
	OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName=F		Primary: RSA (2048 bits), Load Balan	

Ahora el nuevo certificado de identidad está en uso.

Renovación de certificados

Renovación de un certificado inscrito con solicitud de firma de certificado (CSR) con ASDM

La renovación del certificado CSR inscrito requiere crear e inscribir un nuevo punto de confianza. Debe tener un nombre diferente (por ejemplo, nombre antiguo con sufijo de año de inscripción). Puede utilizar los mismos parámetros y par de claves que el certificado anterior, o puede utilizar otros diferentes.

Generación de un CSR con ASDM

- 1. Cree un nuevo punto de confianza con un nombre específico.
 - a. Vaya a Configuración > Administración de dispositivos > Administración de certificados

> Certificados de identidad.



- b. Haga clic en Add (Agregar).
- c. Defina un nombre de punto de confianza.

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

- d. Haga clic en el botón de opción Add a New Identity Certificate .
- 2. (Opcional) Creación de un nuevo par de claves

Nota: De forma predeterminada, se utiliza la clave RSA con el nombre Default-RSA-Key y un tamaño de 2048; sin embargo, se recomienda utilizar un par de claves privada/pública único para cada certificado de identidad.

a. Haga clic en Nuevo para generar un nuevo par de claves.

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. Elija la opción Enter new Key Pair name e ingrese un nombre para el nuevo Key Pair.
- c. Elija el tipo de clave: RSA o ECDSA.
- d. Elija el tamaño de clave; para RSA, elija Propósito general para Uso.
- e. Haga clic en Generar ahora. Ya se ha creado el par de claves.

ssued 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 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
🔁 Add Identit	y Certificate		×			Delete
Trustpoint Nar	me: SSL-Trustpoint-	2023				Export
C 🖾 Add I	Key Pair		× _{Key):}			Install
Key Typ	pe:) RSA	⊖ ECDSA ⊖ EDDS	A			Re-Enrol
Name:	O Use default key pair nar	ne				
Cincu	Enter new key pair nam	e: SSL-KeyPair-2023	ew			
Usage:	General purpose	Special				
	Generate Now Can	cel Help	iced			
	CONTRACT TO CARLE CARDON CA	Autoriti	_			
	Add Certificate	Cancel Help				

3. Seleccione el nombre del par de claves

Elija el par de claves con el que firmar el CSR y al que se vinculará con el nuevo certificado.

ssued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName= (CN=ca.example.com, OU	15:10:00 CEST F	Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🔄 Add Identity Cert	lificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
O Import the identi	ity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Pass	phrase:						Re-Enroll
File to Import Fro	om:		Browse				
Add a new identi	ity certificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate Subje	ect DN: CN=asavpn.exam	ple.com	Select				
Generate sel	lf-signed certificate						
Act as lo	cal certificate aut Crity and	issue dynamic cer	tificates to TL	S-Proxy			
				Advanced			
		vien					

4. Configure el asunto del certificado y el nombre de dominio completamente calificado (FQDN)

Precaución: el parámetro FQDN debe coincidir con el FQDN o la dirección IP de la interfaz ASA para la que se utiliza el certificado. Este parámetro establece el nombre alternativo del sujeto (SAN) para el certificado. El campo SAN es utilizado por el cliente SSL/TLS/IKEv2 para verificar si el certificado coincide con el FQDN al que se conecta.

Nota: CA puede modificar los parámetros FQDN y nombre de sujeto definidos en el punto de confianza cuando firma el CSR y crea un certificado de identidad firmado.

a. Haga clic en Seleccionar.

sued to Issu	ued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
structuredName= CN=	=ca.example.com, OU	15:10:00 CEST F	eb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detai
Add Identity Certific	ate			×			Delete
Trustnoint Name	SSI .Trustpoint.201	23					Export
Import the identity of th	certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Passphra	ase:						Re-Enroll
File to Import From:			Browse				
Add a new identity of the second s	certificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate Subject D	DN: CN=asavpn.examp	ole.com	Select				
Generate self-si	igned certificate						
Act as local of	certificate authority and i	issue dynamic cer	tificates to TL	S-Proxy			
				Advanted			
Enable CA flag ir	n basic constraints exten	sion		Auvanceu			

b. En la ventana Certificate Subject DN, configure certificate attributes - select attribute from drop-down list, ingrese el valor, haga clic en Add.

ssued To	Issued By	Expiry D	late	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName=	CN=ca.example.com, OU	J 15:10:0) CEST Feb 6 2024	SSL-Trustpoint	General Purpo	se RSA (2048 bits)	Show Deta
🧧 Add Identity (Certificate			×			Delete
Trustpoint Name	: SSL-Trustpoint	-2023					Export
ertificate Subject	DN				×		Install
			-				Re-Enroll
			Attribute	Value			
DN Attribute to be	Added		Company Name (CN Company Name (O)	example inc			
Attribute: Cour	ιθγ (C) 🗸	Add>>					
value: US		Delete					
					-		
	-						
	OK	Cancel	Help				
	A flag in basic constraints ex	tension					

Atributo	Descripción
CN	El nombre a través del cual se puede acceder al firewall (normalmente el nombre de dominio completo, por ejemplo, vpn.example.com).
ου	El nombre de su departamento dentro de la organización
0	El nombre registrado legalmente de su organización/empresa
с	Código de país (código de 2 letras sin puntuación)
ST	El estado en el que se encuentra la organización.
L	La ciudad en la que se encuentra su organización.
EA	Dirección de correo

Nota: ninguno de los campos anteriores puede superar un límite de 64 caracteres. Un valor mayor podría causar problemas con la instalación del certificado de identidad. Además, no es necesario definir todos los atributos DN.

Haga clic en Aceptar después de agregar todos los atributos.

c. Para configurar el FQDN del dispositivo, haga clic en Advanced.

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	sst-Trustpoint-20	23					Export
O Import the id	dentity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption P	Passphrase:						Re-Enroll
File to Impor	rt From:		Browse				
Add a new id	dentity certificate:						
Key Pair:	SSL-KeyPair-2023	×	Show	New			
Certificate S	ubject DN: /pn.example.com	,O=example inc	Select				
Generat	e self-signed certificate						
Act a	as local certificate authority and	issue dynamic ce	tificates to TL	S-Proxy			
				Advanced			
			L	Advanced			
	.A flag in basic constraints exter	nsion					

d. En el campo FQDN, introduzca el nombre de dominio completo a través del cual se puede acceder al dispositivo desde Internet. Click OK.

Certificate Parameters and SCEP challenge password are not available for self-signed certificates. Certificate Parameters Enrollment Mode SCEP Challenge Password FQDN: asavpn.example.com	its) Show Deta Delete Export Install
Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates. Certificate Parameters Enrollment Mode SCEP Challenge Password FQDN: asavpn.example.com	Delete Export
Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates. Certificate Parameters Enrollment Mode SCEP Challenge Password	Export
FQDN: asavpn.example.com	Install
FQDN: asavpn.example.com	at the cost
	Re-Enrol
E-mail:	
2	

- 5. Generar y guardar el CSR
 - a. Haga clic en Agregar certificado.

ssued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName=	CN=ca.example.com, OU	. 15:10:00 CEST F	eb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
🔄 Add Identity	Certificate			×			Delete
Trustpoint Name	SSL-Trustpoint-20	023					Export
O Import the id	dentity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption P	Passphrase:						Re-Enroll
File to Impor	rt From:		Browse				
Add a new id	dentity certificate:						
Key Pair:	SSL-KeyPair-2023	3 ~	Show	New			
Certificate S	ubject DN: /pn.example.com	,0=example inc	Select				
Generat	e self-signed certificate						
Act a	as local certificate authority and	l issue dynamic cer	tificates to TL	S-Proxy			
				Advanced			
Enable C	CA flag in basic constraints exter	nsion					

b. Se muestra un mensaje para guardar el CSR en un archivo en la máquina local.

ssued to	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
🗟 Add Identity	Certificate		×			Delete
Trustooint Name	ssi -Trustnoint-20	123				Export
O Import the id	dentity certificate from a file (PK	KCS12 format with Certificate(s	:) +Private Key):			Install
f 🕞 Mart	it. Cadificata Parmat	-	~			Re-Enroll
F		lease save the DVCC 10 secolu				
reques	t (CSR) and send it to the CA.	lease save the PKCS 10 enrollm	ent			
K You wil clicking	I then need to install the certific the Install button in the Identit	ate that is returned from the C ty Certificates panel.	CA by			
[Save C	SR to File: C:\Users\cisco.DES	KTOP-R2CH8G5\Docun Br	owse			
	ОКС	ancel Help				
			Advanced			
Enable C	A flag in basic constraints exter	nsion	Hardente			
	A nug in busic const units exter					

Haga clic en Examinar. Elija una ubicación en la que guardar el CSR y guarde el archivo con la extensión .txt.

Nota: Cuando el archivo se guarda con una extensión .txt, la solicitud PKCS#10 se puede abrir y ver con un editor de texto (como el Bloc de notas).

c. Ahora el nuevo punto de confianza se muestra en un estado Pendiente.

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

Instalación del Certificado de Identidad en Formato PEM con ASDM

En los pasos de instalación se supone que la CA firmó el CSR y proporcionó un nuevo paquete de certificados de identidad y certificados de CA codificado por PEM (.pem, .cer, .crt).

1. Instalar el certificado de CA que firmó el CSR

El certificado de CA que firmó el certificado de identidad se puede instalar en el punto de confianza creado para el certificado de identidad. Si el certificado de identidad está firmado por una CA intermedia, este certificado de CA se puede instalar en el punto de confianza del certificado de identidad. Todos los certificados de CA ascendentes de la jerarquía se pueden instalar en puntos de confianza de CA independientes.

a. Vaya a Configuración > Administración de dispositivos >Administración de certificados
 > y elija Certificados de CA. Haga clic en Add (Agregar).

Configuration > Device Man	agement > Certificate Man	agement > <u>CA Certificates</u>				
Issued To	Issued By	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	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
IdenTrust Commercial Root	CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Show Details
						Request CRL
						Delete

 b. Ingrese el nombre de Trustpoint y elija Install From File, haga clic en el botón Browse y elija el certificado intermedio. También puede pegar el certificado de CA codificado PEM de un archivo de texto en el campo de texto.

Issued To	Issued By ^1	Expiry Date	Associated Trustpoints	Usage	Active		Add
a.example.com	CN=ca.example.com, OU=I	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes		Edit
Trustpoint Name:	SSL-Trustpoint-2023	1					Show Detai
Install from a file	:	Browse				1	Delete

Nota: instale el certificado intermedio con el mismo nombre de punto de confianza que el nombre de punto de confianza del certificado de identidad, si el



Certificado de identidad está firmado por un certificado de CA intermedio.

c. Haga clic en Install Certificate.

ssued To Is	ssued By ^1	Expiry Date	Associated Trustpoints	Usage	Active		Add
a.example.com CI	N=ca.example.com, OU=l	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes		Edit
🔁 Install Certificate						× Sho	w Details
Trustpoint Name: SSL-	-Trustpoint-2023					Req	uest CRI
O Install from a file:		Browse					Delete
Paste certificate in PEM f	format:						
OH EVEDI 147am0 VaMA0	ACCO COT DO OTRO UNA MTO	AOAreVEw/2iNBwOeVbEmaT					
JUL V320/veriBV0.arMul cGqeyDMRhis 3Rs/M0259 25kqaRijsx1533/VLl&B9 QRyaH568FladMc7Rq gW8YmH0vM08svyTXSL dcVcovO/PAxmrAl3+Ng2 END CERTIFICATE Use EST: Specify source Interface EST URL: https:// Certificate Subject DN: allow-untrusted-conr Use SCEP:	JdCSqCsiD 30CeBC/UDAAHBI JdACSqCsiD 30CeBC/UDAAHBI JoAlathA/fQfX6V+h7 JJf0UCdmAY+IG0gqh JJf0UCdmAY+IG0gqh 2jrWFN3MXWZO4530	iformation INFO: Certificate ha Fingerprint: e9ad16 Trustpoint CA certifi	as the following attributes: 5c 2673424c 6e7e0c5fb30b4a02 icate accepted. OK	×		~	
SPL-YS20-VEINSULAINU, GGQeyDMRhs3Rs/W0259 Z9kqaRijsx1533/VLk89 J0Ry3H56BFladkNc7Rc, J0W3YNHOW08svyTXSL dcVcovOl/PAwnAl3-Ng2 END CERTIFICATE Use EST: Specify source Interface EST URL: https:// Certificate Subject DN: allow-untrusted-conr Use SCEP: Specify source Interface	Jac Sqcsib SDCBC/UDAAHB JackAF4472F499gK @ In JoAlathA/fQfK6V+h7 JoAlathA/fQfK6V+h7 JJfDUCdmAY+lG0gh JgrWFN3NXWZO4532 ::None	iformation INFO: Certificate ha Fingerprint: e9ad16 Trustpoint CA certificate	as the following attributes: 5c 2673424c 6e7e0c5fb30b4a02 icate accepted.	×		v .	
SULT 'S2U'HIBULARING GGQEYDMRhis 78,6/W0259 Z9KqaRijsx.1533/VLk89 J0RygHi56BFladkvC76R, GW9YnHO-M08svyTXSL deVcovOj/PAxmAJ-Ng2 END CERTIFICATE Use EST: Specify source Interface EST URL: https:// Certificate Subject DN: allow-untrusted-conr Use SCEP: Specify source Interface SCEP URL: http://	JdCSdcSib DCEC/UDAAHB JdCSdcSib DCEC/UDAAHB JoAlathA/fQfK6V H7 JoAlathA/fQfK6V H7 JdVWR95rbFNRoc JJ6UCdmAY HG0gh JgWFN3NXWZO4532 ::None	iformation INFO: Certificate ha Fingerprint: e9ad16 Trustpoint CA certifi	as the following attributes: 5c 2673424c 6e7e0c5fb30b4a02 icate accepted.	×		v .	

En el ejemplo, el nuevo certificado se firma con el mismo certificado de CA que el antiguo. El mismo certificado de CA está asociado ahora a dos puntos de confianza.

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

- 2. Instalar certificado de identidad
 - a. Elija el certificado de identidad creado anteriormente con la generación CSR. Haga clic en Instale.

nfiguration > Device	e Management > Certifica	ite 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: El certificado de identidad puede tener el campo Emitido por como No disponible y el campo Fecha de vencimiento como Pendiente.

b. Elija un archivo que contenga el certificado de identidad con codificación PEM recibido de la CA, o abra el certificado con codificación PEM en un editor de texto, y copie y pegue el certificado de identidad proporcionado por la CA en el campo de texto.

sued To	Issued By	Expiry Date	Associated Trustpoints ~	¹ Usage	Public Key Type	Add
structuredName	= CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detai
avpn.example.c	om] Not Available	Pending	SSL-Trustpoint-2023	Unknown		Delete
						Delete
						Export
lnstall Identi	ty certificate		×			Install
entity Certifica	te					Re-Enrol
Install from	a filo:		Province			-
			biowse			
O Paste the o	certificate data in base-64 format					

Nota: el certificado de identidad puede tener el formato .pem, .cer o .crt para su instalación.

c. Haga clic en Install Certificate.

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

Después de la instalación, hay certificados de identidad nuevos y antiguos presentes.

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

3. Enlace del Nuevo Certificado a la Interfaz con ASDM

El ASA debe configurarse para utilizar el nuevo certificado de identidad para las sesiones WebVPN que terminan en la interfaz especificada.

- a. Vaya a Configuration > Remote Access VPN > Advanced > SSL Settings.
- b. En Certificados, elija la interfaz que se utiliza para terminar las sesiones WebVPN. En este ejemplo, se utiliza la interfaz externa.

Haga clic en Editar.

c. En la lista desplegable Certificado, elija el certificado recién instalado.

					Edit	
[🔁 Select SSL Certificate		×			
tificates	Specify enrolled trustpoints to be us OUTSIDE-direct interface. To enroll a Management > Identity Certificates.	ed for SSL authentication and VPN load balancing on the a trustpoint, go to Device Management > Certificate		11		
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	~	Key-Type	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. Haga clic en Apply (Aplicar). Ahora el nuevo certificado de identidad está en uso.

	ss VPN > Advanced > SSL Settings			
				Edit Delete
ficates				
ificates ecify which certificates, if ar Interface	ny, should be used for SSL authentication on ear	ch interface. The fallback certificate will be us	sed on interfaces not associated with a certificate of their own. Kev-Type	Edit
ificates ecify which certificates, if ar Interface	ny, should be used for SSL authentication on ear Primary Certificate	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: BSA (4996 bits), Load Balancing: n	Edit
ificates ecify which certificates, if ar Interface OUTSIDE-direct inside	ny, should be used for SSL authentication on ear 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
ficates — ecify which certificates, if ar Interface OUTSIDE-direct inside inside-vlan	ny, should be used for SSL authentication on ear Primary Certificate SSL-Trustpoint-2023;unstructure	ch interface. The failback 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

Renovación de un Certificado Inscrito con el Archivo PKCS12 con ASDM

La renovación del certificado PKCS12 inscrito requiere crear e inscribir un nuevo punto de confianza. Debe tener un nombre diferente (por ejemplo, nombre antiguo con sufijo de año de inscripción).

El archivo PKCS12 (formato .p12 o .pfx) contiene el certificado de identidad, el par de claves y los certificados de CA. Es creado por la CA, por ejemplo, en el caso de un certificado comodín, o exportado desde un dispositivo diferente. Es un archivo binario y no se puede ver con el editor de

texto.

1. Instalación del certificado de identidad renovado y los certificados de CA desde un archivo PKCS12

El certificado de identidad, los certificados de CA y el par de claves deben incluirse en un único archivo PKCS12.

- a. Navegue hasta Configuration > Device Management > Certificate Management, y elija Identity Certificates.
- b. Haga clic en Add (Agregar).
- c. Especifique un nuevo nombre de Trustpoint.

ssued To	Issued By	Expiry Da	te	Associated Trustpoints	Usage	Public Key Type	Add
							Show Detai
📮 Add Identity C	ertificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-	PKCS12					Export
 Import the id 	entity certificate from a file ((PKCS12 format with	Certificate(s)+P	rivate Key):			Install
Decryption Pa	assphrase:						Re-Enroll
File to Import	From:		Browse				
O Add a new id	entity certificate:						
Key Pair:	<default-rsa-< td=""><td>Key> 🗸</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-<>	Key> 🗸	Show	New			
Certificate Su	bject DN: CN=risavpn31		Select				
Generate	self-signed certificate						
Act as	s local certificate authority a	nd issue dynamic ce	rtificates to TLS-F	Proxy			
				Adversed			
Enable C	A flag in basic constraints ex	tension		Advanced			

d. Haga clic en el botón de opción Import The Identity Certificate from a File .

Issued To	Issued By	Exp	iry Date	Associated	Trustpoints	Usage	Publ	іс Кеу Туре		Add
										Show Detail
Table Contract Add Identity Co	ertificate		L.		×				[Delete
Trustpoint Name:	SSL-Trustpoint-	PKCS12			Import ID certi	ficate file				
Import the ide	ntity certificate from a file (PKCS12 forma	t with Certificate(s)+P	rivate Kev):	Look in:	Document	ts	~	🍺 📂 🛄	,
Decryption Pa	ssohrase:				0	CSR.txt				
File to Import	From:		Browse		Recent Items	🏂 vpn.exan	nple.com.pfx			
O Add a new ide	ntity certificate:									
Key Pair:	<default-rsa-k< td=""><td>(ey></td><td>Show</td><td>New</td><td>Desktop</td><td></td><td></td><td></td><td></td><td></td></default-rsa-k<>	(ey>	Show	New	Desktop					
Certificate Sub	oject DN: CN=risavpn31		Select		<u>A-</u>					
Generate	self-signed certificate				Documents					
Act as	local certificate authority ar	nd issue dynar	mic certificates to TLS-P	Proxy						
				A down and	This PC F	File name:	vpn.example.com.pf	K	Import ID	certificate file
	A			Advanced	- <u>(</u>	Files of type:	All Files	~	Ca	ancel
	mag in basic constraints ext	CISION			1					

e. Introduzca la frase de paso utilizada para crear el archivo 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. Haga clic en Agregar certificado.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
🔁 Add Identity C	ertificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-F	PKCS12				Export
Import the 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		Information			×
Certi	Please wait while ASDM device	is delivering the command(s) to	the Created trustpoint WARNING: CA cer the validation-usage	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. Pk t the validation scope, if necessary	elf-signed.
Enable CA	flag in basic constraints ext	tension	Import PKCS 12 op	eration completed success	ifully.	
	Add Contificate	Cancel Hele		OK		

Nota: Cuando se importa una cadena PKCS12 con certificados de CA, el ASDM crea los puntos de confianza de CA ascendentes automáticamente con nombres con el sufijo -number agregado.

figuration > Remote Access VPN > Certificate Management > <u>CA Certificates</u>								
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. Enlace del Nuevo Certificado a la Interfaz con ASDM

El ASA debe configurarse para utilizar el nuevo certificado de identidad para las sesiones WebVPN que terminan en la interfaz especificada.

a. Vaya a Configuration > Remote Access VPN > Advanced > SSL Settings.

b. En Certificados, elija la interfaz que se utiliza para terminar las sesiones WebVPN. En este ejemplo, se utiliza la interfaz externa.

Haga clic en Editar.

c. En la lista desplegable Certificado, seleccione el certificado recién instalado.

	- Contractor	Edit Delete
ertificates Specify which certificates, if ar Interface OUTSIDE-direct inside inside-vlan management	Select SSL Certificate X Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To erroll a trustpoint, go to Device Management > Certificate Interface: OUTSIDE-direct Primary Enrolled Certificate: SSL-Trustpoint-PKCS 12:unstructuredName=FTD72-ek, u v Load Balancing Enrolled Certificate: None v OK Cance Help	with a certificate of their own.
Fallback Certificate: Forced Certification Authentica	ation Timeout: 2 minutes	

- d. Click OK.
- e. Haga clic en Apply (Aplicar).

Certi Sp	ficates — ecify which certificates, if any, should be	e used for SSL authentication on each interface. Ti	he fallback certificate will be used on interfaces not assoc	iated with a certificate of their own.	
	Interface	Primary Certificate	Load Balancing Certificate	Кеу-Туре	Edit
	OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName=F		Primary: RSA (2048 bits), Load Balan	

Ahora el nuevo certificado de identidad está en uso.

Verificación

Siga estos pasos para verificar la correcta instalación del certificado de proveedor de terceros y su uso para conexiones VPN SSL.

Ver certificados instalados mediante ASDM

- 1. Navegue hasta Configuration > Remote Access VPN > Certificate Management, y elija Identity Certificates.
- 2. Puede aparecer el certificado de identidad emitido por el proveedor externo.

Certi	Certificates								
Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.									
	Interface	Primary Certificate	Load Balancing Certificate	Кеу-Туре	Edit				
	OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName=F		Primary: RSA (2048 bits), Load Balan					

Troubleshoot

Este comando de depuración se debe recolectar en la CLI en caso de una falla en la Instalación del Certificado SSL.

• debug crypto ca 14

Preguntas Frecuentes

P. ¿Qué es un PKCS12?

R.En criptografía, PKCS12 define un formato de archivo de almacenamiento creado para almacenar muchos objetos criptográficos como un único archivo. Se suele utilizar para agrupar una clave privada con su certificado X.509 o para agrupar todos los miembros de una cadena de confianza.

P. ¿Qué es una CSR?

R.En los sistemas de infraestructura de clave pública (PKI), una solicitud de firma de certificado (también CSR o solicitud de certificación) es un mensaje enviado por un solicitante a una autoridad de registro de la infraestructura de clave pública para solicitar un Certificado de identidad digital. Normalmente contiene la clave pública para la que se puede emitir el certificado, información que se utiliza para identificar el certificado firmado (como un nombre de dominio en Asunto) y protección de la integridad (por ejemplo, una firma digital).

P. ¿Dónde está la contraseña del PKCS12?

A.Cuando los certificados y los pares de claves se exportan a un archivo PKCS12, la contraseña se proporciona en el comando export. Para importar un archivo pkcs12, el propietario del servidor de la CA o la persona que exportó el PKCS12 desde otro dispositivo debe proporcionar la contraseña.

P. ¿Cuál es la diferencia entre la raíz y la identidad?

R.En criptografía y seguridad del equipo, un certificado raíz es un certificado de clave pública que identifica una entidad emisora de certificados (CA) raíz. Los certificados raíz son autofirmados (y es posible que un certificado tenga varias rutas de confianza, por ejemplo, si el certificado fue emitido por una raíz que tenía una firma cruzada) y constituyen la base de una infraestructura de clave pública (PKI) basada en X.509. Un certificado de clave pública, también conocido como certificado digital o certificado de identidad, es un documento electrónico utilizado para probar la propiedad de una clave pública. El certificado incluye información sobre la clave, información sobre la identidad de su propietario (denominado el sujeto) y la firma digital de una entidad que ha verificado el contenido del certificado (denominada el emisor). Si la firma es válida y el software que examina el certificado confía en el emisor, puede utilizar esa clave para comunicarse de forma segura con el sujeto del certificado.

P. Instalé el certificado, ¿por qué no funciona?

R.Esto podría deberse a muchas razones, por ejemplo:

1. El certificado y el punto de confianza están configurados, pero no se han enlazado al proceso

que los utiliza. Por ejemplo, el punto de confianza que se va a utilizar no está enlazado a la interfaz externa que termina con los clientes de Anyconnect.

2. Hay instalado un archivo PKCS12, pero se producen errores debido a que falta el certificado de CA intermedio en el archivo PKCS12. Los clientes que tienen el certificado de la CA intermedia como de confianza, pero no tienen el certificado de la CA raíz como de confianza, no pueden verificar toda la cadena de certificados y notificar que el certificado de identidad del servidor no es de confianza.

3. Un certificado con atributos incorrectos puede provocar un error en la instalación o errores en el cliente. Por ejemplo, algunos atributos se codifican con un formato incorrecto. Otro motivo es que falta el nombre alternativo del sujeto (SAN) en el certificado de identidad o el nombre de dominio utilizado para acceder al servidor no está presente como SAN.

P. ¿La instalación de un nuevo certificado requiere un período de mantenimiento o provoca tiempo de inactividad?

R. La instalación de un nuevo certificado (identidad o CA) no es intrusiva y no causa tiempo de inactividad ni requiere una ventana de mantenimiento. Habilitar el uso de un nuevo certificado para un servicio existente es un cambio y requiere una ventana de solicitud de cambio/mantenimiento.

P. ¿Añadir o cambiar un certificado puede desconectar a los usuarios conectados? R.No, los usuarios conectados actualmente permanecen conectados. El certificado se utiliza en el establecimiento de conexión. Una vez que los usuarios se vuelven a conectar, se utiliza el nuevo certificado.

P. ¿Cómo puedo crear un CSR con un comodín? ¿O un nombre alternativo del sujeto (SAN)?
 R.Actualmente, el ASA/FTD no puede crear un CSR con comodín; sin embargo, este proceso se puede realizar con OpenSSL. Para generar la clave CSR e ID, puede ejecutar los comandos: openssl genrsa -out id.key 2048

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

Cuando un punto de confianza se configura con el atributo de nombre de dominio completo (FQDN), la CSR creada por ASA/FTD contiene la SAN con ese valor. La CA puede agregar más atributos SAN cuando firma el CSR, o bien el CSR puede crearse con OpenSSL

P. ¿La sustitución de certificados tiene efecto inmediatamente?

R. El nuevo certificado de identidad del servidor se utiliza solamente para las nuevas conexiones. El nuevo certificado está listo para usarse inmediatamente después del cambio, pero en realidad se usa con nuevas conexiones.

P. ¿Cómo puedo comprobar si la instalación ha funcionado? A.El comando CLI para verificar: show crypto ca cert <trustpointname>

P. ¿Cómo generar PKCS12 a partir del certificado de identidad, el certificado de CA y la clave privada?

A. PKCS12 se puede crear con OpenSSL, con el comando: openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt

P. ¿Cómo exportar un certificado para instalarlo en un nuevo ASA? A.

- Con CLI: utilice el comando: crypto ca export <trustpointname> pkcs12 <password>
- Con ASDM:
 - a. Navegue hasta Configuration > Device Management > Certificate Management > Identity Certificates y elija el Identity Certificate. Haga clic en Exportar.

File View Tools Wizards Window Mone 🍣 Configuration	w Help toring 🔚 Save 🔇 Refre	sh 🕜 Back 🕥 Forwar	d 🧿 Help			Type topic to search	Go IlIIII CISCO
Bookmarks and X	Configuration > Device Ma	nagement > Certificate M	lanagement > Identity Ce	rtificates			
o bookmark a page, right-click on a ode in the navigation tree and select Add to bookmarks".	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
🕒 Go 🏦 Delete	unstructuredName=asav unstructuredName=risav unstructuredName=FTD7	CN=ca.example.com, OU CN=ca.example.com, OU CN=KrakowCA-sub1-1	16:10:00 CEDT Apr 6 2024 15:10:00 CEST Feb 6 2024 04:44:00 CEST Dec 21 2024	SSL-Trustpoint-2023 SSL-Trustpoint SSL-Trustpoint-PKCS12	General Purpose General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits) RSA (2048 bits)	Show Details Delete
	[asa.vpn.example.com]	Not Available	Pending	SSL-Irustpoint]	Unknown		Export
							Re-Enrol
Device Management 🗗 🖗							
Management Access System Image/Configuration High Availability and Scalability		_					
Smart Call-Home	Find:	Match Case					
Cloud Web Security Service Module Settings GU Users/AAA	Certificate Expiration Alerts Send the first alert before	e: 60 (days) Set Def	ault				
Certificate Management Certificates CA Certificates	Repeat Alert Interval : Weak Crypto Configurations —	7 (days)					

b. Elija dónde exportar el archivo, especifique la contraseña de exportación y haga clic en Exportar certificado.

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 (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	 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: () () () () () () () () () () () () ()	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 an 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

El certificado exportado puede estar en el disco del equipo. Tome nota de la frase de paso en un lugar seguro, el archivo es inútil sin él.

P. Si se utilizan claves ECDSA, ¿es diferente el proceso de generación de certificados SSL? A.La única diferencia en la configuración es el paso de generación de par de claves, donde se puede generar un par de claves ECDSA en lugar de un par de claves RSA. El resto de los pasos siguen siendo los mismos.

P. ¿Siempre es necesario generar un nuevo par de claves?

R.El paso de generación del par de claves es opcional. Se puede utilizar un par de claves existente o, en el caso de PKCS12, el par de claves se importa con el certificado. Consulte la sección Select the Key Pair Name (Seleccione el nombre del par de claves) para ver el tipo de inscripción o reinscripción correspondiente.

P. ¿Es seguro generar un nuevo par de claves para un nuevo certificado de identidad?R.El proceso es seguro siempre que se utilice un nuevo nombre de par de claves. En tal caso, los pares de claves antiguos no se cambian.

P. ¿Es necesario volver a generar la clave cuando se sustituye un firewall (como RMA)?
R.El nuevo firewall por diseño no tiene pares de claves presentes en el firewall antiguo.
La copia de seguridad de la configuración en ejecución no contiene los pares de claves.
La copia de seguridad completa realizada con ASDM puede contener los pares de claves.
Los certificados de identidad se pueden exportar desde un ASA con ASDM o CLI antes de que

falle.

En el caso de un par de failover, los certificados y los pares de claves se sincronizan con una unidad standby con el comando write standby. En caso de que se reemplace un nodo de par de failover, es suficiente configurar el failover básico e insertar la configuración en el nuevo dispositivo.

En caso de que se pierda un par de claves con el dispositivo y no haya una copia de seguridad, se debe firmar un nuevo certificado con el par de claves presente en el nuevo dispositivo.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).