在ASDM管理的ASA上安裝並續訂證書

目錄

簡介 必要條件 需求 採用元件 背景資訊 使用ASDM請求並安裝新的身份證書 請求並安裝具有證書簽名請求(CSR)的新身份證書 使用ASDM產生CSR 建立具有特定名稱的信任點 (可選)建立新金鑰對 選擇金鑰對名稱 配置證書主題和完全限定域名(FQDN) 產生並儲存CSR 使用ASDM安裝PEM格式的身份證書 安裝簽署CSR的CA證書 安裝身份證書 <u>將新證書繫結到與ASDM的介面</u> 使用ASDM安裝以PKCS12格式接收的身份證書 從PKCS12檔案安裝身份證書和CA證書 將新證書繫結到與ASDM的介面 證書續訂 續訂使用ASDM的證書簽名請求(CSR)註冊的證書 使用ASDM產生CSR 建立具有特定名稱的新信任點。 (可選)建立新金鑰對 選擇金鑰對名稱 配置證書主題和完全限定域名(FQDN) 產生並儲存CSR 使用ASDM安裝PEM格式的身份證書 安裝簽署CSR的CA證書 安裝身份證書 將新證書繫結到與ASDM的介面 使用ASDM續訂用PKCS12檔案註冊的證書 從PKCS12檔案安裝更新的身份證書和CA證書 將新證書繫結到與ASDM的介面 驗證 透過 ASDM 檢視安裝的憑證 疑難排解 常見問題

簡介

本文檔介紹如何在由ASDM管理的Cisco ASA軟體上請求、安裝、信任和續訂特定型別的證書。

必要條件

需求

- 開始之前,請確認自適應安全裝置(ASA)具有正確的時鐘時間、日期和時區。對於證書身份驗證,建議使用網路時間協定(NTP)伺服器來同步ASA上的時間。檢查相關資訊以供參考。
- 若要請求使用憑證簽署請求(CSR)的憑證,必須擁有對受信任內部或第三方憑證授權單位 (CA)的存取許可權。第三方CA供應商的示例包括(但不限於)Entrust、Geotrust、 GoDaddy、Thawte和VeriSign。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- ASAv 9.18.1
- 建立PKCS12時使用OpenSSL。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

此文檔處理的證書型別為:

- 自簽名證書
- 由第三方證書頒發機構或內部CA簽名的證書

用於EAP身份驗證協定的安全套接字層(SSL)、傳輸層安全(TLS)和IKEv2 rfc7296要求 SSL/TLS/IKEv2伺服器為客戶端提供伺服器證書,以便客戶端執行伺服器身份驗證。建議使用受信 任的第三方 CA,以便向 ASA 核發 SSL 憑證做為此用途。

思科建議不要使用自我簽署憑證,因為使用者可能會不當設定瀏覽器信任惡意伺服器的憑證。 如此 亦可能造成使用者不便,必須在連線至安全閘道時回應安全性警告。

使用ASDM請求並安裝新的身份證書

可以通過兩種方式從證書頒發機構(CA)請求證書並在ASA上安裝:

- 使用憑證簽署請求(CSR)。生成金鑰對,使用CSR從CA請求身份證書,安裝從CA獲取的簽名 身份證書。
- 使用從CA獲取或從其他裝置匯出的PKCS12檔案。PKCS12檔案包含金鑰對、身份證書、

請求並安裝具有證書簽名請求(CSR)的新身份證書

在需要身份證書的裝置上建立CSR,使用在裝置上建立的金鑰對。

CSR包含:

- 證書請求資訊 請求的主題和其他屬性,金鑰對中的公鑰,
- 簽名演算法資訊,
- 證書請求資訊的數位簽章,使用金鑰對中的私鑰簽名。

CSR會傳遞至憑證授權單位(CA),以便其在PKCS#10表單中簽署它。

簽名的證書以PEM形式從CA返回。

注意:CA在簽署CSR並建立已簽名的身份證書時,可以更改信任點中定義的FQDN和使用者 名稱引數。

使用ASDM產生CSR

- 1. 建立具有特定名稱的信任點
 - a. 導航到Configuration > Device Management > Certificate Management > Identity Certificates。



- b. 按一下「Add」。
- c. 定義信任點名稱。

sued To	Issued By	Expiry Dat	e	Associated Trustpoints	^1	Usage	Public Key Type	Add
🛓 Add Identity Ce	ertificate						×	Show Deta
Trustpoint Name:	SSL-Trustpoint	_						Delete
O Import the ide	entity certificate from a file (PKCS12 format with	Certificate(s)+P	rivate Key):				Export
Decryption Pas	ssphrase:							Install
File to Import i	From:		Browse					Re-Enro
Add a new ide	entity certificate:							
Key Pair:	<default-rsa-k< td=""><td>ley> ∨</td><td>Show</td><td>New</td><td></td><td></td><td></td><td></td></default-rsa-k<>	ley> ∨	Show	New				
Certificate Sub	bject DN: CN=asavpn.exa	ample.com	Select					
Generate :	self-signed certificate							
Act as	local certificate authority ar	nd issue dynamic cer	tificates to TLS-	Proxy				
				Advanced				
Enable CA	flag in basic constraints ext	ension		Auvanceu				

- d. 按一下Add a New Identity Certificate單選按鈕。
- 2. (可選)建立新金鑰對

注意:預設情況下,使用名為Default-RSA-Key且大小為2048的RSA金鑰;但是,建議 對每個身份證書使用唯一的私有/公共金鑰對。

a. 按一下New以生成新的金鑰對。

ssued To	Issued By	Expiry Date	Associated Trust	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)+Private Key):				Export
Decryption Pas	sphrase:						Install
File to Import F	rom:	Browse.					Re-Enrol
Add a new ider	ntity certificate:						
Key Pair:	<default-rsa-< td=""><td>Key> v Show</td><td>. New</td><td></td><td></td><td></td><td></td></default-rsa-<>	Key> v Show	. New				
Certificate Sub	ject DN: CN=asavpn.ex	ample.com Select.					
Generate s	elf-signed certificate						
Act as I	ocal certificate authority a	nd issue dynamic certificates to	TLS-Proxy				
			Advanced				
Enable CA	flag in basic constraints ex	tension					

- b. 選擇Enter new Key Pair name選項,然後輸入新金鑰對的名稱。
- c. 選擇金鑰型別 RSA或ECDSA。
- d. 選擇Key Size;對於RSA,選擇General purpose for Usage。
- e. 按一下「Generate Now」。金鑰對現已建立。

sued To	Issued By	Expiry Date	Associated Trustpoints		Usage	Public Key Type	Add
🗖 Add Identity Ce	rtificate			×	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)	Show Detai
Trustpoint Name:	SSL-Trustpoin	it					Delete
🔿 Impor 🔁 🗛	ld Key Pair		×				Export
Decry			EDDCA				Install
File to	Type: ORSA	O ECDSA O	EDUSA				Re-Enrol
Add a Nan	e: 🔿 Use default ke	ey pair name					
Key Pa	Enter new ker	y pair name: SSL-Keypair					
Certifi Size	2048	\ ~	N				
Ge Usa	ge:	ose O Special	3				
10 C	Generate Now	Cancel	Help				

3. 選擇金鑰對名稱

選擇金鑰對以簽署CSR並將與新證書繫結。

Add Identity Certifie	cate							
Trustpoint Name:					×	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)	Show Detai
	SSL-Trustpoint							Delete
O Import the identity	certificate from a file (PKCS12 format with	Certificate(s)+Pi	rivate Key):				Export
Decryption Passphr	rase:							Install
File to Import From	:		Browse					Re-Enrol
Add a new identity	certificate:							
Key Pair:	SSL-Keypair	~	Show	New				
Certificate Subject	DN: CN=asavpn.exa	ample.com	Select					
Generate self-s	signed certificate							
Act as local	l certificate authority ar	nd issue dynamic ce	rtificates to TLS-P	тоху				
				Advanced				
				Auvanceu				
	in basic constraints ext	tension						
		6 1						

4. 配置證書主題和完全限定域名(FQDN)

注意: FQDN引數必須與身份證書使用的ASA介面的FQDN或IP地址匹配。此引數為身份 證書設定請求的主題備用名稱(SAN)擴展。SSL/TLS/IKEv2客戶端使用SAN擴展來驗證 證書是否與其連線的FQDN匹配。

a. 按一下「Select」。

	Issued By	Expiry Date	Associated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Certificate						×	Show Deta
Trustpoint Name:	SSL-Trustpoint						Delete
Import the identity cert	ificate from a file (PKCS	S12 format with Certificate(s)+Private Key):				Export
Decryption Passphrase:							Install
File to Import From:		Browse					Re-Enro
Add a new identity cert	ificate:						
Key Pair:	SSL-Keypair	V Show	New				
Certificate Subject DN:	CN=asavpn.example	e.com Select					
Generate self-signe	d certificate						
Act as local cert	ificate authority and iss	sue dynamic certificates to T	LS-Proxy				
			Advanced				
Enable CA flag in ba	eic constraints extensi	00	Advancean				
	are constraints external						
Enable CA flag in ba	sic constraints extension	on					

b. 在「Certificate Subject DN」視窗中,配置證書屬性 — 從下拉選單中選擇屬性,輸入值 ,然後點選Add。

sued To	Issued By	Expiry Date	Associated Trustpoints	^1 Usage	Public Key Type	Add
Add Identity Certificate	e				×	Show Detail
Trustpoint Name:	SSL-Trustpoint					Delete
O Import the identity ce	Castificata Subia	at DN		×		Export
Decryption Passphrase	Certificate Subje	ICT DIN		^		Install
File to Import From:			Attribute	Value		Re-Enroll
Add a new identity cer Key Pair:	DN Attribute to Attribute: C	be Added ommon Name (CN) 🗸	Add>>			
Certificate Subject DN	Value: as	a.vpn.example.com	Delete			
Generate self-sign						
Act as local ce						
🗌 Enable CA flag in t		ОК	Cancel Help			

ssued To	Issued By	Expiry Date	Associated Trustpoir	its ^1 Usage	Public Key Type	Add
Add Identity Certifica	te				×	Show Detail
Trustpoint Name:	SSL-Trustpoint					Delete
Import the identity ce						Export
Decryption Passphras	Certificate Subjec	t DN		~		Install
File to Import From:			Attribute	Value		Re-Enroll
Add a new identity ce	DN Attribute to h	a Addad	Common Na	me (CN) asa.vpn.exam		
Kev Pair:	Attribute: Cou	untry (C) v	Add>>			
Certificate Subject D	Value: Con	nmon Name (CN)	Delete			
Generate self-sig	Con	npany Name (O)				
	Cou Stai	ntry (C) te (St)				
	Loci Ema	ation (L) al Address (EA)				
		ОК	Cancel Help			
Enable CA flag in	t			-		
		Add Certificate	Cancel He	dp		

屬性	說明
CN	用於訪問防火牆的名稱(通常為完全限定域名,例如vpn.example.com)。
OU	組織內您所在部門的名稱
0	您的組織/公司的合法註冊名稱
思	國家/地區代碼(2個不帶標點的字母代碼)
ST	組織所在的狀態。
L	組織所在的城市。
EA	電子郵件地址

註:以上欄位值均不能超過64個字元的限制。值越長,可能會導致身份證書安裝 問題。此外,不必定義所有DN屬性。

- 新增完所有屬性後,按一下OK。
- c. 配置裝置FQDN 按一下Advanced。

ssued To	Issued By	Expiry Dat	te	Associated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Certificat	e						×	Show Detai
Trustpoint Name:	SSI -Trustopint							Delete
Import the identity cer	rtificate from a file (PK	CS12 format with (ertificate(s)+Priv	ate Kev).				Export
Decryption Passphrase	e:							Install
File to Import From:			Browse					Re-Enroll
Add a new identity certain the second sec	rtificate:							
Key Pair:	SSL-Keypair	~	Show	New				
Certificate Subject DN	: CN=asa.vpn.exar	nple.com	Select					
Generate self-sign	ed certificate							
Act as local cer	rtificate authority and	issue dynamic cert	ficates to TLS-Pro	ху				
			A	dvanced				
Enable CA flag in b	oasic constraints exter	ision						
					-			
		Add Certific	ate Ca	incel Help				

d. 在FQDN欄位中,輸入從Internet訪問裝置的完全限定域名。按一下「OK」(確定)。

ssued To	Issund Du Euripe Data Associated Trustminto A1 Hann	Public Key Type	Add
Add Identity Cer	tificate Fronilment mode parameters and SCEP challenge password are not available for self-signed certificates	×	Show Detail
Trustpoint Name:	S Certificate Parameters Enrollment Mode SCEP Challenge Password		Delete
O Import the iden	tity certifica		Export
Decryption Pass	phrase: FQDN: asavpn.example.com		Install
File to Import Fi	rom: E-mail:		Re-Enrol
Add a new iden	IP Address:		
Key Pair:	Include serial number of the device		
Certificate Subj	ect DN: C		
Generate se	elf-signed ce		
Act as k	cal certifica		
Enable CA f	lag in basic		
	OK Cascal Hala		

5. 產生並儲存CSR

a. 按一下「新增憑證」。

	Issued By	Expiry D	ate	Associated Trustpoints	^1	Usage	Public Key Type		Add
Add Identity Certifi	icate						>	<	Show Detail
Trustpoint Name:	SSL-Trustpoint								Delete
Import the identity	v certificate from a file (P	CS12 format with	Certificate(s)+Pri	vate Kev):					Export
Decryption Passoh	rase:]							Install
File to Import Fron	n:		Browse						Re-Enrol
Add a new identity	y certificate:								
Key Pair:	SSL-Keypair	~	Show	New					
Certificate Subject	t DN: CN=asa.vpn.exa	mple.com	Select						
Generate self-	signed certificate								
Act as loca	al certificate authority and	l issue dynamic ce	rtificates to TLS-Pr	oxy				-	
_			4	dvanced					
Enable CA flag) in basic constraints exte	nsion							
		6							

b. 提示隨即顯示,可將 CSR 儲存至本機電腦的檔案中。

ssued To	Issued By	Expiry Da	ate	Associated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Cer	tificate						×	Show Detail
Trustpoint Name:	SSL-Trusto	ointl						Delete
O Import the iden	tity certificate from a	file (PKCS12 format with	Certificate(s)+Priva	te Kev):				Export
Decryption Pass	sphrase:							Install
File to Import Fr	rom:	Identity Certificat	e Request		×			Re-Enroll
Add a new iden	tity certificate:	To complete the enror request (CSR) and s	ollment process, plea end it to the CA.	ase save the PKCS 10 enrollmen	t			
Key Pair:	SSL-Keypa	You will then need to	install the certificat	e that is returned from the CA	by			
Certificate Subj	ect DN: CN=asa.vr	clicking the Install bu	tton in the Identity	Certificates panel.				
Generate se	elf-signed certificate	Save CSR to File:		Brow	/se			
Act as k	ocal certificate author		OK Car	icel Help				
			Adv	vanced				
Enable CA f	lag in basic constraint	s extension						
		Add Cartific	rate Car	rel Helo				

按一下「Browse」,選擇要儲存CSR的位置,並以.txt副檔名儲存檔案。

注意:當檔案以.txt副檔名儲存時,可以使用文本編輯器(如記事本)開啟和檢視 PKCS#10請求。

c. 現在,新信任點顯示為Pending狀態。

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

安裝步驟假設CA對CSR進行簽名,並提供PEM編碼的(.pem、.cer、.crt)身份證書和CA證書捆綁包

1. 安裝簽署CSR的CA證書

0

a. 導覽至Configuration > Device Management > Certificate Management>,然後選擇CA Certificates。按一下「Add」。

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

b. 輸入Trustpoint名稱並選擇Install From File,按一下Browse按鈕,然後選擇中間證書。 或者,也可以將PEM編碼的CA證書從文本檔案貼上到文本欄位中。

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

注意:安裝簽署CSR的CA證書,並使用與身份證書相同的信任點名稱。PKI層次 結構中較高的其他CA證書可以安裝在單獨的信任點中。

c. 按一下「Install Certificate」。

ssued To	Issued By	Expiry Date	Associated Trustpoints	¹ Usage	Active	Add
lenTrust 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 Details
Trustpoint Name: SS	L-Trustpoint					Request CRI
O Install from a file:		Browse				Delete
Pasta certificata in PEN	1 formate					
g1ebnHq10LKN_005J 4noWaXH1boGGD7+5 SKVvFik12LcZEGn6b2 oK5sEPpHZ3IQuVxGiin Oj9xKnYCbPfg3p2FdH VR0OBBYEFE5Sk2sbra 9tLFV52U47em9uXaM cGqevp0MRhs3Rs/wD2	Ult:EAHSATL 2295884W58HDUD: vk0es3ft.287pEHGodLh7Gki1T mmTgaV2818wIIJTHOX48ls3u p/zmomzxl4G/tel6eyMOpjpnV 17wJh1K3prAgMBAAGjUDBOI y999tLFV52U47em9utXaMB8G AGCSqGSIb3DQEBCwUAA41 5M2wkAF4AY2HaN9qK9VCK-	sunktivalyttoriuLasupwicv125vh HrkoqL/DM9LqcOct2kcT7f xTPH8+B5QG0+d1waOsbCWk tDY)Q9HNkQdQT5LKwRsx MwGA1uBcWQFMAMBARBwHQYD A1UdIwQYMBaAFE55kZsbra9b BAQArsxHFwK3JNBwOsh5mqT HwodKMQ2y4/Libiq5ShDU7oFf6f				
z9kqaRijsx153)//tk8 0jRyjalH56BFlackU2K gW8YnHOvM08svyTX dcVcovOi/PAxnrAl3+N END CERTIFICATE	E9oAlathA/fQXSV, 45 August RddtVx/B9sfEbFhi g2jrWFN3MXWZO- E	Please wait while ASDM is deliv device	Information	e following attributes:	×	
Specify source Interfac	ce: None		Fingerprint: e9ad165c 2	573424c 6e7e0c5f b30b	4a02	
Certificate Subject DN:	CN=risavpn31		Trustpoint CA certificate	accepted.		
allow-untrusted-co	nnection					
O Use SCEP:				OK		
Specify source Interfac	ce: None	\sim		2653		
SCEP URL: http://						
Retry Period:	1	minutes				

- 2. 安裝身份證書
 - a. 選擇之前在CSR生成期間建立的身份證書。按一下「Install」。

<u>C</u>	onfiguration > Remote	Access VPN > Cer	tificate Management > Identi	ty 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	

注意:身份證書的Issued By欄位可用,Expiry Date欄位可用Pending。

b. 選擇包含從CA接收的PEM編碼身份證書的檔案,或在文本編輯器中開啟PEM編碼證書 ,然後將CA提供的身份證書複製並貼上到文本欄位中。

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

註:身份證書可以採用.pem、.cer、.crt格式進行安裝。

c. 按一下「Install Certificate」。

sued To ^1 Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
n.example.com] Not Availal	ble Pending	SSL-Trustpoint	Unknown		Show Details
Install Identity certificate		×	General Purpose	RSA (2048 bits)	
		tpoint	General Purpose	RSA (2048 bits)	Delete
lentity Certificate	🧧 Please wait	×			Export
O Install from a file:		Information	×		Install
Paste the certificate data in bis LinNBJ26XgDmVu2gHBEMVR2K Gyer3x2GML7MAHBptyMcHD TBy9Yia7boqMnamQkaQpcKAF KdNqiFbLr6VV9NTUF2DowH3 END CERTIFICATE <	Please wait while ASDM is deli device	Vering the L3	ort succeeded.		Re-Enroll

3. 將新證書繫結到與ASDM的介面

需要將ASA配置為使用新的身份證書,以便在指定介面上終止的WebVPN會話使用。

- a. 導覽至「組態 >「遠端存取 VPN」>「進階」>「SSL 設定」。
- b. 在「憑證」下方,選擇用於終止 WebVPN 作業階段的介面。在此範例中,所使用的是 外部介面。

按一下「Edit」。

c. 在「憑證」下拉式清單中,選擇新安裝的憑證。

o omoin		der michte	l.
	😨 Select SSL Certificate	×	Edit Delete
rtificates	Specify enrolled trustpoints to be used for SSL authentical OUTSIDE-direct interface. To enroll a trustpoint, go to Der Management > Identity Certificates. Interface: OUTSIDE-direct	tion and VPN load balancing on the vice Management > Certificate	a cartificate of their own
Interface OUTSIDE-direct	Primary Enrolled Certificate: SSL-Trustpoint:unstructure Load Balancing Enrolled Certificate: None	ucturedName =asavpn.exampl v Key-Type	Edit
inside inside-vlan	OK Cancel	Help	
management			
allback Certificate:	None	v	

- d. 按一下「OK」(確定)。
- e. 按一下「Apply」。

Interface	Primary Certificate	Load Balancing Certificate	Key-Type	Edit
OUTSIDE-direct	SSL-Trustpoint:unstructuredNa	ame=	Primary: RSA (2048 bits), Load Balancing:	
nside				
nside-vlan				
nanagement				
lagement				

現在,新的身份證書正在使用。

使用ASDM安裝以PKCS12格式接收的身份證書

PKCS12檔案(.p12或.pfx格式)包含身份證書、金鑰對和CA證書。它由CA建立(例如使用萬用字 元憑證),或從不同的裝置匯出。它是二進位制檔案,無法使用文本編輯器檢視。

1. 從PKCS12檔案安裝身份證書和CA證書

身份證書、CA證書和金鑰對需要捆綁到單個PKCS12檔案中。

- a. 導航到Configuration > Device Management > Certificate Management,然後選擇 Identity Certificates。
- b. 按一下「Add」。
- c. 指定信任點名稱。

Issued To	Issued By	Expiry Date	e	Associated Trustpoints	Usage	Public Key Type	Add
							Show Detai
🔁 Add Identity (Certificate			×			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 Impor	t 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 Si	ubject DN: CN=risavpn31		Select				
Generate	self-signed certificate						
Act a	s local certificate authority a	nd issue dynamic cert	tificates to TLS-P	roxy			
				Advanced			
NEnable C	A flag in basic constraints ex	tension					
- Store C							

d. 按一下「從檔案匯入身分識別憑證」單選按鈕。

ssued to	Issued By	Expiry Date		Associated T	rustpoints	Usage	F	Public Key Type		Add
										Show Detail
Add Identity Certifica	te	1 Contraction of the second se		>	<u></u>					Delete
Trustpoint Name:	SSL-Trustpoint-PKCS1	12			import ID certi	ficate file				
Import the identity ce	ertificate from a file (PKCS)	12 format with Cert	ificate(s)+Priv	ate Key):	Look in:	Document	S	~	/ 🤌 📂 🖽	•
Decryption Passphras	se:				<u>@</u> _	CSR.txt	nle com nfr			
File to Import From:		Br	owse		Recent Items	28 vpn.exan	pie.com.pix			
O Add a new identity ce	ertificate:									
Key Pair:	<default-rsa-key></default-rsa-key>	~ S	how	New	Desktop					
Certificate Subject DI	N: CN=risavpn31	S	elect							
Generate self-sig	ned certificate				Documents					
Act as local ce	ertificate authority and issu	ue dynamic certifica	tes to TLS-Pro	ху						
			A	tvanced	This PC	File name:	vpn.example.com	.pfx	Import ID	certificate file
	basic constraints extensio	n		avanceu	S	Files of type:	All Files	~	c	ancel
Enable CA flag in					L-p-					

e. 輸入用於建立 PKCS12 檔案的複雜密碼。

ssued To	Issued By	Expiry Da	te	Associated Trustpoints	Usage	Public Key Type	Add
		1					Show Details
add Identity Certifica	ate			×			Delete
Trustpoint Name:	SSL-Trustpoint-PK	CS12					Export
 Import the identity of 	ertificate from a file (PK	CS12 format with	Certificate(s)+P	rivate Key):			Install
Decryption Passphra	se: ••••						Re-Enroll
File to Import From:	C:\Users\cisco.DE	SKTOP-R2CH8G	Browse				
O Add a new identity of	ertificate:						
Key Pair:	<default-rsa-ke< td=""><td>y> ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-ke<>	y> ~	Show	New			
Certificate Subject D	N: CN=risavpn31		Select				
Generate self-sig	gned certificate						
Act as local o	ertificate authority and	issue dynamic cer	tificates to TLS-F	roxy			
				Advantation			
Enable CA flag in	basic constraints exte	nsion		Advanced			

f. 按一下「新增憑證」。

issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
Add Identity	Certificate		×			Delete
Trustpoint Name	SSL-Trustpoint-	PKCS12				Export
() Import the i	dentity certificate from a file (PKCS12 format with Certificate(s	:)+Private Key):			Install
Decryption F	assphrase: ••••		100000			Re-Enroll
File to Impor	t From: C:\Users\cisco.l	DESKTOP-R2CH8G Browse				
🔿 Add 🔤 P	lease wait		a Information			×
Key f	Please wait while ASDM device	I is delivering the command(s) to	the Created trustpo WARNING: CA (the validation-u	ints for CAs higher in the hie certificates can be used to va sage 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. ease adjust
Enable C	A flag in basic constraints ext	tension	Import PKCS 12	operation completed success	fully.	

注意:匯入帶有CA證書鏈的PKCS12時,ASDM會自動建立帶有新增了 number字尾的名稱的上游CA信任點。

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

2. 將新證書繫結到與ASDM的介面

需要將ASA配置為使用新的身份證書,以便在指定介面上終止的WebVPN會話使用。

- a. 導覽至「組態 >「遠端存取 VPN」>「進階」>「SSL 設定」。
- b. 在「憑證」下方,選取用於終止 WebVPN 作業階段的介面。在此範例中,所使用的是 外部介面。

按一下「Edit」。

c. 在「憑證」下拉式清單中,選擇新安裝的憑證。

ovman	der briede	
tificates pecify which certificates, if ar Interface	Select SSL Certificate Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface: OUTSIDE-direct Primary Enrolled Certificate: SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u Load Balancing Enrolled Certificate: None Key-Type	cate of their own.
outsube-orrect inside inside-vlan management alback Certificate:	OK Cancel Help	
orced Certification Authentica	tion Timeout: 2 minutes	

- d. 按一下「OK」(確定)。
- e. 按一下「Apply」。

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

現在,新的身份證書正在使用。

證書續訂

續訂使用ASDM的證書簽名請求(CSR)註冊的證書

CSR註冊證書的證書續訂需要建立和註冊新的信任點。它需要具有不同的名稱(例如,具有登記年 度字尾的舊名稱)。它可以使用與舊證書相同的引數和金鑰對,也可以使用不同的引數和金鑰對。

使用ASDM產生CSR

- 1. 建立具有特定名稱的新信任點。
 - a. 導航到Configuration > Device Management > Certificate Management > Identity Certificates。

File View Tools Wizards Window Help Type topic to search							Go	cisco		
Device Management 🗗 🖗	<u>C</u>	nfiguration > Device Mana	igement > Certifica	te Management > Identity Cer	tificates					
Management Access Jicensing		Issued To	~1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type		Add
System Image/Configuration High Availability and Scalability		unstructuredName=asa.examp	ole.com, L=San Jos	unstructuredName=asa.example	15:09:09 CEDT Jul 1	TP	General Purpose	RSA (2048 bits)		Show Details
Logging Smart Call-Home										Delete
- 24 Cloud Web Security 										Export
Gertificate Management										Install
-2 Identity Certificates										Re-Enroll

- b. 按一下「Add」。
- c. 定義信任點名稱。

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

- d. 按一下Add a New Identity Certificate單選按鈕。
- 2. (可選)建立新金鑰對

注意:預設情況下,使用名為Default-RSA-Key且大小為2048的RSA金鑰;但是,建議 對每個身份證書使用唯一的私有/公共金鑰對。

a. 按一下New以生成新的金鑰對。

issued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add	
unstructuredName= CN=ca.example.com, OU 15		15:10:00 CEST	Feb 6 2024	SSL-Trustpoint	General Purpose RSA (2048 bits)		Show Detail	
🔄 Add Identity C	Certificate			×			Delete	
Trustpoint Name	rustpoint Name: SSL-Trustpoint-2023					Export		
O Import the id	lentity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install	
Decryption Pa	assphrase:						Re-Enroll	
File to Import	t From:		Browse					
Add a new id	lentity certificate:							
Key Pair:	<default-rsa-ke< td=""><td>y> ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-ke<>	y> ~	Show	New				
Certificate Su	ubject DN: CN=asavpn.exam	ple.com	Select					
Generate	e self-signed certificate							
Act a	s local certificate authority and	issue dynamic cer	rtificates to TL	S-Proxy				
				Advanced				
Enable C	A flag in basic constraints exter	nsion						

- b. 選擇選項Enter new Key Pair name(輸入新金鑰對名稱),然後輸入新金鑰對的名稱。
- c. 選擇Key Type RSA或ECDSA。
- d. 選擇Key Size;對於RSA,選擇General purpose for Usage。
- e. 按一下「Generate Now」。金鑰對現已建立。

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName	e= CN=ca.example.com, O	U 15: 10:00 CEST Feb 6 2024	4 SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
Add Identit	y Certificate		×			Delete
Trustpoint Na	me: SSL-Trustpoin	-2023				Export
C 🔤 Add	Key Pair		Х кеу):			Install
Key Ty	pe: • RSA		DDSA			Re-Enroll
Name:	Use default key pair n	ame				
Circu	Enter new key pair na	ime: SSL-KeyPair-2023	ew			
Lisage:	General nurnose					
	0	0.0				
	Generate Now Ca	ancel Help	ced			
	- on may in pasic conse ainte c	A 661 (2001)				

3. 選擇金鑰對名稱

選擇金鑰對以簽署CSR並將與新證書繫結。

ssued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName=	CN=ca.example.com, OU	15:10:00 CEST	Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
🧧 Add Identity C	Certificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
O Import the ide	entity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Pa	assphrase:						Re-Enroll
File to Import	: From:		Browse				
Add a new ide	entity certificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate Su	bject DN: CN=asavpn.exam	ple.com	Select				
Generate	self-signed certificate			-			
Act as	s local certificate aut prity and	issue dynamic ce	rtificates to TLS	S-Proxy			
			1	Advanced			
Enable CA	A flag in basic constraints exter	ision	l				
_							
	Add Castificate Co	and a large state of the second state of the s	Hala				

4. 配置證書主題和完全限定域名(FQDN)

注意: FQDN引數必須與證書使用的ASA介面的FQDN或IP地址匹配。此引數設定證書的 使用者替代名稱(SAN)。SSL/TLS/IKEv2客戶端使用SAN欄位來驗證證書是否與其所連 線的FQDN匹配。

注意:CA在簽署CSR並建立已簽名的身份證書時,可以更改信任點中定義的FQDN和使 用者名稱引數。

a. 按一下「Select」。

sued to Issue	d 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 Certificat	e			×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
O Import the identity ce	rtificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Passphrase	2:						Re-Enroll
File to Import From:			Browse				
Add a new identity certain the second sec	rtificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate Subject DN	: CN=asavpn.exam	ple.com	Select				
Generate self-sign	ed certificate						
Act as local cer	rtificate authority and	issue dynamic cer	tificates to TL	S-Proxy			
				Advanced			
	anis constraints outer	ncion					

b. 在「Certificate Subject DN」視窗中,配置「certificate attributes - select attribute from」下拉選單,輸入值,然後按一下Add。

sued To Issued By Expiry		Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName=.	tructuredName= CN=ca.example.com, OU 15:10:00 CEST Feb 6 2024		SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Deta
🔁 Add Identity 🤇	ertificate		×			Delete
Trustpoint Name	SSL-Trustpoint-2	023	1			Export
ertificate Subject	DN		×			Install
		(10)				Re-Enrol
		Attribute	Value			
DN Attribute to be	Added	Common Name (Ch Company Name (Ch	asavpn.example.com example inc			
Value: US	τγ (C)	kad >>				
value, USI		Delete				
	OK	Cancel Help				
Enable C	A flag in basic constraints exte	nsion				

屬性	說明
CN	用於訪問防火牆的名稱(通常為完全限定域名,例如 vpn.example.com)。
OU	組織內您所在部門的名稱
0	您的組織/公司的合法註冊名稱
思	國家/地區代碼(2個不帶標點的字母代碼)

屬性	說明
ST	組織所在的狀態。
L	組織所在的城市。
EA	電子郵件地址

註:前面的所有欄位都不能超過64個字元的限制。值越長,可能會導致身份證書 安裝問題。此外,不必定義所有DN屬性。

新增完所有屬性後,按一下OK。

c. 要配置裝置FQDN,請按一下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	y Certificate		×			Delete
Trustpoint Nan	ne: SSL-Trustpoint-20	023				Export
O Import the	identity certificate from a file (Pl	(CS12 format with Certificate(s)	+Private Key):			Install
Decryption	Passphrase:					Re-Enroll
File to Imp	ort From:	Browse				
Add a new	identity certificate:					
Key Pair:	SSL-KeyPair-202	3 ~ Show	New			
Certificate	Subject DN: /pn.example.com	,O=example inc Select				
Genera	ate self-signed certificate					
Act	t as local certificate authority and	l issue dynamic certificates to T	S-Proxy			
Enable	CA flag in basic constraints exte	nsion	Auvanceu			
			_			

d. 在FQDN欄位中,輸入從Internet訪問裝置的完全限定域名。按一下「OK」(確定)。

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
	Ontions	NOLI LISU10-00 CEST SALIS 1	X	General Purpose	RSA (2048 bits)	Show Detail
Auvanceu	options		~			Delete
Certificate Par	ameters and SCEP cha	SCEP Challenge Password	e for self-signed certificates.			Export
	En onnert Hou	Seer challenge rassword				Install
FQDN:	asavpn.example.com					Re-Enrol
E-mail:						
IP Address:						
Indude s	erial number of the device					
		G₂.				

5. 產生並儲存CSR

a. 按一下「新增憑證」。

structuredName= CN				Associated Int	ustpoints	Usage	Public Key Type	Auu
	N=ca.example.com, OU	15:10:00 CEST F	Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Details
🔄 Add Identity Certifi	icate				×			Delete
Trustpoint Name:	SSL-Trustpoint-202	23						Export
O Import the identity	y certificate from a file (PK	CS12 format with	Certificate(s)+	Private Key):				Install
Decryption Passph	arase:							Re-Enroll
File to Import From	n:		Browse	í -				
Add a new identity	y certificate:							
Key Pair:	SSL-KeyPair-2023	~	Show	New]			
Certificate Subject	DN: /pn.example.com,	O=example inc	Select					
Generate self-	signed certificate							
Act as loca	l certificate authority and i	issue dynamic cer	tificates to TLS	Proxy				
			r					
_			L	Advanced				
Enable CA flag	in basic constraints exten	sioni						

b. 提示隨即顯示,可將 CSR 儲存至本機電腦的檔案中。

	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	SSL-Trustpoint-20	023				Export
O Import the id	dentity certificate from a file (Pl	KCS12 format with Certificate(s)+Private Key):			Install
E Ident	tity Certificate Request		×			Re-Enroll
K You will dicking C Save C	I then need to install the certifit the Install button in the Identi SR to File: C:\Users\cisco.DES	cate that is returned from the C ity Certificates panel. SKTOP-R2CH8G5'Docun Br Cancel Help	A by			
Contraction of the second			11			
K You will dicking C Save C	I then need to install the certific the Install button in the Identi ISR to File: C:\Users\cisco.DES	cate that is returned from the C ity Certificates panel. SKTOP-R2CH8G5'/Docun Br Cancel Help	A by			

按一下「Browse」。 選擇要儲存CSR的位置,並使用.txt副檔名儲存檔案。

注意:當檔案以.txt副檔名儲存時,可以使用文本編輯器(如記事本)開啟和檢視 PKCS#10請求。

c. 現在,新信任點顯示為Pending狀態。

sued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
structuredName= CN=ca.example.com,	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	5 2024 SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
avpn.example.com]	Not Available	Pending	SSL-Trustpoint-2023	Unknown		Show Detail
						Delete
						Export
						Install
						Re-Enroll

使用ASDM安裝PEM格式的身份證書

安裝步驟假設CA對CSR進行簽名,並提供PEM編碼(.pem、.cer、.crt)的新身份證書和CA證書捆綁 包。

1. 安裝簽署CSR的CA證書

簽名身份證書的CA證書可以安裝在為身份證書建立的信任點中。如果身份證書是由中間CA簽 名的,則此CA證書可以安裝在身份證書信任點中。層次結構中上游的所有CA證書可以安裝在 單獨的CA信任點中。

a. 導覽至Configuration > Device Management > Certificate Management>,然後選擇CA Certificates。按一下「Add」。

sued To Issued By	∧ ¹ Expiry Date	Associated Trustpoints	Usage	Active	Add
.example.com CN=ca.exam	nple.com, OU=I 15:10:00 CEST F	eb 6 2030 SSL-Trustpoint	General Purpose	Yes	Edit
uoVadis Root CA 2 CN=QuoVad	lis Root CA 2, 19:23:33 CEST N	Nov 24 2031 _SmartCallHome_ServerC	CA2 General Purpose	No	Curt
enTrust Commercial Root CN=IdenTru	ist Commercial 19:12:23 CEST	Jan 16 2034 _SmartCallHome_ServerC	CA General Purpose	No	Show Details

b. 輸入Trustpoint名稱並選擇Install From File,按一下Browse按鈕,然後選擇 intermediate證書。或者,也可以將PEM編碼的CA證書從文本檔案貼上到文本欄位中。

ssued To	Issued By ^1	Expiry Date	Associated Trustpoints	Usage	Active		Add
a.example.com	CN=ca.example.com, OU=l	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes		Edit
install Certificate						×	Show Detai
Trustpoint Name:	SSL-Trustpoint-2023]				1	Request CR
Install from a file:		Browse					Delete
O Prote service states	DEM formati						

注意:如果身份證書由中間CA證書簽名,請安裝信任點名稱與身份證書信任點名 稱相同的中間證書。

c. 按一下「Install Certificate」。

ssued To	Issued By	∧ ¹ Expi	ry Date	Associated Trustpoints	Usage	Active	Ad
.example.com	CN=ca.example.com, O	U=l 15:10	0:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes	Edi
Install Certificate							X Show D
Trustpoint Name:	SL-Trustpoint-2023						Reques
O Install from a file:			Browse				Dele
Paste certificate in PE	EM format:						
<pre>howakH loodoD/+ skv/Fit21z2EGn6b oK5sEPpH23(Qu/xGi Oj9xk/r2bFg3p2d VROOBBYEFE55k2sbr 9tLFV52U47em9xXal cGqey0Mrks?Bs/vb/ 25kqaRijsx153)V/Tk OjRyjal#56BFladkv2 gW8YnHOvM08svyT dc/cov0/PAxmrAl+END CERTIFICA Use EST: Specify source Interfi EST URL: https:// Certificate Subject DV allow-untrusted-co Use SCEP: Specify source Interfi SCEP URL: http://</pre>	svkuesJL 29 /pen/sodin // zumlgav/28 /ewiUnHOX44 irp/zmorzid4G/tel6eyMOg H7W jh IX59-AgM8AsQU a9b9tLFV52U47em9uXaM 4A0GCSqGSID3OQEBCwU 2950/24A74/25gN9gK 8E90A1atnA/fQ7K6V +h7 KKddtVx1985fEbFNN80c KSUJf0UCdmAY +lG0gqh Ng2r/VHN3MXWZO453C Ferrer ace: None 	ala 11 4K3qL/ II SJAXTPHS I Jjpo/tb/YQ9 JBOMAwGA B8GA 1UdIw AA4IBAOArs Inform	UM964ge20ct2kCl // BSQG0+d1wa0sbCVlk HNKgdQTSLKwRsX LUdewQFMMABR6wHQ QYMBaAFE55kZsbra9b XlfwK3llNBwCsYhSmdT ation INFO: Certificate h Fingerprint: e9ad16 Trustpoint CA certif	YD as the following attributes: 55c 2673424c 6e7e0c5f b30b4a02 ficate accepted.	×		• •
Red y Period.	1		minutes				

在本例中,新證書使用與舊證書相同的CA證書簽名。同一個CA證書現在與兩個信任點 關聯。

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

- 2. 安裝身份證書
 - a. 選擇之前通過生成CSR建立的身份證書。按一下「Install」。

onfiguration > Device	Management > Certification	ate Management > Identit	<u>y Certificates</u>				
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
[asavpritexample:com]	NOT AVAILABLE	ir chung	35L-1105(point-2023		Orishown		Delete
							Export
							Install
							Re-Enrol

注意:身份證書的Issued By欄位可用,Expiry Date欄位可用Pending。

b. 選擇包含從CA接收的PEM編碼身份證書的檔案,或在文本編輯器中開啟PEM編碼證書 ,然後將CA提供的身份證書複製並貼上到文本欄位中。

sued to	Issued By	Expiry Date	Associated Trustpoints	~ 1	Usage	Public Key Type	Add
structuredName=	. CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Deta
savpn.example.com] Not Available	Pending	SSL-Trustpoint-2023		Unknown		
							Delete
							Export
lnstall Identity	certificate		×				Install
dentity Certificate							Re-Enrol
	e						
 Install from a 	nie:		browse				
O Paste the cer	tificate data in base-64 format	:					

註:身份證書可以採用.pem、.cer、.crt格式進行安裝。

c. 按一下「Install Certificate」。

ssued to	Issued By	Expiry Date	Associated Trustpoints	~ 1	Usage	Public Key Type	Add
nstructuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detail
isavpn.example.com	j Not Available	Pending	SSL-Trustpoint-2023		Unknown		Delete
							Export
Install Identity of	certificate		×				Install
dentity Certificate							Re-Enroll
	e wait		~				
Pa	🔄 Informa	ition	×				
H	Please wait wł		1				
ð 🄁		Certificate import succeede	d.				
e W			1				

安裝後,存在舊身份證書和新身份證書。

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

3. 將新證書繫結到與ASDM的介面

需要將ASA配置為使用新的身份證書,以便在指定介面上終止的WebVPN會話使用。

- a. 導覽至「組態 >「遠端存取 VPN」>「進階」>「SSL 設定」。
- b. 在「憑證」下方,選擇用於終止 WebVPN 作業階段的介面。在此範例中,所使用的是 外部介面。

按一下「Edit」。

c. 在「憑證」下拉式清單中,選擇新安裝的憑證。

					Edit Delete
[select SSL Certificate		×		
ertificates	Specify enrolled trustpoints to be us OUTSIDE-direct interface. To enroll Management > Identity Certificates	ied for SSL authentication and VPN load balancing on the a trustpoint, go to Device Management > Certificate			
Specify which certificates, if an	Interface:	OUTSIDE-direct	ces not as	sociated with a certificate of their own.	
Interface	Primary Enrolled Certificate:	SSL-Trustpoint-2023:unstructuredName=asavpn.exampl	Key-T	ype	Edit
OUTSIDE-direct	Load Balancing Enrolled Certificate:	None	Primar	y: RSA (2048 bits), Load Balancing: n	
inside	OK	Canad	1.0	1	
inside-vlan	- OK	Cancel Help	1.00		
management			_		

- d. 按一下「OK」(確定)。
- e. 按一下「Apply」。現在,新的身份證書正在使用。

		1		
				Edit
				Delete
icates	nv. should be used for SSL authentication or	each interface. The fallback certificate will be u	sed on interfaces not associated with a certificate of their own.	
icates	ny, should be used for SSL authentication or	n each interface. The fallback certificate will be u	sed on interfaces not associated with a certificate of their own.	
icates cofy which certificates, if ar Interface	ny, should be used for SSL authentication or Primary Certificate	n each interface. The fallback certificate will be u Load Balancing Certificate	sed on interfaces not associated with a certificate of their own. Key-Type	Edit
icates cify which certificates, if ar Interface OUTSIDE-direct	ny, should be used for SSL authentication or Primary Certificate SSL-Trustpoint-2023:unstructu	n each interface. The fallback certificate will be u Load Balancing Certificate (e	sed on interfaces not associated with a certificate of their own. Key-Type Primary: RSA (4096 bits), Load Balancing: n	Edit
icates cify which certificates, if ar Interface OUTSIDE-drect nside	ny, should be used for SSL authentication or Primary Certificate SSL-Trustpoint-2023:unstructu	n each interface. The fallback certificate will be u Load Balancing Certificate (c	sed on interfaces not associated with a certificate of their own. Key-Type Primary: RSA (4096 bits), Load Balancing: n	Edit
icates	ny, should be used for SSL authentication or Primary Certificate SSL-Trustpoint-2023/unstructu	n each interface. The fallback certificate will be u: Load Balancing Certificate (e	sed on interfaces not associated with a certificate of their own. Key-Type Primary: RSA (4096 bits), Load Balancing: n	Edit

使用ASDM續訂用PKCS12檔案註冊的證書

PKCS12註冊證書的證書續訂需要建立和註冊新的信任點。它需要具有不同的名稱(例如,具有登 記年度字尾的舊名稱)。

PKCS12檔案(.p12或.pfx格式)包含身份證書、金鑰對和CA證書。例如,遇到萬用字元證書,它 由CA建立,或者從其他裝置匯出。它是二進位制檔案,不能使用文本編輯器檢視。

1. 從PKCS12檔案安裝更新的身份證書和CA證書

身份證書、CA證書和金鑰對需要捆綁到單個PKCS12檔案中。

- a. 導覽至Configuration > Device Management > Certificate Management,然後選擇 Identity Certificates。
- b. 按一下「Add」。
- c. 指定新的Trustpoint名稱。

Issued To	Issued By	Expiry Da	ate	Associated Trustpoints	Usage	Public Key Type	Add
							Show Detail
🔁 Add Identity C	ertificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-	PKCS12					Export
Import the ide	entity certificate from a file (PKCS12 format wit	h Certificate(s)+P	rivate Key):			Install
Decryption Pa	assphrase:						Re-Enroll
File to Import	From:		Browse				
O Add a new ide	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	ertificates to TLS-f	Proxy			
				Adversed			
The Frankland	0			Advanced			
	A flag in basic constraints ex	tension					

d. 按一下「從檔案匯入身分識別憑證」單選按鈕。

ssued to	Issued By	Expiry Date		Associated T	rustpoints	Usage	F	Public Key Type		Add
										Show Detail
Add Identity Certifica	te	1 Alexandre		>	<u></u>					Delete
Trustpoint Name:	SSL-Trustpoint-PKCS1	12			import ID certi	ficate file				
Import the identity ce	ertificate from a file (PKCS)	12 format with Cert	ificate(s)+Priv	ate Key):	Look in:	Document	S	~	/ 🤌 📂 🖽	•
Decryption Passphras	se:				<u>@</u> _	CSR.txt	nle com nfr			
File to Import From:		Br	owse		Recent Items	28 vpn.exan	pie.com.pix			
O Add a new identity ce	ertificate:									
Key Pair:	<default-rsa-key></default-rsa-key>	~ S	how	New	Desktop					
Certificate Subject DI	N: CN=risavpn31	S	elect							
Generate self-sig	ned certificate				Documents					
Act as local ce	ertificate authority and issu	ue dynamic certifica	tes to TLS-Pro	ху						
			A	tvanced	This PC	File name:	vpn.example.com	.pfx	Import ID	certificate file
	basic constraints extensio	n		avanocu	S	Files of type:	All Files	~	c	ancel
Enable CA flag in					L-p-					

e. 輸入用於建立 PKCS12 檔案的複雜密碼。

ssued To	Issued By	Expiry Da	te	Associated Trustpoints	Usage	Public Key Type	Add
		1					Show Details
add Identity Certifica	ate			×			Delete
Trustpoint Name:	SSL-Trustpoint-PK	CS12					Export
 Import the identity of 	ertificate from a file (PK	CS12 format with	Certificate(s)+P	rivate Key):			Install
Decryption Passphra	se: ••••						Re-Enroll
File to Import From:	C:\Users\cisco.DE	SKTOP-R2CH8G	Browse				
O Add a new identity of	ertificate:						
Key Pair:	<default-rsa-ke< td=""><td>y> ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-ke<>	y> ~	Show	New			
Certificate Subject D	N: CN=risavpn31		Select				
Generate self-sig	gned certificate						
Act as local o	ertificate authority and	issue dynamic cer	tificates to TLS-F	roxy			
				Advantation			
Enable CA flag in	basic constraints exte	nsion		Advanced			

f. 按一下「新增憑證」。

issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
🔁 Add Identity (Certificate		×			Delete
Trustpoint Name	SSL-Trustpoint-	PKCS12				Export
 Import the id 	entity certificate from a file ((PKCS12 format with Certificate(s)+Private Key):			Install
Decryption P	assphrase: ••••					Re-Enroll
File to Impor	From: C:\Users\cisco.	DESKTOP-R2CH8G Browse.				
🔿 Add 📮 P	ease wait		Information			×
Key F Certi	Please wait while ASDM device	I is delivering the command(s) to	the Created trustpoi WARNING: CA o the validation-us	nts for CAs higher in the hie ertificates can be used to va age 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 ex	tension	Import PKCS 12 o	peration completed success	sfully.	

注意: 匯入具有CAs證書鏈的PKCS12時, ASDM會自動建立具有新增了 — number字尾的名稱的上游CAs信任點。

ľ		1,05		0, 10 IH	
	Configuration	Domete	Contificate M	ana annant a	CA Contification

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. 將新證書繫結到與ASDM的介面

需要將ASA配置為使用新的身份證書,以便在指定介面上終止的WebVPN會話使用。

- a. 導覽至「組態 >「遠端存取 VPN」>「進階」>「SSL 設定」。
- b. 在「憑證」下方,選擇用於終止 WebVPN 作業階段的介面。在此範例中,所使用的是 外部介面。

按一下「Edit」。

c. 在「憑證」下拉式清單中,選擇新安裝的憑證。

Pomoin	Contractor.	
[Select SSL Certificate	Edit Delete
tificates pecify which certificates, if ar Interface OUTSIDE-direct inside inside-vlan management	Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate Interface: OUTSIDE-direct Interface: OUTSIDE-direct es not associated with a certificate Primary Enrolled Certificate: SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u v Load Balancing Enrolled Certificate:	of their own.
allback Certificate:	tion Timeout:	

- d. 按一下「OK」(確定)。
- e. 按一下「Apply」。

c	ertificates Specify 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	

現在,新的身份證書正在使用。

驗證

使用以下步驟驗證第三方廠商憑證的成功安裝以及用於SSL VPN連線。

透過 ASDM 檢視安裝的憑證

- 1. 導覽至「組態」>「遠端存取 VPN」>「 Certificate Management」,然後選擇「身分識別憑 證」。
- 2. 可能會顯示第三方供應商頒發的身份證書。

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

疑難排解

如果SSL證書安裝失敗,則會在CLI上收集此debug命令。

• debug crypto ca 14

常見問題

問。什麼是PKCS12?

A.在加密中,PKCS12定義了一種存檔檔案格式,建立該格式是為了將許多加密對象儲存為一個檔 案。它通常用於將私鑰與其X.509證書捆綁在一起,或者用於捆綁信任鏈中的所有成員。

問:什麼是CSR?

A.在公鑰基礎設施(PKI)系統中,證書簽名請求(也稱為CSR或證書請求)是從申請人傳送到公鑰基 礎結構的註冊機構以申請數位身份證書的消息。它通常包含可為其頒發證書的公鑰、用於標識已簽 名證書的資訊(如主題中的域名)以及完整性保護(如數位簽章)。

問:PKCS12的口令在哪裡?

A.將證書和金鑰對匯出到PKCS12檔案時,在export命令中給出口令。對於匯入pkcs12檔案,密碼 需要由所有者從另一裝置匯出PKCS12的CA伺服器或人員提供。

根與身份之間有什麼區別?

答:在密碼學和電腦保安領域,根證書是用來標識根證書頒發機構(CA)的公鑰證書。根證書是自簽 名的(並且證書可以具有多個信任路徑,例如證書是否由交叉簽名的根頒發),並構成基於 X.509的公鑰基礎架構(PKI)的基礎。公鑰證書也稱為數位證書或身份證書,是一種用於證明公鑰所 有權的電子文檔。證書包括有關金鑰的資訊、有關其所有者(稱為主題)的標識的資訊以及驗證證 書內容的實體(稱為頒發者)的數位簽章。如果簽名有效,並且檢查證書的軟體信任頒發者,那麼 它就可以使用該金鑰與證書的使用者安全地通訊。

問:我安裝了證書,為什麼它無法工作? A.這可能是由於多種原因,例如:

1.已配置證書和信任點,但尚未將其繫結到應使用該證書和信任點的進程。 例如,要使用的信任點 不會繫結到終止Anyconnect客戶端的外部介面。

2.已安裝PKCS12檔案,但由於PKCS12檔案中缺少中間CA證書而出現錯誤。如果客戶端的中間 CA證書為受信任,但根的CA證書不是受信任,則無法驗證整個證書鏈並報告伺服器身份證書為不 受信任。

3.使用不正確的屬性填充的證書可能會導致安裝失敗或客戶端錯誤。例如,某些屬性可能使用錯誤 的格式進行編碼。另一個原因是標識證書缺少主體備用名稱(SAN),或者用於訪問伺服器的域名沒 有作為SAN存在。

問:安裝新證書是否需要維護視窗或導致停機時間?

A.安裝新證書(身份或CA)不會帶來干擾,不應導致停機或要求維護視窗。要啟用新證書用於已存 在的服務,需要更改並且可能需要更改請求/維護視窗。

問:添加或更改證書可以斷開連線的使用者嗎?

答:不,當前連線的使用者保持連線。該證書在建立連線時使用。使用者重新連線後,會使用新憑 證。

問:如何使用萬用字元建立CSR?還是主題備用名稱(SAN)?

A.目前,ASA/FTD無法使用萬用字元建立CSR;但是,此過程可以使用OpenSSL完成。若要產生 CSR和ID金鑰,您可以執行以下命令: openssl genrsa -out id.key 2048

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

使用完全限定域名(FQDN)屬性配置信任點時,由ASA/FTD建立的CSR包含具有該值的SAN。CA在 簽署CSR時可以新增更多SAN屬性,或可以使用OpenSSL建立CSR

問:證書更換是否立即生效?

A.新伺服器身份證書僅用於新連線。新證書可在更改後立即使用,但實際上用於新連線。

問:如何檢查安裝是否成功?

A.要驗證的CLI命令: show crypto ca cert <trustpointname>

問。如何從身份證書、CA證書和私鑰生成PKCS12? A.PKCS12可以使用OpenSSL使用以下命令建立: openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt

問:如何匯出證書以在新ASA中安裝該證書? A.

- 使用CLI:使用命令:crypto ca export <trustpointname> pkcs12 <password>
- 使用ASDM:
 - a. 導航到Configuration > Device Management > Certificate Management > Identity Certificates,然後選擇Identity Certificate。按一下「Export」。

File View Tools Wizards Windo	ow Help					Type topic to search	Go	ahaha
Home 🎭 Configuration 🔯 Mor	itoring 🔚 Save 🔇 Refre	esh 🔇 Back 🔘 Forwar	rd 🦻 Help					cisco
Bookmarks 🗗 म 兴	Configuration > Device Ma	nagement > Certificate I	lanagement > Identity Ce	rtificates				
o bookmark a page, right-dick on a ode in the navigation tree and select	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type		Add
Go Trelete	unstructuredName=asav unstructuredName=risav	CN=ca.example.com, OU CN=ca.example.com, OU CN=KrakewCA.crb1.1	16:10:00 CEDT Apr 6 2024 15:10:00 CEST Feb 6 2024	SSL-Trustpoint-2023 SSL-Trustpoint SSL-Trustpoint	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)	[Show Details
	[asa.vpn.example.com]	Not Available	Pending	SSL-Trustpoint	Unknown	K5A (2046 DIS)		Export
								Instal
								Re-Enroll
Device Management 리 무								
Management Access Josephine System Image/Configuration								
Grant Call-Home	Find:	🔘 🔘 🗌 Match Case						
Cloud Web Security Service Module Settings Users/AAA	Certificate Expiration Alerts Send the first alert befor	re: 60 (days) Set Def	ault					
Certificate Management	Repeat Alert Interval :	7 (days)						

b. 選擇匯出檔案的位置,指定匯出密碼,然後按一下Export Certificate。

sued To	Issued By	Expiry Date	Associated Trustpoints	Usag	ge -	Public Key Type	Add
structuredName=asav	CN=ca.example.com, OU	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023		General Purpose	RSA (4096 bits)	Show Detail
structuredName=risav	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detail
structuredName=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
							Install
							De Coul
nd:	💿 🙆 🗌 Match Case						
nd:	💿 💿 🗌 Match Case						
nd: tificate Expiration Alerts – Send the first alert before	Case Go (days) Set Defa	sult					
nd: tificate Expiration Alerts - Send the first alert before Repeat Alert Interval :	 Match Case 60 (days) Set Defn 7 (days) 	sult					
nd: tificate Expiration Alerts – Send the first alert before Repeat Alert Interval : Crypto Configurations –	 Match Case 60 (days) Set Defa 7 (days) 7 Export certificate 	sult		×			
nd: tificate Expiration Alerts – Send the first alert before Repeat Alert Interval : Crypto Configurations — Permit Weak key sizes and	 Match Case Match Case (days) Set Defi (days) Export certificate Ha Export to File: 	sult C:\Users\visco.DESKTOP4	R2CH8G5\Documents\ce Brow	×	-		
nd: tificate Expiration Alerts – Send the first alert before Repeat Alert Interval : Crypto Configurations – Permit Weak key sizes and CA Enrollment	 Match Case Match Case Gays) Set Defa (days) Export certificate Export to File: Certificate Format: 	sult C:\Users\cisco.DESKTOP4	R2CH8G5\Documents\ce Brow	×			
nd: tificate Expiration Alerts – Send the first alert before Repeat Alert Interval : Crypto Configurations – Permit Weak key sizes and CA Enrollment – your Cisco ASA security a	Match Case Match Case Match Case Go (days) Set Defa 7 (days) Export certificate Certificate Format: Optic	sult C:\Users\cisco.DESKTOP4 @ PKCS12 Format (Certif	R2CH8G5\Documents\ce Brown	×	stomers a special	promotional price for certificat	tes and trial certificates
tificate Expiration Alerts – Send the first alert before Repeat Alert Interval : Crypto Configurations – Permit Weak key sizes and CA Enrollment – your Cisco ASA security a ing.	Match Case Match Case Match Case Go (days) Set Defa 7 (days) Export certificate tha Export to File: Certificate Format: ppliz	C:\Users\visco.DESKTOP4	R2CH8G5\Documents\ce Brow icate(s) + Private Key)	× se	stomers a special	promotional price for certifical	tes and trial certificates
id: bificate Expiration Alerts Send the first alert before Repeat Alert Interval : Crypto Configurations Permit Weak key sizes and CA Enrollment	Match Case Match Case Match Case Go (days) Set Defi (days) Export certificate Ha Export to File: Certificate Format: ppla	ault C:\Users\cisco.DESKTOP+ PKCS 12 Format (Certificat PEM Format (Certificat	R2CH8G5\Documents\ce Brow icate(s) + Private Key) e Only)	× se	stomers a special	promotional price for certifical	tes and trial certificates t
id: bificate Expiration Alerts Send the first alert before Repeat Alert Interval : Crypto Configurations Permit Weak key sizes and CA Enrollment	Match Case Match Case Match Case Go (days) Set Defa (days) Export certificate Ha Export to File: Certificate Format: ppla fica Configuration Encryption	C:\Users\cisco.DESKTOP+ PKCS12 Format (Certif PEM Format (Certificat an Passohrase	R2CH8G5\Documents\ce Brow icate(s) + Private Key) e Only)	se	stomers a special	promotional price for certifical	tes and trial certificates
nd: tificate Expiration Alerts Send the first alert before Repeat Alert Interval : Crypto Configurations Permit Weak key sizes and CA Enrollment	Match Case Match Case Go (days) Set Defi (days) Export certificate Ha Export to File: Certificate Format: pple fice Configuration Encryptio Encryption Paseobra	ault C:\Users\cisco.DESKTOP4 PKCS12 Format (Certificat PEM Format (Certificat on Passphrase	R2CH8G5\Documents\ce Brow icate(s) + Private Key) e Only)	× se	stomers a special	promotional price for certificat	tes and trial certificates t
Id: thicate Expiration Alerts – Send the first alert before Repeat Alert Interval : Crypto Configurations — Permit Weak key sizes and CA Enrollment your Cisco ASA security a ing. Ig a previously saved cert Identity Certificate Wizan	Match Case Match Case Match Case Match Case Match Case Certificate Certificate Format: pplic Export to File: Certificate Format: pplic Ecryption Passphra	ault C:\Users\cisco.DESKTOP4 (a) PKCS12 Format (Certificat PEM Format (Certificat an Passphrase se:	R2CH8G5\Documents\ce Brow icate(s) + Private Key) e Only)	× se	stomers a special	promotional price for certifical	tes and trial certificates t

匯出的證書可以在電腦磁碟上。請記下安全位置的密碼,否則檔案將無用。

問:如果使用ECDSA金鑰,則SSL證書生成過程是否不同?

A.配置的唯一區別是金鑰對生成步驟,在該步驟中可生成ECDSA金鑰對,而不是RSA金鑰對。其他 步驟皆維持不變。

問:是否總是需要生成新的金鑰對?

答:金鑰對生成步驟是可選的。可以使用現有的金鑰對,或者,在PKCS12的情況下,金鑰對隨證 書匯入。請參閱選擇金鑰對名稱部分,瞭解相應的註冊/重新註冊型別。

問:為新的身份證書生成新的金鑰對是否安全?

A.只要使用新的金鑰對名稱,該過程就是安全的。在這種情況下,舊金鑰對不會更改。

問:在更換防火牆(如RMA)時,是否需要再次生成金鑰?

A.新防火牆的設計沒有在舊防火牆上提供金鑰對。

運行配置的備份不包含金鑰對。

使用ASDM完成的完全備份可以包含金鑰對。

可以在身份證書失敗之前通過ASDM或CLI從ASA中匯出身份證書。

在故障轉移對的情況下,使用write standby命令將證書和金鑰對同步到備用裝置。如果替換了故障 轉移對中的一個節點,則只需配置基本故障轉移並將配置推送到新裝置即可。

如果裝置丟失了金鑰對,並且沒有備份,則需要使用新裝置上存在的金鑰對來簽署新證書。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。