# 在ASDM管理的ASA上安装并续订证书

### 目录

简介 先决条件 要求 使用的组件 背景<u>信息</u> 使用ASDM请求并安装新的身份证书 请求并安装具有证书签名请求(CSR)的新身份证书 使用ASDM生成CSR 创建具有特定名称的信任点 (可选)创建新密钥对 选择密钥对名称 配置证书主题和完全限定域名(FQDN) 生成并保存CSR 使用ASDM安装PEM格式的身份证书 安装签署CSR的CA证书 安装身份证书 使用ASDM将新证书绑定到接口 使用ASDM安装以PKCS12格式收到的身份证书 从PKCS12文件安装身份和CA证书 使用ASDM将新证书绑定到接口 证书续订 使用ASDM续订使用证书签名请求(CSR)注册的证书 使用ASDM生成CSR 创建具有特定名称的新信任点。 (可选)创建新密钥对 选择密钥对名称 配置证书主题和完全限定域名(FQDN) 生成并保存CSR 使用ASDM安装PEM格式的身份证书 安装签署CSR的CA证书 安装身份证书 使用ASDM将新证书绑定到接口 使用ASDM续订使用PKCS12文件注册的证书 从PKCS12文件安装更新的身份证书和CA证书 使用ASDM将新证书绑定到接口 验证 通过 ASDM 查看已安装的证书 故障排除 常见问题解答

## 简介

本文档介绍如何在通过ASDM管理的Cisco ASA软件上请求、安装、信任和续订特定类型的证书。

### 先决条件

#### 要求

- 开始之前,请确认自适应安全设备(ASA)具有正确的时钟时间、日期和时区。对于证书身份验证,建议使用网络时间协议(NTP)服务器同步ASA上的时间。检查相关信息以供参考。
- 要请求使用证书签名请求(CSR)的证书,需要具有访问受信任的内部或第三方证书颁发机构 (CA)的权限。第三方CA供应商的示例包括(但不限于)Entrust、Geotrust、GoDaddy、 Thawte和VeriSign。

#### 使用的组件

本文档中的信息基于以下软件和硬件版本:

- ASAv 9.18.1
- 创建PKCS12时,使用OpenSSL。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

### 背景信息

此文档处理的证书类型为:

- 自签名证书
- 由第三方证书颁发机构或内部CA签名的证书

安全套接字层(SSL)、传输层安全(TLS)和用于EAP身份验证协议的IKEv2 rfc7296要求 SSL/TLS/IKEv2服务器为客户端提供服务器证书,以便客户端执行服务器身份验证。为此,建议使 用受信任第三方 CA 将 SSL 证书颁发给 ASA。

思科不建议使用自签证书,因为用户可能会无意中将浏览器配置为信任来自欺诈服务器的证书。连 接到安全网关后,用户必须对安全警告作出响应,这也会给用户带来不便。

### 使用ASDM请求并安装新的身份证书

可以通过两种方式从证书颁发机构(CA)请求证书并在ASA上安装:

- 使用证书签名请求(CSR)。生成密钥对,通过CSR从CA请求身份证书,安装从CA获取的签名 身份证书。
- 使用从CA获取或从其他设备导出的PKCS12文件。PKCS12文件包含密钥对、身份证书、

### 请求并安装具有证书签名请求(CSR)的新身份证书

在需要身份证书的设备上创建CSR,使用设备上创建的密钥对。

CSR包含:

- 证书请求信息 请求的主题和其他属性,密钥对中的公钥,
- 签名算法信息,
- 证书请求信息的数字签名,使用密钥对中的私钥签名。

CSR被传递到证书颁发机构(CA),以便其以PKCS#10形式对其进行签名。

签名证书以PEM形式从CA返回。

注意:CA可在签署CSR并创建签名身份证书时更改信任点中定义的FQDN和主题名称参数。

#### 使用ASDM生成CSR

- 1. 创建具有特定名称的信任点
  - a. 导航到Configuration > Device Management > Certificate Management > Identity Certificates。



b. 单击 Add。

c. 定义信任点名称。

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&gt; ∨</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. 单击 Add a new identity certificate 单选按钮。
- 2. (可选)创建新密钥对

注意:默认情况下,使用名称为Default-RSA-Key且大小为2048的RSA密钥;但是,建 议为每个身份证书使用唯一的专用/公共密钥对。

a. 单击New生成新的密钥对。

ssued To	Issued By	Expiry Date	Associated Trustpo	ints	Usage	Public Key Type	Add
Add Identity C	ertificate			X	General Purpose	RSA (4096 bits)	Show Deta
					General Purpose	RSA (2048 bits)	Delete
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the ide	entity certificate from a file (	(PKCS12 format with Certificate)	(s)+Private Key):				Export
Decryption Pa	ssphrase:						Install
File to Import	From:	Browse.					Re-Enrol
Add a new ide	entity certificate:						_
( Add the ride		14					
Key Pair:	<default-rsa-< td=""><td>Key&gt; ∨ Snow</td><td>New</td><td></td><td></td><td></td><td></td></default-rsa-<>	Key> ∨ Snow	New				
Certificate Sul	bject DN: CN=asavpn.ex	ample.com Select.	•				
Generate	self-signed certificate						
Act as	local certificate authority a	nd issue dynamic certificates to	TLS-Proxy				
			Advanced				
Enable CA	flag in basic constraints ex	tension					

- b. 选择输入新密钥对名称选项,然后输入新密钥对的名称。
- c. 选择密钥类型 RSA或ECDSA。
- d. 选择Key Size;对于RSA,选择General purpose for Usage。
- e. 单击 Generate Now。密钥对现已创建。

ssued To		Issued By	Expiry Date	Associated Tru	stpoints	Usage	Public Key Type	Add
🔁 Add Ident	tity Certific	cate			×	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)	Show Detai
Trustpoint N	Name:	SSL-Trustpoint			100			Delete
	🔄 Add Ke	ey Pair		;	<			Export
Decry	Key Trees	0.054	0.55554	50064				Install
File to	Key Type	e:   RSA	O ECDSA O	EDUSA				Re-Enrol
Add a	Name:	O Use default key	pair name					
Key Pa		Enter new key p	pair name: SSL-Keypair					
Certifi	Size:	2048	] ~	N				
Ge	Usage:	General purpose	O Special	13				
<b>—</b>								
□ Er		Generate Now	Cancel	Help				

3. 选择密钥对名称

选择密钥对以签署CSR并将与新证书绑定。

sued To	Issued By	Expiry Date	Associated Trus	tpoints	Usage	Public Key Type	Add
🗧 Add Identity Certif	ficate			×	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)	Show Detail
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the identit	ty certificate from a file (	PKCS12 format with Ce	rtificate(s)+Private Key):				Export
Decryption Passpl	hrase:						Install
File to Import From	m:		Browse				Re-Enrol
Add a new identit	ty certificate:						
Key Pair:	SSL-Keypair	~	Show New				
Certificate Subjec	t DN: CN=asavpn.exa	ample.com	Select				
Generate self	-signed certificate						
Act as loca	al certificate authority ar	nd issue dynamic certific	cates to TLS-Proxy				
			Advanced				
	a la basis constrainte ovi	topping	Auvanceu				
	g in basic constraints ext	lension					

4. 配置证书主题和完全限定域名(FQDN)

注意:FQDN参数必须与身份证书用于的ASA接口的FQDN或IP地址匹配。此参数为身份 证书设置请求的主题备用名称(SAN)扩展。SSL/TLS/IKEv2客户端使用SAN扩展来验证 证书是否与其连接的FQDN匹配。

a. 单击选择。

	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窗口中,配置证书属性 — 从下拉列表中选择属性,输入值,然 后点击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	Cartificate Subject	DN		×		Export
Decryption Passphrase	Certificate Subject	DIN		~		Install
File to Import From:			Attribute V	alue		Re-Enroll
<ul> <li>Add a new identity certificate Subject DN</li> </ul>	DN Attribute to b Attribute: Com Value: asa.	e Added mon Name (CN) v vpn.example.com	Add>> Delete			
Generate self-sign						
Act as local ce						
Enable CA flag in t		ОК	Cancel Help			

Issued To	Issued By	Expiry Date	Associated Trust	points ^1 Us	age	Public Key Type	Add
Add Identity Certific	ate					×	Show Details
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the identity of					~		Export
Decryption Passphra	Certificate Subje	ect DIN			^		Install
File to Import From:			Attribut	ta Value			Re-Enroll
Add a new identity of the second s	EI DN Attribute to	be ådded	Commo	Name (CN) asa.vpn.exa	n		
Key Pair:	Attribute: C	ountry (C) V	Add>>				
Certificate Subject D	Value: Co	ommon Name (CN) epartment (OU)	Delete				
Generate self-si	an	ompany Name (O)					
Act as local of	St	tate (St)					
	La	ocation (L) mail Address (EA)					
		ОК	Cancel Help				
Enable CA flag ir	nt						
		Add Certificate	Cancel	Help			

属性	描述
CN	用于访问防火墙的名称(通常为完全限定域名,例如vpn.example.com)。
OU	组织内您所在部门的名称
0	您的组织/公司的合法注册名称
С	国家/地区代码(不带标点的 2 位字母代码)
ST	您的组织所在的州。
L	组织所在的城市。
企业协议 (EA)	电子邮件地址

注:前面任何一个字段值都不能超过64个字符的限制。值越长,可能导致身份证 书安装问题。此外,无需定义所有DN属性。

- 添加完所有属性后,单击OK。
- c. 配置设备FQDN 单击Advanced。

Issued To	Issued By	Expiry Date	Associated Trust	points ^1 Usag	e Public Key Typ	xe 📃	Add
Add Identity Certificat	e					× Sho	w Detai
Trustpoint Name:	SSL-Trustpoint					-	Delete
	rtificate from a file (PKC	S12 format with Certificate	e(s)+Private Kev)			E	Export
Decryption Passphrase	e:					1	Install
File to Import From:		Browse				Re	e-Enrol
Add a new identity cer	rtificate:						
Key Pair:	SSL-Keypair	<ul> <li>✓ Show.</li> </ul>	New				
Certificate Subject DN	: CN=asa.vpn.exam	ple.com Select					
Generate self-sign	ed certificate						
Act as local cer	rtificate authority and is	ssue dynamic certificates t	o TLS-Proxy				
						-	
			Advanced				
	oasic constraints extens	aon					
		Add Castificate	Canad	Usla			

d. 在FQDN字段中,输入从互联网访问设备的完全限定域名。Click OK.

ssued To	Issund Du Euripe Data Associated Trustanista A 1 Haza	Public Key Type	Add
Add Identity Cer	tificate Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.	×	Show Deta
Trustpoint Name:	S Certificate Parameters Enrollment Mode SCEP Challenge Password		Delete
O Import the iden	tity certifica		Export
Decryption Pass	sphrase: FQDN: asavpn.example.com		Install
File to Import Fi	rom: E-mail:		Re-Enrol
Add a new iden	IP Address:		
Key Pair:	S Include serial number of the device		
Certificate Subj	ect DN: C		
Generate se	elf-signed ce		
Act as k	pcal certifica		
Enable CA f	lag in basic i		

#### 5. 生成并保存CSR

a. 点击添加证书。

Issued To	Issued By	Expiry D	ate	Associated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Certific	ate						×	Show Detail
Trustpoint Name:	SSL-Trustpoint							Delete
O Import the identity	certificate from a file (PK	CS12 format with	Certificate(s)+Pri	vate Kev):				Export
Decryption Passphra	ase:							Install
File to Import From:			Browse					Re-Enroll
Add a new identity	certificate:							
Key Pair:	SSL-Keypair	~	Show	New				
Certificate Subject	DN: CN=asa.vpn.exa	nple.com	Select					
Generate self-si	gned certificate certificate authority and	issue dynamic cer	tificates to TLS-Pr	оху				
				Advanced				 
Enable CA flag in	n basic constraints exter	nsion						
		<b>6</b>						

b. 系统显示一则提示,以将 CSR 保存到本地计算机上的文件中。

ssued To	Issued By	Expiry	Date	Associated Trustpoints	~1	Usage	Public Key Type	Add
Add Identity Certif	icate						×	Show Detail
Trustpoint Name:	SSL-Trusto	ointl	]					Delete
O Import the identity	y certificate from a	file (PKCS12 format wi	ith Certificate(s)+Priv	ate Key):				Export
Decryption Passph	rase:		1					Install
File to Import From	n:	Identity Certifie	cate Request		×			Re-Enrol
Add a new identity	y certificate:	To complete the e request (CSR) and	nrollment process, pl d send it to the CA.	ease save the PKCS10 enrollme	nt			
Key Pair:	SSL-Keypa	You will then need	to install the certifica	ate that is returned from the C/	by			
Certificate Subject	t DN: CN=asa.vp	clicking the Install	button in the Identity	y Certificates panel.				
Generate self-	signed certificate	Save CSR to File:		Bro	wse			
Act as loca	l certificate author		OK Ca	ancel Help				
			A	dvanced				
Enable CA flag	in basic constraint	s extension						

单击 Browse,选择用于保存 CSR 的位置,然后使用.txt 扩展名保存文件。

注意:使用.txt扩展名保存文件时,可以使用文本编辑器(如记事本)打开和查看 PKCS#10请求。

c. 现在,新信任点显示为Pending状态。

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

安装步骤假设CA对CSR签名,并提供PEM编码(.pem、.cer、.crt)身份证书和CA证书捆绑包。

- 1. 安装签署CSR的CA证书
  - a. 导航到配置>设备管理>证书管理>,然后选择CA证书。单击 Add。

<u>C</u>	onfiguration > Remote Acc	ess VPN > Certificate Mana	agement > <u>CA Certificates</u>				
	N						
	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	Lon

b. 输入信任点名称并选择从文件安装,点击浏览按钮,然后选择中间证书。或者,将 PEM编码的CA证书从文本文件粘贴到文本字段中。

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

注意:安装签署CSR的CA证书,并使用与身份证书相同的信任点名称。PKI层次 结构中较高的其他CA证书可以安装在单独的信任点中。

c. 单击 Install Certificate。

denTrust Commercial Poot	Issued By	Expiry Date	Associated Trustpoints	Usage	Active	Add
denniast 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	Edit
Install Certificate					×	Show Details
Trustpoint Name: SS	L-Trustpoint	1.				Request CRI
O Install from a file:		Browse				Delete
Paste certificate in PEN	formati					
VR00BYCFE5St2sbra 9tLFV52U47em9tXaMu cGqeyDMRhs3Rs/wD2 2skqaRijsx153jV7Lk8 0jRyjaH56BFladkh270 gW8YpHNOvM08svyTX3 dcVcovOi/PAxnrAlJ+N END CERTIFICATE	Multinspragment b99LPVS2UPZem9UXAMBBGA1 00GCSQGSIb3DQBECWUAAHBS SM2wkAF4AYZHJ99gK9VCK+M SM2WXPB9sEbFh RddtVxPB9	Nova Doceworman Station Rep Udworm Statistics of the Statistical QArsXIPwK3JINBwoshSman QArsXIPwK3JINBwoshSman QArsXIPwK3JINBwoshSman QArsXIPWK3JINBwoshSman Wait Please wait while ASDM is delive device	Information	following attributes:	×	

- 2. 安装身份证书
  - a. 选择之前在CSR生成期间创建的身份证书。单击 Install。

				<u>rtificates</u>	Management > Identity	cess VPN > Certificat	iote Ac	nfiguration > Rem	Cor
Add		Public Key Type	Usage	Associated Trustpoints	Expiry Date	Issued By	^1	Issued To	[
Details	Sho		Unknown	SSL-Trustpoint	Pending	Not Available		[vpn.example.com]	1
elete									
port	E								
istall	1								
por ista	E								

注意:身份证书的Issued By字段可用,Expiry Date字段可用作Pending。

b. 选择包含从CA接收的PEM编码身份证书的文件,或在文本编辑器中打开PEM编码证书 ,然后将CA提供的身份证书复制并粘贴到文本字段中。

sued To ^1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
on.example.com]	Not Available	Pending	SSL-Trustpoint	Unknown		Show Details
La segui dal sede constante			×	General Purpose	RSA (2048 bits)	
Install Identity certifie	ate		tpoint	General Purpose	RSA (2048 bits)	Delete
lentity Certificate						Export
Install from a file:			Browse			Install
Install from a file:     Paste the certificate	data in base-64 forma	t:	Browse			Install Re-Enrol
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:     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:     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-Erroll

- 注:身份证书可以采用.pem、.cer、.crt格式进行安装。
- c. 单击 Install Certificate。

sued To ^1 Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
n.example.com] Not Available	Pending	SSL-Trustpoint	Unknown		Show Details
Install Identify antificate		~	General Purpose	RSA (2048 bits)	Show Details
Install identity certificate		tpoint	General Purpose	RSA (2048 bits)	Delete
lentity Certificate	ait	×			Export
O Install from a file:		information	×		Install
Paste the certificate data in bx     PARE     ICNNBJ26XQDmVUQ1HEBMVXR2K     Gyer3x26XXIL7NAIHBptyMcHD     T8y9Yia7poqMnamQkaQpcKAF     KdNqIFbUr6VW9NTuF2DowH3    END CERTIFICATE     <	ease wait while ASDM is deliverin	g th Le Certificate import su	ucceeded.		Re-Enroll

3. 使用ASDM将新证书绑定到接口

需要将ASA配置为使用新的身份证书,以便在指定接口上终止的WebVPN会话使用。

- a. 导航到Configuration > Remote Access VPN > Advanced > SSL Settings。
- b. 在"证书"下,选择用于端接 WebVPN 会话的接口。在本例中,使用的是外部接口。 单击 Edit。
- c. 在"证书"下拉菜单中,选择新安装的证书。

ooman		- Certimente			
					Edit
					Delete
	Select SSL Certificate		×		
	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	•		
tificates	Hanagement > tuenary cerandates.				
pecify which certificates, if ar	Interface:	OUTSIDE-direct		es not associated with a certificate of the	eir own.
	Primary Enrolled Certificate:	SSL-Trustpoint:unstructuredName =asavpn.exampl	$\sim$		Edit
Interface	Load Balancing Enrolled Certificate:	None	~	Кеу-Туре	Curt
OUTSIDE-direct			_		
inside when	OK	Cancel Help			
manacement	· · · · · · · · · · · · · · · · · · ·				
management					
	-				
allback Certificate:	None	~			

- d. Click OK.
- e. 单击 Apply。

Interface	Primary Certificate	Load Balancing Certificate	Кеу-Туре	Edit
OUTSIDE-direct	SSL-Trustpoint:unstructuredNa	me=	Primary: RSA (2048 bits), Load Balancing:	
nside				
nside-vlan				
management				

现在新的身份证书正在使用。

# 使用ASDM安装以PKCS12格式收到的身份证书

PKCS12文件(.p12或.pfx格式)包含身份证书、密钥对和CA证书。它由CA创建,例如使用通配符 证书,或者从其他设备导出。它是二进制文件,不能使用文本编辑器查看。

1. 从PKCS12文件安装身份和CA证书

身份证书、CA证书和密钥对需要捆绑到单个PKCS12文件中。

- a. 导航到Configuration > Device Management > Certificate Management,然后选择 Identity Certificates。
- b. 单击 Add。
- c. 指定信任点名称。

Issued 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 ide	entity certificate from a file (	PKCS12 format with	Certificate(s)+P	rivate Key):			Install
Decryption Pa	ssphrase:						Re-Enrol
File to Import	From:		Browse				
O Add a new ide	entity certificate:						
Key Pair:	<default-rsa-< td=""><td><ey> &lt;</ey></td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-<>	<ey> &lt;</ey>	Show	New			
Certificate Sul	bject DN: CN=risavpn31		Select				
Generate	self-signed certificate						
Act as	local certificate authority a	nd issue dynamic ce	rtificates to TLS-P	Proxy			
				Advanced			
BEnable CA	fac in basis constraints ov	tancian		Advanced			
LI STIADIE CA	a nag in basic consulaints ex	LETISION 8					

d. 单击Import The Identity Certificate from a File单选按钮。

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	<b>S</b>	Files of type:	All Files	~	c	ancel
Enable CA flag in					L-p-					

e. 输入用于创建 PKCS12 文件的密码。

ssued To	Issued By	Expiry Da	te	Associated Trustpoints	Usage	Public Key Type	Add
							Show Detail
🔁 Add Identity Ce	ertificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-P	KCS12					Export
<ul> <li>Import the idea</li> </ul>	ntity certificate from a file (P	KCS12 format with	Certificate(s)+P	rivate Key):			Install
Decryption Pas	ssphrase: ••••						Re-Enroll
File to Import F	rom: C:\Users\cisco.D	ESKTOP-R2CH8G	Browse				
O Add a new ider	ntity certificate:						
Key Pair:	<default-rsa-k< td=""><td>ey&gt; 🗸</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-k<>	ey> 🗸	Show	New			
Certificate Sub	ject DN: CN=risavpn31		Select				
Generate s	elf-signed certificate						
Act as	local certificate authority an	d issue dynamic ce	rtificates to TLS-P	roxy			
				Advanced			
Enable CA	flag in basic constraints exte	ansion		Auvanceu			
	nag in basic constraints exte						
	Add Cartificate	and	Hala	1			

f. 点击添加证书。

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Detail
add Identity	Certificate		×			Delete
Trustpoint Name	SSL-Trustpoint-	PKCS12				Export
Import the is	dentity certificate from a file (	PKCS12 format with Certificate(	(s)+Private Key):			Install
Decryption Passphrase: ••••			10000			Re-Enroll
File to Impor	t From: C:\Users\cisco.I	DESKTOP-R2CH8G Browse.				
🔿 Add  📮 P	lease wait		Information			×
Certi	Please wait while ASDM device	is delivering the command(s) to	Created trustpo WARNING: CA c the validation-us	ints for CAs higher in the hie ertificates can be used to va rage of this trustpoint to limit	rarchy as the CA certificate was not s alidate VPN connections,by default. Ple t the validation scope, if necessary	elf-signed.
	A flag in basic constraints ext	tension	Import PKCS12 d	operation completed success	fully.	
Enable C						

注意:导入带CA证书链的PKCS12时,ASDM会自动创建带有添加了 — number后 缀的名称的上游CA信任点。

onfiguration > Remote Access VPN > Certificate Management > CA Certificates									
Expiry Date	Associated Trustpoints	Usage	Active						
12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes						
12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes						
12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes						
	Expiry Date 12: 16:00 CEDT Oct 19 2028 12: 16:00 CEDT Oct 19 2028 12: 16:00 CEDT Oct 19 2028	Expiry Date         Associated Trustpoints           12: 16:00 CEDT Oct 19 2028         SSL-PKCS12           12: 16:00 CEDT Oct 19 2028         SSL-PKCS12-1           12: 16:00 CEDT Oct 19 2028         SSL-PKCS12-2	Expiry Date         Associated Trustpoints         Usage           12: 16:00 CEDT Oct 19 2028         SSL-PKCS12         Signature           12: 16:00 CEDT Oct 19 2028         SSL-PKCS12-1         Signature           12: 16:00 CEDT Oct 19 2028         SSL-PKCS12-1         Signature           12: 16:00 CEDT Oct 19 2028         SSL-PKCS12-2         Signature						

2. 使用ASDM将新证书绑定到接口

需要将ASA配置为使用新的身份证书,以便在指定接口上终止的WebVPN会话使用。

- a. 导航到Configuration > Remote Access VPN > Advanced > SSL Settings。
- b. 在"证书"下,选择用于端接 WebVPN 会话的接口。在本例中,使用的是外部接口。 单击 Edit。
- c. 在"证书"下拉菜单中,选择新安装的证书。

oomon		der micade		
rtificates Specify which certificates, if ar Interface OUTSIDE-direct inside inside -vlan management	Select SSL Certificate Specify enrolled trustpoints to be u OUTSIDE-direct interface. To enro Management > Identity Certificate Interface: Primary Enrolled Certificate: Load Balancing Enrolled Certificate ON	used for SSL authentication and VPN load balancing on the a trustpoint, go to Device Management > Certificate s. OUTSIDE-direct SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u : None	× ves not associated with a cert Key-Type	ificate of their own.
Fallback Certificate: Forced Certification Authentica	None	2 minutes		

- d. Click OK.
- e. 单击 Apply。

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

现在新的身份证书正在使用。

证书续订

# 使用ASDM续订使用证书签名请求(CSR)注册的证书

CSR注册证书的证书续订需要创建和注册新的信任点。它需要具有不同的名称(例如,具有注册年 份后缀的旧名称)。它可以使用与旧证书相同的参数和密钥对,也可以使用不同的参数和密钥对。

使用ASDM生成CSR

- 1. 创建具有特定名称的新信任点。
  - a. 导航到Configuration > Device Management > Certificate Management > Identity Certificates。

File       View       Tools       Wizards       Window       Help       Type topic to search       ()         Image: Home       Image: Configuration       Image: Configuration							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. 单击 Add。

c. 定义信任点名称。

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 Details
Add Identity Certificate						×	Delete
Trustpoint Name:	ASDM_TrustPoint0						Export
<ul> <li>Import the identity certif</li> </ul>	icate from a file (PKC	S12 format with Certificate(s)+Priva	te Key):				Install
Decryption Passphrase:							Re-Enroll
File to Import From:		Browse					1
O Add a new identity certif	icate:						
Key Pair:	<default-rsa-key:< td=""><td>&gt; v Show</td><td>New</td><td></td><td></td><td></td><td></td></default-rsa-key:<>	> v Show	New				
Certificate Subject DN:	CN=risavpn31	Select					
Generate self-signed	certificate						
Act as local certif	icate authority and is	sue dynamic certificates to TLS-Prox	ſγ				
		Adv	vanced				
🗹 Enable CA flag in bas	ic constraints extens	ion					

- d. 单击 Add a new identity certificate 单选按钮。
- 2. (可选)创建新密钥对

注意:默认情况下,使用名称为Default-RSA-Key且大小为2048的RSA密钥;但是,建 议为每个身份证书使用唯一的专用/公共密钥对。

a. 单击New生成新的密钥对。

ssued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName=	CN=ca.example.com, OU	OU 15:10:00 CEST Feb 6 2024		SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
🔄 Add Identity Cer	tificate			×			Delete
Trustpoint Name:	rustpoint Name: SSL-Trustpoint-2023					Export	
O Import the iden	tity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Pass	phrase:						Re-Enrol
File to Import Fr	rom:		Browse				
Add a new identication	tity certificate:						
Key Pair:	<default-rsa-key< td=""><td>/&gt; ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-key<>	/> ~	Show	New			
Certificate Subje	ect DN: CN=asavpn.exam	ple.com	Select				
Generate se	elf-signed certificate						
Act as lo	ocal certificate authority and	issue dynamic cer	tificates to TL	S-Proxy			
				Advanted			
				Advanced			
	iag in basic constraints exter	ision					

- b. 选择选项Enter new Key Pair name并输入新密钥对的名称。
- c. 选择Key Type RSA或ECDSA。
- d. 选择Key Size;对于RSA,选择General purpose for Usage。
- e. 单击 Generate Now。密钥对现已创建。

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredNam	e= CN=ca.example.com	, OU 15:10:00 CEST Feb 6 20	024 SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🔄 Add Identii	y Certificate		×			Delete
Trustpoint Na	me: SSL-Trustp	oint-2023				Export
C 🖾 Add	Key Pair		× <sub>key):</sub>			Install
Key Ty	pe: • RSA	○ ECDSA ○	EDDSA			Re-Enrol
Name:	O Use default key pa	ir name				
Ciner	Enter new key par	r name: SSL-KeyPair-2023	ew			
Usage:	General purpose	 ◯ Special				
	0	0.1				
	Generate Now	Cancel Help	iced			
	Con may in public constraint	a contentation				

3. 选择密钥对名称

选择密钥对以签署CSR并将与新证书绑定。

sued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
structuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
Add Identity	Certificate		×			Delete
Trustpoint Name	rustpoint Name: SSL-Trustpoint-2023					Export
Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):		s)+Private Key):			Install	
Decryption Passphrase:						Re-Enrol
File to Impor	rt From:	Browse				
Add a new id	dentity certificate:					
Key Pair:	SSL-KeyPair-2023	Show	New			
Certificate S	ubject DN: CN=asavpn.exam	select				
Generat	e self-signed certificate					
Act a	as local certificate aut grity and	issue dynamic certificates to T	TLS-Proxy			
			Advanced			
Enable C	CA flag in basic constraints exter	nsion				

4. 配置证书主题和完全限定域名(FQDN)

注意:FQDN参数必须与证书使用的ASA接口的FQDN或IP地址匹配。此参数设置证书的主题备用名称(SAN)。SSL/TLS/IKEv2客户端使用SAN字段验证证书是否与其连接的FQDN匹配。

注意:CA可在签署CSR并创建签名身份证书时更改信任点中定义的FQDN和主题名称参数。

a. 单击选择。

sued To Iss	sued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
structuredName= CN	=ca.example.com, OU	15:10:00 CEST Feb 6 2024		SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Deta
Add Identity Certifie	cate			×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
Import the identity	certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Passphr	ase:						Re-Enroll
File to Import From	:		Browse				
Add a new identity	certificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate Subject	DN: CN=asavpn.exam	ple.com	Select				
Generate self-s	igned certificate						
Act as local	certificate authority and	issue dynamic ce	rtificates to TL	S-Proxy			
				Advanced			
Enable CA flag	in basic constraints exten	ision					

b. 在Certificate Subject DN窗口中,配置证书属性 — 从下拉列表中选择属性,输入值,然 后点击Add。

Issued To Issued By		Expiry Date	Associated Trustpoints	Usage	Public Key Type RSA (2048 bits)	Add
nstructuredName=	nstructuredName= CN=ca.example.com, OU 15:10:00 CEST Feb 6		SSL-Trustpoint	General Purpose		Show Deta
Add Identity Certificate Trustpoint Name: SSI-Trustpoint-2023			×			Delete
		23				Export
Certificate Subject DN			×			Install
						Re-Enrol
		Attribute	Value			
DN Attribute to be	e Added	Common Name (CN Company Name (C	asavpn.example.com     example inc			
Attribute: Cou	ntry (C) 🗸 🗛	.dd>>				
value: US		Delete				
	OK	Cancel Help				
	A flag in basic constraints exter	nsion				

属性	描述
CN	用于访问防火墙的名称(通常为完全限定域名,例如 vpn.example.com)。
ου	组织内您所在部门的名称
0	您的组织/公司的合法注册名称
С	国家/地区代码(不带标点的 2 位字母代码)

属性	描述
ST	您的组织所在的州。
L	组织所在的城市。
企业协议 (EA)	电子邮件地址

注:前面的所有字段都不能超过64个字符的限制。值越长,可能导致身份证书安 装问题。此外,无需定义所有DN属性。

添加完所有属性后,单击OK。 c. 要配置设备FQDN,请单击Advanced。

C. 安凯直以留FQDN,旧半面Auvanceu。

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	4 SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🔄 Add Identity	y Certificate		×			Delete
Trustpoint Nar	ne: SSL-Trustpoint-2	2023				Export
O Import the	identity certificate from a file (	PKCS12 format with Certificate	e(s) +Private Key):			Install
Decryption	Passphrase:					Re-Enrol
File to Imp	ort From:	Browse				
Add a new	identity certificate:					
Key Pair:	SSL-KeyPair-202	23 v Show.	New			
Certificate	Subject DN: /pn.example.com	m,O=example inc Select.				
Genera	ate self-signed certificate					
Ac	t as local certificate authority an	nd issue dynamic certificates to	o TLS-Proxy			
			Advanced			
Enable	CA flag in basic constraints ext	ension				

d. 在FQDN字段中,输入从互联网访问设备的完全限定域名。Click OK.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
	Ontions	NOLI HELIOLOGICEST SALIS T	X	General Purpose	RSA (2048 bits)	Show Detail
						Delete
Certificate Par	ameters Forollment Mode	SCEP Challenge Password	e for self-signed certificates.			Export
						Install
FQDN:	asavpn.example.com					Re-Enroll
E-mail:						
IP Address:	arial number of the deutse					
	endemoter of the device					
		Ν				
		63				
	OK	Cancel Help				

- 5. 生成并保存CSR
  - a. 点击添加证书。

ssued To	Issued By	Expiry Date		Associated Tru	stpoints	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 Details
add Identity Co	ertificate				×			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	ssphrase:							Re-Enroll
File to Import	From:		Browse	1				
Add a new ide	entity certificate:							
Key Pair:	SSL-KeyPair-2023	~	Show	New				
Certificate Sub	bject DN: /pn.example.com,	O=example inc	Select	]				
Generate	self-signed certificate				-			
Act as	local certificate authority and	issue dynamic cer	tificates to TLS	-Proxy	-			
			r					
_			L	Advanced				
Enable CA	A flag in basic constraints exten	ision						
	Add Cartificate	Innel	Hala		-			

b. 系统显示一则提示,以将 CSR 保存到本地计算机上的文件中。

sued to	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
structuredName	= CN=ca.example.com, OU	. 15:10:00 CEST Feb 6 20	24 SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🗟 Add Identit	y Certificate		×			Delete
Trustpoint Nar	ne: SSL-Trustpoint-20	023				Export
O Import the	identity certificate from a file (Pl	KCS12 format with Certifica	te(s)+Private Key):			Install
E Ide	ntity Certificate Request		×			Re-Enrol
K You v dickir C Save	vill then need to install the certific ig the Install button in the Identi CSR to File: C:\Users\cisco.DES	cate that is returned from t ty Certificates panel. SKTOP-R2CH8G5\Docun	Browse			
	ОК С	Cancel Help	Advanced			

单击浏览。选择保存CSR的位置,并保存扩展名为.txt的文件。

注意:使用.txt扩展名保存文件时,可以使用文本编辑器(如记事本)打开和查看 PKCS#10请求。

c. 现在,新信任点显示为Pending状态。

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	SSL-Trustpoint	General Purpose	General Purpose RSA (2048 bits)	Show Detail
savpn.example.com]	Not Available	Pending	SSL-Trustpoint-2023	Unknown		Show Detail
						Delete
						Export
						Install
						Re-Enroll
						1

使用ASDM安装PEM格式的身份证书

安装步骤假设CA对CSR进行签名,并提供PEM编码(.pem、.cer、.crt)的新身份证书和CA证书捆绑 包。

1. 安装签署CSR的CA证书

签名身份证书的CA证书可以安装在为身份证书创建的信任点中。如果身份证书由中间CA签名 ,则此CA证书可以安装在身份证书信任点中。层次结构中上游的所有CA证书可以安装在单独 的CA信任点中。

a. 导航到Configuration > Device Management > Certificate Management > , 然后选择CA Certificates。单击 Add。

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
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

b. 输入信任点名称并选择从文件安装,单击浏览按钮,然后选择中间证书。或者,将 PEM编码的CA证书从文本文件粘贴到文本字段中。

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
🧧 Install Certificate						×	Show Detai
Trustpoint Name:	SSL-Trustpoint-2023						Request CR
Install from a file		Browse					Delete
	in DEM formati						

注意:如果身份证书由中间CA证书签名,请安装信任点名称与身份证书信任点名 称相同的中间证书。

c. 单击 Install Certificate。

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						X Show Deta
Trustpoint Name: SSL	-Trustpoint-2023					Request Cl
O Install from a file:		Browse				Delete
Paste certificate in PEM	format:					
SIXVFik1212CEGn6b2u GK55EPH23QU/X6III OJ9X4nYCPPf33QD/X6III VR0089YEF253L2sbraf 9tLFY52U47em3Ux1AM cGqey0MRhsRs/M023 z9kqaRjist1539/Y/L66 OJRxy1alH56BFladdxc7K3 gW8YnH0CM408svyTX5 dC/ccvc/DAxmAIJH4 END CERTIFICATE Use EST: Specify source Interfac EST URL: https:// Certificate Subject DN:	mri qa V23 tewiu THOX 488-3ux //momx46/Ckelse/MOSpinvLi abb/stu 2014/2014/2014/2014/2014/2014/2014/2014/	1PH9 B BSQG0 + d1waOBBCWk VyQ9HNkQd7US1KwRaX wGA1UdEwQFMAMBARBawHQI LUdIwQVMBaAFE55K2sbra9b ADArsKErwK3NBwOshfsmdT. formation INFO: Certificate ha Fingerprint: e9ad16 Trustpoint CA certificate	YD as the following attributes: ISC 2673424c 6e7e0c5f b30b4a02 icate accepted.	×		
allow-untrusted-cor	nection					
O Use SCEP:						
Specify source Interfac	e: None	~				
SCEP URL: http://						
Retry Period:	1	minutes				

在本例中,新证书使用与旧证书相同的CA证书签名。同一个CA证书现在与两个信任点 关联。

nfiguration > 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-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
IdenTrust Commercial Root	CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Show Details
						Request CRL
						Delete

- 2. 安装身份证书
  - a. 选择之前通过CSR生成创建的身份证书。单击 Install。

Configuration > Devi	ce Management > Certific	ate Management > Identii	ty Certificates				l
Issued To	Issued By	Expiry Date	Associated Trustpoints	v 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
							Testall
							Install
							Re-Enroll

注意:身份证书的Issued By字段可为Not available,而Expiry Date字段为 Pending。

b. 选择包含从CA接收的PEM编码身份证书的文件,或在文本编辑器中打开PEM编码证书 ,然后将CA提供的身份证书复制并粘贴到文本字段中。

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
🛓 Install Identity	certificate		×				Install
dentity Certificate							Re-Enro
<ul> <li>Install from a</li> </ul>	file:		Browse				
Paste the cert	ificate data in base-64 format						

注:身份证书可以采用.pem、.cer、.crt格式进行安装。

c. 单击 Install Certificate。

	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
avpn.example.com	n] Not Available	Pending	SSL-Trustpoint-2023		Unknown		Delete
							Decte
							Export
Install Identity	certificate		×				Install
entity Certificate							Re-Enrol
	e wait						
Prease	Informa	ation	×				
E E	Please wait wr		7				
	device 🕥	Carlifornia impact averaged					
g III	(i)	Certificate import succeede					
		Certificate import succeede					
		Certificate import succeede					

### 安装后,存在旧身份证书和新身份证书。

		1 1				
Issued To	Issued By	Expiry Date	Associated Trustpoints	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 Details
nstructuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	- Short Declara
						Delete
						Export
						Install
						Re-Enroll

3. 使用ASDM将新证书绑定到接口

需要将ASA配置为使用新的身份证书,以便在指定接口上终止的WebVPN会话使用。

- a. 导航到Configuration > Remote Access VPN > Advanced > SSL Settings。
- b. 在"证书"下,选择用于端接 WebVPN 会话的接口。在本例中,使用的是外部接口。

单击 Edit。

c. 在"证书"下拉菜单中,选择新安装的证书。

				Edit Delete
	Select SSL Certificate Specify enrolled trustpoints to be us	ed for SSL authentication and VPN load balancing on the		
ertificates	OUTSIDE-direct interface. To enroll Management > Identity Certificates	a trustpoint, go to Device Management > Certificate OLITSIDE-direct	res and pressing with a santificate of their sum	]
Interface	Primary Enrolled Certificate:	SSL-Trustpoint-2023:unstructuredName=asavpn.exampl v	Key-Type	Edit
OUTSIDE-direct inside inside-vlan	Load balancing chrolled Certificate:	Cancel Help	Primary: RSA (2048 bits), Load Balancing: n	
management				

- d. Click OK.
- e. 单击 Apply。现在新的身份证书正在使用。

				Edit
				Delete
ficates	iy, should be used for SSL authentication or	each interface. The failback certificate will be u	sed on interfaces not associated with a certificate of their own.	
ficates ecify which certificates, if ar Interface	ny, should be used for SSL authentication on Primary Certificate	each interface. The fallback certificate will be us Load Balancing Certificate	sed on interfaces not associated with a certificate of their own. Key-Type	Edit
ficates ecify which certificates, if ar Interface OUTSIDE-direct	ry, should be used for SSL authentication on Primary Certificate SSL-Trustpoint-2023kunstructur	each interface. The fallback certificate will be us Load Balancing Certificate	sed on interfaces not associated with a certificate of their own. Key-Type Primary: RSA (4096 bits), Load Balancing: n	Edit
ficates — ecify which certificates, if ar Interface OUTSIDE-direct inside	ny, should be used for SSL authentication on Primary Certificate SSL-Trustpoint-2023;unstructur	each interface. The fallback certificate will be u Load Balancing Certificate	sed on interfaces not associated with a certificate of their own. Key-Type Primary: RSA (4096 bits), Load Balancing: n	Edit
ficates edfy which certificates, if ar Interface OUTSIDE-direct inside inside-vlan	ry, should be used for SSL authentication on Primary Certificate SSL-Trustpoint-2023:unstructur	each interface. The failback certificate will be u Load Balancing Certificate	sed on interfaces not associated with a certificate of their own. Key-Type Primary: RSA (4096 bits), Load Balancing: n	Edit

# 使用ASDM续订使用PKCS12文件注册的证书

PKCS12注册证书的证书续订需要创建和注册新的信任点。它需要具有不同的名称(例如,具有注 册年份后缀的旧名称)。

PKCS12文件(.p12或.pfx格式)包含身份证书、密钥对和CA证书。例如,通配符证书由CA创建 ,或从其他设备导出。它是二进制文件,不能通过文本编辑器查看。

1. 从PKCS12文件安装更新的身份证书和CA证书

身份证书、CA证书和密钥对需要捆绑到单个PKCS12文件中。

- a. 导航到Configuration > Device Management > Certificate Management,然后选择 Identity Certificates。
- b. 单击 Add。
- c. 指定新的信任点名称。

Issued To	Issued By	Expiry Da	ite	Associated Trustpoints	Usage	Public Key Type	Add
				10			Show Detail
🔁 Add Identity C	ertificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-	PKCS12					Export
Import the ide	entity certificate from a file (	PKCS12 format with	n Certificate(s)+P	rivate Key):			Install
Decryption Pa	assphrase:						Re-Enrol
File to Import	From:		Browse				
O Add a new ide	entity certificate:						
Key Pair:	<default-rsa+< td=""><td>(ey&gt; 🗸</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa+<>	(ey> 🗸	Show	New			
Certificate Su	bject DN: CN=risavpn31		Select	10-07 mm-02			
Generate	self-signed certificate						
Act as	local certificate authority a	nd issue dynamic ce	rtificates to TLS-P	roxy			
				thread			
The state of	0			Advanced			
	A flag in basic constraints ext	tension;					

d. 单击Import The Identity Certificate from a File单选按钮。

ssued to	Issued By	Expiry Date		Associated T	rustpoints	Usage	F	Public Key Type		Add
										Show Detail
Add Identity Certifica	te	1 Acres 1		>	<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	<b>S</b>	Files of type:	All Files	~	c	ancel
Enable CA flag in					L-p-					

e. 输入用于创建 PKCS12 文件的密码。

ssued To	Issued By	Expiry Da	te	Associated Trustpoints	Usage	Public Key Type	Add
							Show Detail
🔁 Add Identity Ce	ertificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-P	KCS12					Export
<ul> <li>Import the idea</li> </ul>	ntity certificate from a file (P	KCS12 format with	Certificate(s)+P	rivate Key):			Install
Decryption Pas	ssphrase: ••••						Re-Enroll
File to Import F	rom: C:\Users\cisco.D	ESKTOP-R2CH8G	Browse				
O Add a new ider	ntity certificate:						
Key Pair:	<default-rsa-k< td=""><td>ey&gt; 🗸</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-k<>	ey> 🗸	Show	New			
Certificate Sub	ject DN: CN=risavpn31		Select				
Generate s	elf-signed certificate						
Act as	local certificate authority an	d issue dynamic ce	rtificates to TLS-P	roxy			
				Advanced			
Enable CA	flag in basic constraints exte	ansion		Auvanceu			
	nag in basic constraints exte						
	Add Cartificate	and	Hala	1			

f. 点击添加证书。

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
🔁 Add Identity (	Certificate		×			Delete
Trustpoint Name	: SSL-Trustpoint-f	PKCS12				Export
<ul> <li>Import the id</li> </ul>	lentity certificate from a file (I	PKCS12 format with Certificate	(s) +Private Key):			Install
Decryption P	assphrase: ••••					Re-Enrol
File to Impor	t From: C:\Users\cisco.E	DESKTOP-R2CH8G Browse.				
🔿 Add 🔚 P	lease wait					×
	device	is delivering the command(s) to	Created trustpo	nts for CAs higher in the hie	erarchy as the CA certificate was not s	elf-signed.
C			WARNING: CA o the validation-u	ertificates can be used to va age of this trustpoint to limi	alidate VPN connections,by default. Ple t the validation scope, if necessary	ease adjust
Enable C	A flag in basic constraints ext	tension	Import PKCS12	operation completed success	sfully.	

注意:导入带CA证书链的PKCS12时,ASDM会自动创建带有添加后缀的名称的 上游CA信任点。

onfiguration > Remote Access VPN > Certificate Management > CA Certificates										
Issued To	~ 1	Issued By	Expiry Date	Associated Trustpoints	Usage	Active				
KrakowCA-sub1-1		CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes				
KrakowCA-sub1		CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes				
KrakowCA		CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes				

2. 使用ASDM将新证书绑定到接口

需要将ASA配置为使用新的身份证书,以便在指定接口上终止的WebVPN会话使用。

- a. 导航到Configuration > Remote Access VPN > Advanced > SSL Settings。
- b. 在"证书"下,选择用于端接 WebVPN 会话的接口。在本例中,使用的是外部接口。 单击 Edit。
- c. 在"证书"下拉菜单中,选择新安装的证书。

					Alexand and a second
					Edit Delete
[	😰 Select SSL Certificate		×		See Pr
	Specify enrolled trustpoints to be OUTSIDE-direct interface. To enro Management > Identity Certificate	used for SSL authentication and VPN load balancing on the ill a trustpoint, go to Device Management > Certificate es.			
ificates becify which certificates, if ar	Interface:	OUTSIDE-direct	ies	not associated with a certificate	of their own.
Interface	Primary Enrolled Certificate:	SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u	~	Key-Type	Edit
OUTSIDE-direct	Load Balancing Enrolled Certificate	None	~		
inside					
inside-vlan	0	K Cancel Help			
management					
allback Certificate:	None	×			
orced Certification Authenticat	tion Timeout:	2 minutes			

- d. Click OK.
- e. 单击 Apply。

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

现在新的身份证书正在使用。

# 验证

使用以下步骤验证第三方供应商证书的安装是否成功以及是否用于SSL VPN连接。

### 通过 ASDM 查看已安装的证书

- 1. 导航至配置 > 远程接入 VPN > 证书管理,并选择身份证书。
- 2. 可能会显示第三方供应商颁发的身份证书。

Certi	ficates									
Sp	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	${\tt SSL-Trustpoint-PKCS12:} unstructured {\tt Name=F}$		Primary: RSA (2048 bits), Load Balan						

### 故障排除

如果SSL证书安装失败,则将在CLI上收集此debug命令。

• debug crypto ca 14

# 常见问题解答

问:什么是PKCS12?

A.在加密中,PKCS12定义了一个存档文件格式,创建该格式以将多个加密对象存储为单个文件。 它通常用于将私钥与其X.509证书捆绑在一起,或者用于捆绑信任链的所有成员。

问:什么是CSR?

A.在公钥基础设施(PKI)系统中,证书签名请求(也称为CSR或证书请求)是从申请人发送到公钥基 础结构的注册机构以申请数字身份证书的消息。它通常包含可为其颁发证书的公钥、用于标识已签 名证书的信息(例如主题中的域名)以及完整性保护(例如数字签名)。

问:PKCS12的密码在哪里?

A.当证书和密钥对导出到PKCS12文件时,在export命令中给出口令。 对于导入pkcs12文件,密码 需要由所有者、从其他设备导出PKCS12的CA服务器或人员提供。

问:根和身份之间有什么区别?

答:在加密和计算机安全中,根证书是标识根证书颁发机构(CA)的公钥证书。根证书是自签名的 (并且证书可以有多个信任路径,例如证书是否由交叉签名的根颁发),并构成基于X.509的公钥 基础设施(PKI)的基础。公钥证书,也称为数字证书或身份证书,是一种用于证明公钥所有权的电子 文档。证书包括有关密钥的信息、有关其所有者(称为主题)的标识的信息以及已验证证书内容的 实体(称为颁发者)的数字签名。如果签名有效,并且检查证书的软件信任颁发者,那么它就可以 使用该密钥与证书的使用者进行安全通信。

问:我安装了证书,为什么它不工作? A.这可能有许多原因,例如:

1.已配置证书和信任点,但尚未将其绑定到应使用该证书和信任点的进程。例如,要使用的信任点 不会绑定到终止Anyconnect客户端的外部接口。

2.已安装PKCS12文件,但由于PKCS12文件中缺少中间CA证书而出现错误。如果客户端的中间 CA证书为受信任的,但根CA证书不是受信任的,则无法验证整个证书链并将服务器身份证书报告 为不受信任。

3.使用不正确的属性填充的证书可能会导致安装失败或客户端错误。例如,某些属性可能使用错误 的格式进行编码。另一个原因是身份证书缺少主题备用名称(SAN),或者用于访问服务器的域名没 有作为SAN出现。

问:安装新证书是否需要维护窗口或导致停机时间?

A.安装新证书(身份或CA)不会带来干扰,不应导致停机或需要维护窗口。要启用新证书以用于现 有的服务,需要更改并且可能需要更改请求/维护窗口。

问:添加或更改证书能否断开连接的用户?

答:不,当前连接的用户保持连接。证书用于连接建立。用户重新连接后,将使用新证书。

问:如何使用通配符创建CSR?或主题备用名称(SAN)?

A.目前,ASA/FTD无法使用通配符创建CSR;但是,此过程可以通过OpenSSL完成。要生成 CSR和ID密钥,可以运行以下命令:

openssl genrsa -out id.key 2048

openssl req -out id.csr -key id.key -new 使用完全限定域名(FQDN)属性配置信任点时,ASA/FTD创建的CSR包含具有该值的SAN。当CA签

署CSR时,可以添加更多SAN属性,也可以使用OpenSSL创建CSR

问:证书更换是否立即生效?

A.新服务器身份证书仅用于新连接。新证书可在更改后立即使用,但实际上用于新连接。

问:如何检查安装是否有效?

A.用于验证的CLI命令: show crypto ca cert <trustpointname>

问:如何从身份证书、CA证书和私钥生成PKCS12?

A.PKCS12可以通过OpenSSL使用以下命令创建:

openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt

问:如何导出证书以将其安装在新的ASA中?

Α.

- 使用CLI:使用命令crypto ca export <trustpointname> pkcs12 <password>
- 使用ASDM:
  - a. 导航到Configuration > Device Management > Certificate Management > Identity Certificates,然后选择Identity Certificate。单击Export。

File View Tools Wizards Wind	low Help					Type topic to search	Go	ababa
🚮 Home 🦓 Configuration 🔯 Mo	onitoring 🔚 Save 🔇 Refre	esh 🔇 Back 🔘 Forwar	d 🦻 Help					cisco
Bookmarks 🗗 🖓 🗡	Configuration > Device Ma	nagement > Certificate M	lanagement > Identity Ce	rtificates				
o bookmark a page, right-dick on a ode in the navigation tree and select Add to bookmarks".	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type		Add
🕒 Go   Delete	unstructuredName=asav unstructuredName=risav	CN=ca.example.com, OU CN=ca.example.com, OU	16:10:00 CEDT Apr 6 2024 15:10:00 CEST Feb 6 2024	SSL-Trustpoint-2023 SSL-Trustpoint	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)		Show Details
	[asa.vpn.example.com]	CN=KrakowCA-sub1-1 Not Available	04:44:00 CEST Dec 21 2024 Pending	SSL-Trustpoint-PKCS12 SSL-Trustpoint	General Purpose Unknown	RSA (2048 bits)		Delete
								Instal
							i	Re-Enrol
Device Management 🗗 🖗								
Management Access     Licensing								
System Image/Configuration     Generation     Generation     Generation								
Logging     Smart Call-Home	Find:	💿 🙆 🗌 Match Case						
Cloud Web Security     Service Module Settings	Certificate Expiration Alerts Send the first alert befor	e : 60 (days) Set Def	ault					
Gerbificate Management     Gerbificate Management     Gerbificates	Repeat Alert Interval :	7 (days)						
	Weak Cruste Configurations							

b. 选择导出文件的位置,指定导出密码,然后点击Export Certificate。

sued To Issu	ued By	Expiry Date	Associated Trustpoints	Usag	e	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 Detai
structuredName=risav CN=	ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	(	General Purpose	RSA (2048 bits)	Show Detai
structuredName=FTD7 CN=	KrakowCA-sub1-1	04:44:00 CEST Dec 21 2024	SSL-Trustpoint-PKCS12	(	Seneral Purpose	RSA (2048 bits)	Delete
a.vpn.example.com] Not	Available	Pending	SSL-Trustpoint		Unknown		Export
							Install
							Re-Enroll
nd: Send the first alert before : 60 Repeat Alert Interval : 7	Match Case     (days) Set Defa     (days)	ult					
nd: Send the first alert before : 60 Repeat Alert Interval : 7 Crypto Configurations	Match Case      Match Case      (days) Set Defa      (days)      Export certificate	ult		×			
d:        d: <ul> <li>iffcate Expiration Alerts</li> <li>Send the first alert before : 60</li> <li>Repeat Alert Interval : 7</li> <li>Crypto Configurations</li> <li>Permit Weak key sizes and Ha</li> </ul>	<ul> <li>Match Case</li> <li>(days) Set Defa</li> <li>(days)</li> <li>Export certificate</li> <li>Export to File:</li> </ul>	ult C:\Users\disco.DESKTOP+	R2CH8G5\Documents\ce Brows	×	-		
d: Send the first alert before : 60 Repeat Alert Interval : 7 Crypto Configurations Permit Weak key sizes and Ha CA Enrollment	Match Case   (days) Set Defa   (days)   Export certificate   Export to File:   Certificate Format:	ult C:\Users\disco.DESKTOP+	R2CH8G5\Documents\ce	×			
d:        oil     oil       tificate Expiration Alerts	<ul> <li>Match Case</li> <li>(days) Set Defa</li> <li>(days)</li> <li>Export certificate</li> <li>Export to File: Certificate Format:</li> </ul>	ult C:\Users\disco.DESKTOP+ @ PKCS12 Format (Cerbif	R2CH8G5\Documents\ce Brows	×	stomers a special	promotional price for certificat	tes and trial certificates
d: State Expiration Alerts Send the first alert before : 60 Repeat Alert Interval : 7 Crypto Configurations Permit Weak key sizes and Ha CA Enrollment your Cisco ASA security applia ing.	Match Case Match Case Gays) Set Defa (days) Export certificate Export to File: Certificate Format:	ult C:\Users\cisco.DESKTOP+ PKCS12 Format (Certifi DBM Event (castfact)	R2CH8G5\Documents\ce Brows icate(s) + Private Key)	×	stomers a special	promotional price for certifical	tes and trial certificates
d: Send the first alert before : 60 Repeat Alert Interval : 7 Crypto Configurations — Permit Weak key sizes and Ha CA Enrollment — your Cisco ASA security applia ing.	<ul> <li>Match Case</li> <li>(days) Set Defa</li> <li>(days)</li> <li>Export certificate</li> <li>Export to File:</li> <li>Certificate Format:</li> </ul>	C:\Users\dsco.DESKTOP+ PKCS12 Format (Certification of the second secon	R2CH8G5\Documents\ce  Brows icate(s) + Private Key) e Only)	e	stomers a special	promotional price for certifical	tes and trial certificates
d: Send the first alert before : 60 Repeat Alert Interval : 7 Crypto Configurations Permit Weak key sizes and Ha CA Enrollment your Cisco ASA security applia ing.	Match Case     Match Case     (days) Set Defa     (days)     Export certificate     Export to File:     Certificate Format:     Configuration Encryptic	Ult C:\Users\cisco.DESKTOP + @ PKCS 12 Format (Certification) @ PEM Format (Certification) PEM Format (Certification)	R2CH8G5\Documents\ce Brows icate(s) + Private Key) e Only)	× e	stomers a special	promotional price for certifical	tes and trial certificates
nd: Send the first alert before : 60 Repeat Alert Interval : 7 Crypto Configurations Permit Weak key sizes and Ha CA Enrollment your Cisco ASA security applia ing. ng a previously saved certifica	Match Case     Match Case     (days) Set Defa     (days)     Export certificate     Export to File:     Certificate Format:     Configuration Encryption     Pasphra	C:\Users\cisco.DESKTOP+ PKCS 12 Format (Certification) PEM Format (Certification) P	R2CH8G5\Documents\ce Brows icate(s) + Private Key) e Only)	×	stomers a special	promotional price for certifical	tes and trial certificates

导出的证书可以在计算机磁盘上。请注意安全位置的口令,否则文件将毫无用处。

问:如果使用ECDSA密钥,则SSL证书生成过程是否不同?

答:配置的唯一区别是密钥对生成步骤,在该步骤中可生成ECDSA密钥对,而不是RSA密钥对。其 余步骤保持不变。

问:是否始终需要生成新的密钥对?

答:密钥对生成步骤是可选的。可以使用现有的密钥对,如果是PKCS12,则密钥对将与证书一起 导入。有关各自的注册/重新注册类型,请参阅"选择密钥对名称"部分。

问:为新的身份证书生成新的密钥对是否安全?

答:只要使用新的密钥对名称,该过程就是安全的。在这种情况下,旧密钥对不会更改。

问:在更换防火墙时(如RMA),是否需要再次生成密钥?

A.新防火墙的设计没有在旧防火墙上提供密钥对。

运行配置的备份不包含密钥对。

使用ASDM完成的完全备份可以包含密钥对。

可以在身份证书发生故障之前,通过ASDM或CLI从ASA导出身份证书。

如果出现故障切换对,则使用write standby命令将证书和密钥对同步到备用设备。如果替换了故障 切换对中的一个节点,则配置基本故障切换并将配置推送到新设备就足够了。

如果设备丢失了密钥对,并且没有备份,则需要使用新设备上存在的密钥对来签署新证书。

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。