ASDMで管理されるASAでの証明書のインスト ールと更新

内容

概要 前提条件 要件 使用するコンポーネント 背景説明 ASDMを使用した新しいID証明書の要求とインストール 証明書署名要求(CSR)を使用した新しいID証明書の要求とインストール ASDMを使用したCSRの生成 特定の名前を使用したトラストポイントの作成 (オプション)新しいキーペアの作成 キーペア名の選択 証明書のサブジェクトと完全修飾ドメイン名(FQDN)の設定 CSRの 生成 と保存 ASDMを使用したPEM形式でのID証明書のインストール CSRに署名したCA証明書のインストール ID 証明書のインストール ASDMを使用したインターフェイスへの新しい証明書のバインド ASDMを使用したPKCS12形式で受信したID証明書のインストール PKCS12ファイルからのID証明書とCA証明書のインストール ASDMを使用したインターフェイスへの新しい証明書のバインド 証明書の更新 ASDMを使用した証明書署名要求(CSR)に登録された証明書の更新 ASDMを使用したCSRの生成 特定の名前で新しいトラストポイントを作成します。 (オプション)新しいキーペアの作成 キーペア名の選択 証明書のサブジェクトと完全修飾ドメイン名(FQDN)の設定 CSRの生成と保存 ASDMを使用したPEM形式でのID証明書のインストール <u>CSRに署名したCA証明書のインストール</u> ID 証明書のインストール ASDMを使用したインターフェイスへの新しい証明書のバインド ASDMを使用したPKCS12ファイルに登録された証明書の更新 PKCS12ファイルからの更新されたID証明書とCA証明書のインストール ASDMを使用したインターフェイスへの新しい証明書のバインド 確認 ASDM を使用してインストールされた証明書の表示 トラブルシュート

概要

このドキュメントでは、ASDMで管理されているCisco ASAソフトウェアで特定のタイプの証明 書を要求、インストール、信頼、および更新する方法について説明します。

前提条件

要件

- 開始する前に、適応型セキュリティアプライアンス(ASA)のクロック時刻、日付、およびタ イムゾーンが正しいことを確認します。証明書認証では、ネットワークタイムプロトコル (NTP)サーバを使用してASAの時刻を同期することをお勧めします。関連情報を参照してく ださい。
- 証明書署名要求(CSR)を使用する証明書を要求するには、信頼できる内部またはサードパー ティの認証局(CA)にアクセスできる必要があります。サードパーティCAベンダーの例とし ては、Entrust、Geotrust、GoDaddy、Thawte、VeriSignなどがあります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASAv 9.18.1
- PKCS12の作成には、OpenSSLが使用されます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

このドキュメントで扱う証明書の種類は次のとおりです。

- 自己署名証明書
- サードパーティ認証局または内部CAによって署名された証明書

EAP認証プロトコル用のSecure Socket Layer(SSL)、Transport Layer Security(TLS)、および IKEv2 rfc7296では、SSL/TLS/IKEv2サーバが、クライアントがサーバ認証を実行するためのサー バ証明書をクライアントに提供する必要があります。この目的のために、信頼できるサードパー ティの CA を使用して ASA に SSL 証明書を発行することをお勧めします。

ユーザが不正なサーバからの証明書を信頼するようにブラウザを誤って設定する可能性があるため、自己署名証明書を使用することは推奨されません。また、ユーザがセキュリティ ゲートウェ イに接続するときにセキュリティ警告に応答する必要があるという不便さもあります。

ASDMを使用した新しいID証明書の要求とインストール

証明書は、認証局(CA)から要求し、次の2つの方法でASAにインストールできます。

- 証明書署名要求(CSR)を使用します。キーペアを生成し、CSRを使用してCAからID証明書 を要求し、CAから取得した署名付きID証明書をインストールします。
- CAから取得した、または別のデバイスからエクスポートしたPKCS12ファイルを使用しま す。PKCS12ファイルには、キーペア、ID証明書、CA証明書が含まれています。

証明書署名要求(CSR)を使用した新しいID証明書の要求とインス トール

ID証明書を必要とするデバイス上にCSRが作成されます。デバイス上に作成されたキーペアを使 用します。

CSRには次のものが含まれます。

- 証明書要求情報:要求されたサブジェクトおよびその他の属性、キーペアからの公開キー、
- シグニチャアルゴリズム情報、
- キーペアからの秘密キーで署名された、証明書要求情報のデジタル署名。

CSRは認証局(CA)に渡され、PKCS#10形式で署名されます。

署名付き証明書は、PEM形式でCAから返されます。

注:CAは、CSRに署名して署名付きID証明書を作成するときに、トラストポイントで定義 されているFQDNパラメータとサブジェクト名パラメータを変更できます。

ASDMを使用したCSRの生成

- 1. 特定の名前を使用したトラストポイントの作成
 - a. Configuration > Device Management > Certificate Management > Identity Certificatesの順に移動します。



b. [Add] をクリックします。

c. トラストポイント名を定義します。

ssued To	Issued By	Expiry Date	Associated Trustpoints	^1 Usage	Public Key Type	Add
🧧 Add Identity (Certificate				×	Show Deta
Trustpoint Name	SSL-Trustpoint					Delete
O Import the id	entity certificate from a file (PKCS12 format with Certificate(s)+Private Key):			Export
Decryption Pa	assphrase:					Install
File to Import	t From:	Browse				Re-Enrol
Add a new id	entity certificate:	(av) Show	New			
Key Pair: Certificate Su	<pre></pre>	ample.com Select	New			
Generate	self-signed certificate	,				
Act a	s local certificate authority ar	nd issue dynamic certificates to T	TLS-Proxy		_	
			Advanced			
Enable C	A flag in basic constraints ext	tension				

- d. [Add a new identity certificate] オプション ボタンをクリックします。
- 2. (オプション)新しいキーペアの作成

注:デフォルトでは、Default-RSA-Keyという名前とサイズが2048のRSAキーが使用 されますが、各ID証明書に一意の秘密キーと公開キーのペアを使用することをお勧め します。

a. Newをクリックして、新しいキーペアを生成します。

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
Add Identity (Certificate		X	General Purpose	RSA (4096 bits)	Show Detai
- Add Identity (General Purpose	RSA (2048 bits)	
Trustpoint Name	: SSL-Trustpoint					Delete
O Import the id	lentity certificate from a file ((PKCS12 format with Certificate(s	:)+Private Key):			Export
Decryption P	assphrase:					Install
File to Import	t From:	Browse				Re-Enrol
Add a new id	lentity certificate:					
Key Pair:	<default-rsa-< td=""><td>Key> v Show</td><td>New</td><td></td><td></td><td></td></default-rsa-<>	Key> v Show	New			
Certificate Su	ubject DN: CN=asavpn.ex	ample.com Select				
Generate	e self-signed certificate					
Act a	s local certificate authority a	nd issue dynamic certificates to T	LS-Proxy			
			Advanced			
Enable C	A flag in basic constraints ex	tension				
	Add Certificate	Cancel	Help			

- b. Enter new Key Pair nameオプションを選択し、新しいキーペアの名前を入力します。
- c. [キータイプ(Key Type)] に RSA または ECDSA を選択します。
- d. Key Sizeを選択し、RSAの場合はGeneral purpose for Usageを選択します。
- e. [Generate Now] をクリックします。これでキーペアが作成されます。

sued To	Issued By	Expiry Date	Associated Trustpoir	nts	Usage	Public Key Type	Add
🧧 Add Identity Certi	ficate			×	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)	Show Deta
Trustpoint Name:	SSL-Trustpoint						Delete
🔿 Impor 🔂 Add	Key Pair		×				Export
Decry			DDCA				Install
File to	pe: () RSA	O'ECDSA O'E	DUSA				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	e O Special	5				
				-			
				-			
□ En	Generate Now	Cancel	Help				
□ Er	Generate Now	Cancel	Help				

3. キーペア名の選択

CSRに署名し、新しい証明書にバインドするキーペアを選択します。

ssued To	Issued By	Expiry Date	Associated Trustpoints		Usage	Public Key Type	Add
📴 Add Identity Ce	ertificate		1	×	General Purpose General Purpose	RSA (4096 bits) RSA (2048 bits)	Show Detai
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the ide	ntity certificate from a file	(PKCS 12 format with Certificate)	(s) +Private Key):				Export
Decryption Pas	ssphrase:						Install
File to Import F	From:	Browse.					Re-Enrol
Add a new ide	ntity certificate:						
Key Pair:	SSL-Keypair	Show	. New				
Certificate Sub	oject DN: CN=asavpn.ex	ample.com Select	•				
Generate s	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					
				- 84			
	Add Certificate	Cancel	Help				

4. 証明書のサブジェクトと完全修飾ドメイン名(FQDN)の設定

注意:FQDNパラメータは、ID証明書が使用されるASAインターフェイスのFQDNまた はIPアドレスと一致する必要があります。このパラメーターは、ID証明書に対して要 求されたサブジェクト代替名(SAN)拡張を設定します。SAN拡張は、証明書が接続先 のFQDNと一致するかどうかを確認するためにSSL/TLS/IKEv2クライアントによって 使用されます。

a. [Select] をクリックします。

							Add	
					×		Show Detail	
SL-Trustpoint							Delete	
te from a file (PKCS12 for	rmat with Certificate(s) +Priva	te Key):					Export	
							Install	
	Browse						Re-Enrol	
te:								
SL-Keypair	V Show	New						
N=asavpn.example.com	Select							
ertificate								
te authority and issue dy	namic certificates to TLS-Prox	У						
	Adv	anced						
constraints extension								
	SL-Trustpoint te from a file (PKCS12 for te: SL-Keypair N=asavpn.example.com rtificate te authority and issue dy constraints extension	SL-Trustpoint te from a file (PKCS 12 format with Certificate(s) +Prival Browse te: SL-Keypair Show N=asavpn.example.com Select rtificate te authority and issue dynamic certificates to TLS-Prox Add constraints extension	SL-Trustpoint te from a file (PKCS12 format with Certificate(s) +Private Key): Browse Browse Essume State St	SL-Trustpoint te from a file (PKCS 12 format with Certificate(s) +Private Key): Browse Browse te: SL-Keypair Show New N=asavpn.example.com Select rtificate te authority and issue dynamic certificates to TLS-Proxy Advanced	SL-Trustpoint te from a file (PKCS12 format with Certificate(s) +Private Key): Browse Browse Es: SL-Keypair Show New N=asavpn.example.com Select rtificate te authority and issue dynamic certificates to TLS-Proxy Advanced constraints extension	SL-Trustpoint te from a file (PKCS 12 format with Certificate(s) +Private Key): Browse te: SL-Keypair Show New N=asavpn.example.com Select rtificate te authority and issue dynamic certificates to TLS-Proxy Advanced constraints extension	SL-Trustpoint te from a file (PKCS12 format with Certificate(s) +Private Key): Browse te: SL-Keypair Show New N=asavpn.example.com Select rtificate te authority and issue dynamic certificates to TLS-Proxy Advanced constraints extension	

b. Certificate Subject DNウィンドウで、certificate attributes - choose attribute fromドロ ップダウンリストを設定し、値を入力して、Addをクリックします。

sued To	Issued By	Expiry Date	Associated Trustpoints	^1 Us	age	Public Key Type	Add
Add Identity Certificat	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	Value			Re-Enroll
Add a new identity certain the second sec	DN Attribute to be	e Added					
Key Pair:	Attribute: Com	mon Name (CN) 🗸	Add>>				
Certificate Subject DN	Value: asa.	vpn.example.com	Delete				
Generate self-sign							
Act as local ce					_		
Enable CA flag in t		ОК	Cancel Help		_		

issued To	Issued By	Expiry Date	Associated Trustpoi	nts ^1 Usage	Public Key Type	Add
Add Identity Certifie	ate				×	Show Details
Trustpoint Name:	SSL-Trustpoint					Delete
Import the identity						Export
Decryption Passphr	asi	ect DN		^		Install
File to Import From			Attribute	Value		Re-Enroll
Add a new identity	CEL DN Attribute t	o he Added	Common Na	ame (CN) asa.vpn.exam		
Key Pair:	Attribute:	Country (C) v	Add>>			
Certificate Subject	DN Value:	common Name (CN)	Delete			
Generate self-s	ion	company Name (O)				
Act as local	S	ountry (C) tate (St)				
Accusiocal	L F	ocation (L) mail Address (FA)				
	E	OK	Cancel Help			
Enable CA flag	in t					
		Add Certificate	Cancel H	elp		

Attribute	説明
CN	ファイアウォールへのアクセスに使用される名前(通常は、
	vpn.example.comなどの完全修飾ドメイン名)。
OU	組織内の部署の名前
0	法的に登録されている組織/会社の名前
С	国コード(句読点のない 2 文字のコード)
ST	組織の所在する都道府県。
起	組織が所在する市区町村。
EA	電子メールアドレス

注:上記のフィールドの値はいずれも、64文字の制限を超えることはできません。この値を大きくすると、ID証明書のインストールで問題が発生する可能性があります。また、すべてのDN属性を定義する必要はありません。

すべての属性を追加したら、OKをクリックします。 c. デバイスのFQDNを設定し、Advancedをクリックします。

ssued To	Issued By	Expiry D	ate	Associated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Certificate							×	Show Detai
Trustpoint Name:	SSL-Trustpoint							Delete
○ Import the identity cert	ificate from a file (PKC	S12 format with	Certificate(s)+Pri	vate Kev):				Export
Decryption Passphrase:								Install
File to Import From:			Browse					Re-Enrol
Add a new identity cert	ificate:							
Key Pair:	SSL-Keypair	~	Show	New				
Certificate Subject DN:	CN=asa.vpn.exam	ple.com	Select					
Generate self-signe	d certificate							
Act as local cert	ificate authority and i	ssue dynamic ce	rtificates to TLS-Pr	оху				
				Idvanced				
Enable CA flag in ba	asic constraints exten	sion						
		-			_			

d. FQDNフィールドに、デバイスがインターネットからアクセス可能な完全修飾ドメイ ン名を入力します。[OK] をクリックします。

ssued To	Issund Bu	Euroisu Data	Associated Trustasiate	A 1 16000	Public Key Type	Add
Add Identity Ce	ertificate Advanced	Options		×	×	Show Detai
Touche sink Name	Enrolment mod	le parameters and SCEP challe	enge password are not available for s	elf-signed certificates.		Delete
Trustpoint Name:	Certificate Pa	rameters Enrollment Mode	SCEP Challenge Password			Export
	FODN:	asavpn.example.com				Install
Decryption Pas	E-mail:					Re-Enrol
File to Import F	-rom: IP Address:					
Add a new iden	ntity certifica	serial number of the device				
Key Pair:	s					
Certificate Subj	ject DN: C					
Generate s	self-signed ce					
Act as l	local certifica					
Enable CA 1	flag in basic (
	20		Cancel			

5. CSRの生成と保存

a. [証明書の追加(Add Certificate)] をクリックします。

Juca To	Issued By	Expiry D	ate	Associated Trustpoi	nts ^1	Usage	Public Key Type	Add
Add Identity Certificate							×	Show Detai
Trustpoint Name:	SSL-Trustpoint							Delete
Import the identity cert	tificate from a file (PKC	S12 format with	Certificate(s)+Pri	vate Kev).				Export
Decryption Passphrase	:			in the recy ju				Install
File to Import From:			Browse					Re-Enrol
Add a new identity cert	tificate:							
Key Pair:	SSL-Keypair	~	Show	New				
Certificate Subject DN:	CN=asa.vpn.examp	ole.com	Select					
Generate self-signe	ed certificate							
Act as local cer	tificate authority and is	sue dynamic ce	rtificates to TLS-Pr	оху				
				Advanced				
Enable CA flag in b	asic constraints extens	ion						

b. CSR をローカル マシン上のファイルに保存するためのプロンプトが表示されます。

ssued To	Issued By	Expiry Date	Associated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Certi	ficate					×	Show Details
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the identit	ty certificate from a file (PKC	S12 format with Certificate(s)+Private Key):				Export
Decryption Passp	hrase:				-		Install
File to Import Fro	m: 🔁 Ide	entity Certificate Request		×			Re-Enroll
Add a new identities	ty certificate: To concerning to concerning the termination of terminatio	omplete the enrollment proce lest (CSR) and send it to the	ss, please save the PKCS10 enrollme CA.	nt			
Key Pair:	SSL-Keypa You	will then need to install the o	ertificate that is returned from the C	by			
Certificate Subject	ct DN: CN=asa.vp clicki	ing the Install button in the Io	lentity Certificates panel.				
Generate self	f-signed certificate Save	e CSR to File:	Bro	wse			
Act as loc	al certificate author	ОК	Cancel Help				
		200	Advanced				
Enable CA fla	g in basic constraints extensi	ion					
		Add Contribution	Coursel Units				

[Browse] をクリックし、CSR を保存する場所を選択し、.txt 拡張子を付けてファイル を保存します。

注:ファイルを.txt拡張子で保存すると、PKCS#10要求をテキストエディタ(メ モ帳など)で開いて表示できます。

c. 新しいトラストポイントがPending状態で表示されます。

figuration > Device M	lanagement > Certifi	<u>cate Management</u> > <u>Iden</u>	tity Certificates			
Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
asa.vpn.example.com]	Not Available	Pending	SSL-Trustpoint	Unknown		Show Details
						Delete
						Export
						Install
						Re-Enroll

ASDMを使用したPEM形式でのID証明書のインストール

インストール手順では、CAがCSRに署名し、PEMエンコード(.pem、.cer、.crt)のID証明書と CA証明書バンドルが提供されていることを前提としています。

- 1. CSRに署名したCA証明書のインストール
 - a. Configuration > Device Management > Certificate Management >の順に移動し、CA Certificatesを選択します。[Add] をクリックします。

<u>_</u>	onfiguration > Remote Acc	ess VPN > Certificate Mana	igement > <u>CA Certificates</u>				
	A.						
	Issued To	Issued By	Expiry Date	Associated Trustpoints	¹ 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	Lever C

b. トラストポイント名を入力してInstall From Fileを選択し、Browseボタンをクリックし て中間証明書を選択します。または、テキストファイルのPEMエンコードCA証明書を テキストフィールドに貼り付けます。

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				
Paste certificate in	PEM format:					

注:CSRに署名したCA証明書をインストールし、ID証明書と同じトラストポイン ト名を使用します。PKI階層の上位にあるその他のCA証明書は、別々のトラスト ポイントにインストールできます。 c. [Install Certificate] をクリックします。

denTrust Commercial Roo JuoVadis Root CA 2		Expiry Date	Associated Trustpoints ^1	Usage	Active	Add
uoVadis Root CA 2	ot CN=IdenTrust Commercial .	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Edit
	CN=QuoVadis Root CA 2,	. 19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	Lor
Install Certificate					×	Show Details
Trustopiot Name:	SSI -Trustmoint					Request CRI
Install from a file:		Browse				Delete
Paste certificate in	PEM format:	0101100111				
9tLFV52U47em9u) cGqeyDMRhs3Rs/ z9kqaRijxs153jV/ 0jRyjalH56BFladd gW8YnHOvM08sv dcVcovOi/PAxnrAl	IaMA06CSqGSIb30QEBCvUAA4E ND25M2vKAF4AY2HgN9gK9VCK+ UKE90A1aTaA/fQfkKy LX7RddfVXfB9FBFh ICXRJfQUCAAY460 J+Ng2yWFN3MXWZO- XTE	BAQArsXII:wK3JII:BWOSYN5mgT ModKMQ2y4X/uhj6SNDU70Ff6f Evident Enutron Control of SNDU70Ff6f Evident Enutron Control of SNDU70Ff6f Evident Enutron Control of SNDU70Ff6f Please wait while ASDM is delive device	Information	following attributes: 3424c 6e7e0c5f b30b4	x	
O Use EST: Specify source Inte	erface: None		ringerprinte estatione zor			
Use EST: Specify source Intr EST URL: https:// Certificate Subject	erface: None DN: CN=risavpn31		Trustpoint CA certificate a	ccepted.		
Use EST: Specify source Intr EST URL: https:// Certificate Subject allow-untruster Use SCEP:	erface: None DN: CN=risavpn31 d-connection		Trustpoint CA certificate a	ccepted. K		
Use EST: Specify source Int EST URL: https:// Certificate Subject allow-untrustee Use SCEP: Specify source Into	erface: None DN: CN=risavpn31 d-connection rface: None		Trustpoint CA certificate a	ccepted.		
Use EST: Specify source Int EST URL: https:// Certificate Subject allow-untruste Use SCEP: Specify source Int SCEP URL: http://	erface: None DN: CN=risavpn31 d-connection xrface: None		Trustpoint CA certificate a	ccepted. K		
Use EST: Specify source Into EST URL: https:// Certificate Subject allow-untrustee Use SCEP:	erface: None DN: CN=risavpn31		Trustpoint CA certificate a	ccepted. K		

2. ID 証明書のインストール

o

a. CSRの生成中に以前に作成したID証明書を選択します。[INSTALL] をクリックします

quiation > Keniote	AC	cess VPN > Certificate Ma	anagement > <u>Identity Cert</u>	<u>ficates</u>			
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
							Delete
							Export
							Install
	sued To	sued To ^i n.example.com]	sued To ^1 Issued By m.example.com Not Available	sued To ^1 Issued By Expiry Date n.example.com) Not Available Pending	sued To ^1 Issued By Expiry Date Associated Trustpoints n.example.com Not Available Pending SSL-Trustpoint	sued To ^1 Issued By Expiry Date Associated Trustpoints Usage In.example.com Not Available Pending SSL-Trustpoint Unknown	sued To ^1 Issued By Expiry Date Associated Trustpoints Usage Public Key Type n.example.com) Not Available Pending SSL-Trustpoint Unknown

注:ID証明書では、Issued ByフィールドをNot available、Expiry Dateフィールド をPendingにすることができます。

b. CAから受信したPEMでエンコードされたID証明書を含むファイルを選択するか、 PEMでエンコードされた証明書をテキストエディタで開き、CAから提供されたID証明 書をコピーしてテキストフィールドに貼り付けます。

ued To	^1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
n.example.com]		Not Available	Pending	SSL-Trustpoint	Unknown		Show Detail
Lastall Islanda				~	General Purpose	RSA (2048 bits)	
Install identity	certifica	ite		tpoint	General Purpose	RSA (2048 bits)	Delete
entity Certificate							Export
Install from a	file:			Browse			Install
 Install from a Paste the cer 	file:	ata in base-64 forma	t:	Browse			Install Re-Enroll
Install from a Paste the cer	file:	ata in base-64 forma	t:	Browse			Install Re-Enroll
Install from a Paste the cer	file:	ata in base-64 forma	t:	Browse			Install Re-Enroll
Install from a Paste the cer	file: tificate d	ata in base-64 forma	tı	Browse			Install Re-Enroll
Install from a Paste the cer	file: tificate d	ata in base-64 forma	t	Browse			Instal Re-Enroll

注:ID証明書は、.pem、.cer、.crt形式でインストールできます。

c. [Install Certificate] をクリックします。

		Haaddated Traaqpointa	Usage	Public Key Type	Auu
pn.example.com] Not Availal	ble Pending	SSL-Trustpoint	Unknown		Show Detail
			General Purpose	RSA (2048 bits)	Show Detail
Install Identity certificate		tpoint	General Purpose	RSA (2048 bits)	Delete
dentity Certificate	Please wait	×			Export
Install from a file:		Information	×		Install
Paste the certificate data in be [InNBJ26XgDmVuQjfBEMVxR2K Gyer3x2GKML7MAIHBptyMcHD TSy9Yia2poqMnamQkaQpcKAF KdNqiFbUr6VWSNTuF2DowH3 END CERTIFICATE	device	dervering the L ₂	port succeeded.		Re-Enroll

3. ASDMを使用したインターフェイスへの新しい証明書のバインド

指定されたインターフェイスで終端するWebVPNセッションに新しいID証明書を使用する ようにASAを設定する必要があります。

- a. [構成(Configuration)] > [リモートアクセスVPN(Remote Access VPN)] > [詳細 (Advanced)] > [SSL設定(SSL Settings)] の順に移動します。
- b. [証明書(Certificates)] で、WebVPN セッションの終端に使用されるインターフェイ スを選択します。この例では、外部インターフェイスが使用されています。

[Edit] をクリックします。

c. [証明書(Certificate)] ドロップダウン リストで、新しくインストールした証明書を 選択します。

				Delete
i i i i i i i i i i i i i i i i i i i	elect SSL Certificate	×		
Spec OUT: Man	fy enrolled trustpoints to be used for SSL authentication and VPN load balancing on the IDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate onement > Identity Certificates.			
ertificates				
Specify which certificates, if an Prime	rv Enrolled Certificate: SSL-Trustpoint:unstructuredName =asavon.exampl	~	tes not associated with a certificate of their own.	
Interface	Balancing Enrolled Certificate: None		Кеу-Туре	Edit
OUTSIDE-direct	balancing childred certaincates	~		
inside	OK Cancel Help			
management				

- d. [OK] をクリックします。
- e. [APPLY] をクリックします。

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

これで、新しいID証明書が使用されています。

ASDMを使用したPKCS12形式で受信したID証明書のインストール

PKCS12ファイル(.p12または.pfx形式)には、ID証明書、キーペア、およびCA証明書が含まれています。これは、CAによって作成されます(ワイルドカード証明書の場合など)。または、別のデバイスからエクスポートされます。これはバイナリファイルであり、テキストエディタで表示することはできません。

1. PKCS12ファイルからのID証明書とCA証明書のインストール

ID証明書、CA証明書、およびキーペアを1つのPKCS12ファイルにバンドルする必要があります。

- a. Configuration > Device Management > Certificate Managementの順に移動し、Identity Certificatesを選択します。
- b. [Add] をクリックします。
- c. トラストポイント名を指定します。

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
🔤 Add Identity Certifi	cate		×			Delete
Trustpoint Name:	SSL-Trustpoint-PK	CS12				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				
O Add a new identity	certificate:					
Key Pair:	<default-rsa-ke< td=""><td>y> v Show</td><td>New</td><td></td><td></td><td></td></default-rsa-ke<>	y> v Show	New			
Certificate Subject	DN: CN=risavpn31	Select				
Generate self-s	signed certificate					
Act as local	certificate authority and	issue dynamic certificates to TL	.S-Proxy			
			Advanced			
NEnable CA flag	in basic constraints exter	nsion				
- Super cring						

d. [アイデンティティ証明書をファイルからインポートする(Import the identity certificate from a file)] ラジオ ボタンをクリックします。

Add Identity Certificate SSL-Trustpoint-PKCS12 Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):	ID certificate file
Add Identity Certificate Trustpoint Name: SSL-Trustpoint PKCS12 (e) Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):	ID certificate file
Trustpoint Name: SSL-Trustpoint-PKCS12 SSL-Trustpoint-PKCS12 Lc	ID certificate file
Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):	
	ok in: 🗄 Documents 🗸 🤌 😰 🖽 🗸
Decryption Passohrase:	CSR.txt
File to Import From: Browse Recent It	wpn.example.com.pfx
Add a new identity certificate:	
Key Pair: <default-rsa-key> Show New Desktop</default-rsa-key>	
Certificate Subject DN: CN=risavpn31 Select	
Generate self-signed certificate	ts
Act as local certificate authority and issue dynamic certificates to TLS-Proxy	
This PC	File name: vpn.example.com.pfx Import ID certificate file
Advanced	Files of type: All Files V Cancel

e. PKCS12 ファイルの作成に使用するパスフレーズを入力します。

ssued To	Issued By	Expiry Da	te	Associated Trustpoints	Usage	Public Key Type	Add
							Show Detail
Add Identity Certif	icate			×			Delete
Trustpoint Name:	SSL-Trustpoint-PK	CS12					Export
 Import the identity 	y certificate from a file (PK	CS12 format with	Certificate(s)+Pr	ivate Key):			Install
Decryption Passph	rase: ••••						Re-Enroll
File to Import From	n: C:\Users\cisco.DE	SKTOP-R2CH8G	Browse				
O Add a new identity	y certificate:						
Key Pair:	<default-rsa-ke< td=""><td>γ> ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-ke<>	γ> ~	Show	New			
Certificate Subject	t DN: CN=risavpn31		Select				
Generate self-	signed certificate						
Act as loca	al certificate authority and	l issue dynamic cer	tificates to TLS-P	roxy			
				Advanced			
Enable CA flag	in hasic constraints exter	nsion					
	in busic constraints exter						

f. [証明書の追加(Add Certificate)] をクリックします。

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
		,				Show Details
🔁 Add Identity C	Certificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-	PKCS12				Export
Import the id	entity certificate from a file (PKCS12 format with Certificate(s)+Private Key):			Install
Decryption Pa	assphrase: ••••					Re-Enroll
File to Import	From: C:\Users\cisco.0	DESKTOP-R2CH8G Browse.				
🔿 Add 🛅 Pl	ease wait		Information			×
Cert	Please wait while ASDM device	is delivering the command(s) to	the Created trustpoint WARNING: CA cer the validation-usage	s for CAs higher in the hie lificates can be used to va le of this trustpoint to limi	erarchy as the CA certificate was not s alidate VPN connections,by default. Pli It the validation scope, if necessary	ease adjust
Enable C/	A flag in basic constraints ext	tension	Import PKCS 12 opt	eration completed success	sfully.	

注:CA証明書チェーンを含むPKCS12をインポートすると、ASDMは追加された – numberサフィックスを持つ名前でアップストリームCAトラストポイントを自 動的に作成します。

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. ASDMを使用したインターフェイスへの新しい証明書のバインド

指定されたインターフェイスで終端するWebVPNセッションに新しいID証明書を使用する ようにASAを設定する必要があります。

a. [構成(Configuration)] > [リモートアクセスVPN(Remote Access VPN)] > [詳細

(Advanced)] > [SSL設定(SSL Settings)]の順に移動します。

b. [証明書(Certificates)] で、WebVPN セッションの終端に使用されるインターフェイ スを選択します。この例では、外部インターフェイスが使用されています。

[Edit] をクリックします。

c. [証明書(Certificate)] ドロップダウン リストで、新しくインストールした証明書を 選択します。

Domon	OF PROVE	
tificates pecify which certificates, if ar Interface OUTSIDE-direct inside inside-vlan management	Select SSL Certificate X Specify errolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To erroll a trustpoint, go to Device Management > Certificate Management > Identity Certificates. Interface: OUTSIDE-direct Primary Enrolled Certificate: SSL-Trustpoint-PKCS 12:unstructuredName =FTD72-ek, u ✓ Load Balancing Enrolled Certificate:None OK Cancel Help	heir own.
allback Certificate:	tion Timeout:	

- d. [OK] をクリックします。
- e. [APPLY] をクリックします。

Certi Sp	ificates ecify 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	

これで、新しいID証明書が使用されています。

証明書の更新

ASDMを使用した証明書署名要求(CSR)に登録された証明書の更 新

CSRに登録された証明書の証明書の更新では、新しいトラストポイントを作成して登録する必要 があります。別の名前(登録年のサフィックスを持つ古い名前など)にする必要があります。古 い証明書と同じパラメータとキーペアを使用することも、異なるパラメータとキーペアを使用す ることもできます。

ASDMを使用したCSRの生成

- 1. 特定の名前で新しいトラストポイントを作成します。
 - a. Configuration > Device Management > Certificate Management > Identity Certificatesの順に移動します。

File View Tools Wizards Wind	dow	Help	Back O Fo	rward ? Help	tificator		Type topic	to search	Go	cisco
Anagement Access Solution		Issued To	∧1	Issued By	Expiry Date	Associated Trustpoints	Usage General Purnose	Public Key Type		Add
High Availability and Scalability 		unst de la containeasa. e xam	Second Cash Soon	Junisu uctur currante =asa.exanipie	15.05.05 CEDT 54 1		dene ar Porpose	K3A (2010 013)		Show Details Delete
Cloud Web Security										Export Install
Certificate Management Certificates CA Certificates										Re-Enroll

- b. [Add] をクリックします。
- c. トラストポイント名を定義します。

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 Detail
Add Identity Certificate						×	Delete
Trustpoint Name:	ASDM_TrustPoint0						Export
 Import the identity certif 	ficate from a file (PKC	S12 format with Certificate(s)+Priva	te Key):				Install
Decryption Passphrase:							Re-Enrol
File to Import From:		Browse					11
O Add a new identity certif	ficate:						
Key Pair:	<default-rsa-key< td=""><td>> V Show</td><td>New</td><td></td><td></td><td></td><td></td></default-rsa-key<>	> V Show	New				
Certificate Subject DN:	CN=risavpn31	Select					
Generate self-signed	l certificate						
Act as local certif	ficate authority and is	sue dynamic certificates to TLS-Prox	У			1	
		Adv	anced				
Enable CA flag in bas	sic constraints extens	ion					

- d. [Add a new identity certificate] オプション ボタンをクリックします。
- 2. (オプション)新しいキーペアの作成

注:デフォルトでは、Default-RSA-Keyという名前とサイズが2048のRSAキーが使用 されますが、各ID証明書に一意の秘密キーと公開キーのペアを使用することをお勧め します。

a. Newをクリックして、新しいキーペアを生成します。

sueu 10 155ueu	By Expiry Date			Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName= CN=ca.example.com		U 15:10:00 CEST Feb 6 2024		SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
Add Identity Certificate	2			×			Delete
Trustopint Name:	SSL-Trustpoint-202	23					Export
O Import the identity cer	tificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Passphrase	:						Re-Enroll
File to Import From:			Browse				
Add a new identity cer	tificate:						
Key Pair:	<default-rsa-key< td=""><td>/> ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-key<>	/> ~	Show	New			
Certificate Subject DN:	CN=asavpn.examp	ple.com	Select				
Generate self-sign	ed certificate						
Act as local cer	tificate authority and i	issue dynamic cer	tificates to TL	S-Proxy			
				Advanced			
Enable CA flag in b	asic constraints exten	ision					

- b. Enter new Key Pair nameオプションを選択し、新しいキーペアの名前を入力します。
- c. [キータイプ(Key Type)] に RSA または ECDSA を選択します。
- d. Key Sizeを選択します。RSAの場合は、UsageのGeneral purposeを選択します。
- e. [Generate Now] をクリックします。これでキーペアが作成されます。

isued To Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
structuredName= CN=ca.example.co	m, OU 15:10:00 CEST Feb 6 2024	4 SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
Add Identity Certificate		×			Delete
Trustpoint Name: SSL-Trus	tpoint-2023				Export
C 🔤 Add Key Pair		× _{Key):}			Install
Key Type: () RSA	⊖ ECDSA ⊖ EL	DDSA			Re-Enroll
Name: O Use default key p	pair name				
Enter new key p	air name: SSL-KeyPair-2023	ew			
Size: 4096	✓ Special				
	Objection				
Generate Now	Cancel Help	ced			

3. キーペア名の選択

CSRに署名し、新しい証明書にバインドするキーペアを選択します。

ssued To Issue	ed To Issued By ucturedName= CN=ca.example.com, OU			Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName= CN=c			eb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🝯 Add Identity Certificat	te			×			Delete
Trustpoint Name:	rustpoint Name: SSL-Trustpoint-2023					Export	
 Import the identity ce 	rtificate from a file (PK	CS12 format with C	Certificate(s)	+Private Key):			Install
Decryption Passphras	e:						Re-Enrol
File to Import From:			Browse				
Add a new identity ce	rtificate:						
Key Pair:	SSL-KeyPair-2023	~	Show	New			
Certificate Subject DN	I: CN=asavpn.exam	ple.com	Select				
Generate self-sign	ned certificate						
Act as local ce	rtificate aut grity and	issue dynamic certi	ficates to TL	S-Proxy			
				Advanced			
Enable CA flag in l	basic constraints exter	nsion					

4. 証明書のサブジェクトと完全修飾ドメイン名(FQDN)の設定

注意:FQDNパラメータは、証明書が使用されるASAインターフェイスのFQDNまたは IPアドレスと一致する必要があります。このパラメーターは、証明書のサブジェクト 代替名(SAN)を設定します。SANフィールドは、証明書が接続先のFQDNと一致する かどうかを確認するためにSSL/TLS/IKEv2クライアントによって使用されます。

注:CAは、CSRに署名して署名付きID証明書を作成するときに、トラストポイントで 定義されているFQDNパラメータとサブジェクト名パラメータを変更できます。

a. [Select] をクリックします。

Issued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Typ	e Add
nstructuredName=.	CN=ca.example.com, OU	15:10:00 CEST	ST Feb 6 2024 SSL-Trustpoint		General Purpose	ose RSA (2048 bits)	Show Detail
🔄 Add Identity C	Certificate			×			Delete
Trustpoint Name:	Trustpoint Name: SSL-Trustpoint-2023					Export	
O Import the id	entity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Pa	assphrase:						Re-Enroll
File to Import	From:		Browse	r I.			
Add a new id	entity certificate:			_			
Key Pair:	SSL-KeyPair-2023	3 v	Show	New			
Certificate Su	bject DN: CN=asavpn.exam	nple.com	Select				
Generate	self-signed certificate						
Act as	s local certificate authority and	issue dynamic cer	tificates to TL	S-Proxy			
				Advanted			
				Auvanceu			
Enable C/	A flag in basic constraints exter	nsion					

b. Certificate Subject DNウィンドウで、certificate attributes - select attribute fromドロッ プダウンリストを設定し、値を入力して、Addをクリックします。

ssued To	Issued By	Expiry (Date	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName=	CN=ca.example.com,	=ca.example.com, OU 15:10:00 CEST Feb 6 2		SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
📴 Add Identity	Certificate			×			Delete
Trustpoint Name	: SSL-Trustpo	int-2023					Export
ertificate Subject	DN			;	<		Install
			_				Re-Enroll
			Attribute	Value			
DN Attribute to be Attribute: Cou	e Added	Add>>	Company Name (O	example inc			
Value: US		Delete					
	ОК	Cancel	Help				
	A flag in basic constraints	extension					

Attribute	説明
CN	ファイアウォールへのアクセスに使用される名前(通常は、 vpn.example.comなどの完全修飾ドメイン名)。
OU	組織内の部署の名前
0	法的に登録されている組織/会社の名前
С	国コード(句読点のない 2 文字のコード)
ST	組織の所在する都道府県。
起	組織が所在する市区町村。
EA	電子メールアドレス

注:上記のフィールドはいずれも、64文字の制限を超えることはできません。 この値を大きくすると、ID証明書のインストールで問題が発生する可能性があり ます。また、すべてのDN属性を定義する必要はありません。

すべての属性を追加したら、OKをクリックします。 c. デバイスのFQDNを設定するには、Advancedをクリックします。

sued To Issu	ed 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 Certifica	te			×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
O Import the identity of	ertificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Passphra	se:						Re-Enroll
File to Import From:			Browse				
Add a new identity of	ertificate:						
Key Pair:	SSL-KeyPair-2023	۶ v	Show	New			
Certificate Subject D	N: /pn.example.com,	,0=example inc	Select				
Generate self-sig	ned certificate						
Act as local c	ertificate authority and	issue dynamic ce	tificates to TL	S-Proxy			
			- T	Advanced			
Enable CA flag in	basic constraints exter	nsion					

d. FQDNフィールドに、デバイスがインターネットからアクセス可能な完全修飾ドメイ ン名を入力します。[OK] をクリックします。

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
Advanced (Ontions	DU IS-10-00 CERTISAN 6-2	N24 SSI Trustociat	General Purpose	RSA (2048 bits)	Show Details
Auvanceu (~			Delete
Certificate Para	parameters and SCEP cha	allenge password are not availabl	e for self-signed certificates.			Export
	Entoiment hour	Seer challenge rassiford				Install
FQDN:	asavpn.example.com					Re-Enrol
E-mail:						
IP Address:						
Include se	rial number of the device					
		C2				
			_			

- 5. CSRの生成と保存
 - a. [証明書の追加(Add Certificate)] をクリックします。

Issued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName=	. CN=ca.example.com, OU	15:10:00 CEST	Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🔄 Add Identity Co	ertificate			×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
O Import the ide	entity certificate from a file (PF	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption Pa	ssphrase:						Re-Enroll
File to Import	From:		Browse				
Add a new ide	entity certificate:						
Key Pair:	SSL-KeyPair-2023	3 v	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 ce	rtificates to TL	S-Proxy			
				Advanced			
	0			Advanceu			
	nag in basic constraints exte	rision					

b. CSR をローカル マシン上のファイルに保存するためのプロンプトが表示されます。

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 Detai
🧧 Add Identi	ty Certificate		×			Delete
Trustopiot N	ame: SSI -Trustoo	int-2023				Export
O Import th	e identity certificate from a f	ile (PKCS12 format with Certifica	ate(s)+Private Key):			Install
1 🕞 🖬	antity Cartificate Request		×			Re-Enroll
K You did	will then need to install the o ing the Install button in the I e CSR to File: C:\Users\cisco	entificate that is returned from t dentity Certificates panel.	Browse			
[Sav						
[Sav	ОК	Cancel Help	Advanced			
[Sav	OK le CA flag in basic constraints	Cancel Help	Advanced			

[Browse] をクリックします。 CSRを保存する場所を選択し、.txt拡張子を付けてファ イルを保存します。

注:ファイルを.txt拡張子で保存すると、PKCS#10要求をテキストエディタ(メ モ帳など)で開いて表示できます。

c. 新しいトラストポイントがPending状態で表示されます。

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
isavpn.example.com	1] Not Available	Pending	SSL-Trustpoint-2023	Unknown		
						Delete
						Export
						Install
						Re-Enrol

ASDMを使用したPEM形式でのID証明書のインストール

インストール手順では、CAがCSRに署名し、PEMエンコード(.pem、.cer、.crt)された新しい ID証明書およびCA証明書バンドルが提供されていることを前提としています。

1. CSRに署名したCA証明書のインストール

0

ID証明書に署名したCA証明書は、ID証明書用に作成されたトラストポイントにインストー ルできます。ID証明書が中間CAによって署名されている場合、このCA証明書をID証明書ト ラストポイントにインストールできます。階層内のアップストリームのすべてのCA証明書 は、個別のCAトラストポイントにインストールできます。

a. Configuration > Device Management >Certificate Management >の順に移動し、CA Certificatesを選択します。[Add] をクリックします。

Issued To	Issued By ^1	Expiry Date	Associated Trustpoints	Usage	Active	Add
ca.example.com	CN=ca.example.com, OU=I	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	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	Lonc
denTrust Commercial Root	CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Show Detai

b. トラストポイント名を入力し、Install From Fileを選択して、Browseボタンをクリック し、intermediate証明書を選択します。または、テキストファイルのPEMエンコード CA証明書をテキストフィールドに貼り付けます。

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	2					X	Show Detai
Trustpoint Name:	SSL-Trustpoint-2023						Request CF
 Install from a fil 	e:	Browse					Delete
	o in DEM formati						

注:ID証明書が中間CA証明書によって署名されている場合は、ID証明書のトラス トポイント名と同じトラストポイント名を持つ中間証明書をインストールします c. [Install Certificate] をクリックします。

isued To Is	sued By	^1	Expiry Date	Associated Trustpoints	Usage	Active		Add
.example.com Cl	N=ca.example.com,	I=UC	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes		Edit
o Install Certificate							× Show	w Detail
Trustpoint Name: SSL-	Trustpoint-2023]				Requ	uest CR
O Install from a file:			Browse				D	elete
Paste certificate in PEM f	ormat:							
SkXvFik1Z1cZEGn6b2um ok5sE5pH23UqVXGiirp, Oj9xKv7CbPf3p32FdH7v VR00B8YEFE5s2sbra9 9tLFV52U47em9uXaMA0 cGqeyDMRhs3Rs/w025N 29kqaRijsx1533/v/Lk89 0jRvjaH56BFladkvC7Rc gkv8YnHOvM08vyTXSL dcVcovOj/PAxnrAJ3H0g2 END CERTIFICATE	IQaVZB LewIuTHOX momzxI4G/tel6eyMC u511KSprAgMBAAG; 99LFV5ZU47emSuXa GCSqGSI5130QEBCw 12wkAF4AYZHgN9gK AlatnA/fQfXSV+h7 Jf0UCdmAY+IG0gh Jf0UCdmAY+IG0gh JfWVZO453C	itäls3uxT pjpnVtD JDBOMA MB8GA1 JAA4IBA	PH8+B5QG0+d1waOsbCWk YYQ9HWkQdQTSLKwRaX wGA1UdEwQFMMBaR8wHQ UdIwQYWBaAFE55kZsbra9b AQAraXEwKSIINBwQsYh5mdT formation INFO: Certificate h Fingerprint: e9ad16	YD as the following attributes: 55c 2673424c 6e7e0c5f b30b4a02	×		•	
Specify source Interface	None		Trustpoint CA certif	ficate accepted.				
EST URL: https://								
Certificate Subject DN:	CN=risavpn31			ОК				
allow-untrusted-conn	ection	_	200					
O Use SCEP:								
Specify source Interface:	None		\sim					
SCEP URL: http://								
Retry Period:	1		minutes					

この例では、新しい証明書が古い証明書と同じCA証明書で署名されています。同じ CA証明書が2つのトラストポイントに関連付けられました。

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

- 2. ID 証明書のインストール
 - a. CSR生成で以前作成したID証明書を選択します。[INSTALL] をクリックします。

ce Management > Certific	ate Management > Identit	ty Certificates				
Issued By	Expiry Date	Associated Trustpoints	~ 1	Usage	Public Key Type	Add
. CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Details
ij inot Avaliable	Pending	SSL-Trustpoint-2023		Unknown		Delete
						Export
						Install
						Re-Enrol
	c Management > Certific Issued By . CN=ca.example.com, OU Not Available	ce Management > Certificate Management > Identificate	Issued By Expiry Date Associated Trustpoints . CN=ca.example.com, OU 15:10:00 CEST Feb 6 2024 SSL-Trustpoint Not Available Pending SSL-Trustpoint-2023	Issued By Expiry Date Associated Trustpoints 1 . CN=ca.example.com, OU 15: 10:00 CEST Feb 6 2024 SSL-Trustpoint 1 Not Available Pending SSL-Trustpoint-2023 1	Issued By Expiry Date Associated Trustpoints V1 Usage . CN=ca.example.com, OU 15:10:00 CEST Feb 6 2024 SSL-Trustpoint General Purpose Not Available Pending SSL-Trustpoint-2023 Unknown	Issued By Expiry Date Associated Trustpoints ¹ Usage Public Key Type . CN=ca.example.com, OU 15:10:00 CEST Feb 6 2024 SSL-Trustpoint General Purpose RSA (2048 bits)] Not Available Pending SSL-Trustpoint-2023 Unknown

注:ID証明書では、Issued ByフィールドをNot availableに、Expiry Dateフィール ドをPendingに設定できます。

b. CAから受信したPEMでエンコードされたID証明書を含むファイルを選択するか、

PEMでエンコードされた証明書をテキストエディタで開き、CAから提供されたID証明 書をテキストフィールドにコピーアンドペーストします。

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

注:ID証明書は、.pem、.cer、.crt形式でインストールできます。

c. [Install Certificate] をクリックします。

sued To	Issued By	Expiry Date	Associated Trustpoints	~1	Usage	Public Key Type	Add
structuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detai
avpn.example.comj	Not Available	Pending	SSL-Trustpoint-2023		Unknown		Delete
							Export
linstall Identity c	certificate		×				Install
Carlo Carlo							Re-Enrol
entity certificate –							
O In The Please	wait						1
In Please Pa	e wait	tion	×				
In Please Pa	e wait Please wait wł device	tion	×				
In Please Pe F	e wait Please wait wir device	tion Certificate import succeede	×				
In Please Pz Fz V V V	e wait Please wait wi device	tion Certificate import succeede	×				

インストール後、古いID証明書と新しいID証明書が存在します。

		ite Hanagement > Iterut	<u>y certificates</u>				
Issued To	Issued By	Expiry Date	Associated Trustpoints	v 1	Usage	Public Key Type	Add
unstructuredName=	CN=ca.example.com, OU	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023		General Purpose	RSA (4096 bits)	Show Details
unstructuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Details
							Delete
							Export
							Install
							Re-Enroll

3. ASDMを使用したインターフェイスへの新しい証明書のバインド

指定されたインターフェイスで終端するWebVPNセッションに新しいID証明書を使用する ようにASAを設定する必要があります。

a. [構成(Configuration)] > [リモートアクセスVPN(Remote Access VPN)] > [詳細 (Advanced)] > [SSL設定(SSL Settings)] の順に移動します。 b. [証明書(Certificates)] で、WebVPN セッションの終端に使用されるインターフェイ スを選択します。この例では、外部インターフェイスが使用されています。

[Edit] をクリックします。

c. [証明書(Certificate)] ドロップダウン リストで、新しくインストールした証明書を 選択します。

				Edit Delete
	Select SSL Certificate Specify enrolled trustpoints to be us	X		
rtificates Specify which certificates, if an	Management > Identity Certificates	outspont, go to bevice management > Cerunicate	res not associated with a certificate of their own.	
Interface	Primary Enrolled Certificate:	SSL-Trustpoint-2023:unstructuredName=asavpn.exampl v	Кеу-Туре	Edit
OUTSIDE-direct	Load Balancing Enrolled Certificate:	None 🗸	Primary: RSA (2048 bits), Load Balancing: n	
inside				
inside-vlan	OK	Cancel Help		
management				

- d. [OK] をクリックします。
- e. [APPLY] をクリックします。これで、新しいID証明書が使用されています。

				Edit
icates cify which certificates, if a Interface	ny, should be used for SSL authentication on ea Primary Certificate	ch interface. The fallback certificate will be us	sed on interfaces not associated with a certificate of their own Key-Type	n. Edit
icates cify which certificates, if a Interface	ny, should be used for SSL authentication on ea Primary Certificate	ch interface. The fallback certificate will be us	sed on interfaces not associated with a certificate of their own Key-Type Primary: RSA (4096 bits). Load Balancing: n.	n. Edit
icates crify which certificates, if a Interface OUTSIDE-direct naide	ny, should be used for SSL authentication on ea Primary Certificate SSL-Trustpoint-2023:unstructure.	ch 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.	n. Edit
icates cify which certificates, if a Interface DUTSIDE-direct nside nside-vian	ny, should be used for SSL authentication on ea Primary Certificate SSL-Trustpoint-2023:unstructure	ich 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.	n. Edit

ASDMを使用したPKCS12ファイルに登録された証明書の更新

PKCS12登録済み証明書の証明書の更新では、新しいトラストポイントを作成して登録する必要 があります。別の名前(登録年のサフィックスを持つ古い名前など)にする必要があります。

PKCS12ファイル(.p12または.pfx形式)には、ID証明書、キーペア、およびCA証明書が含まれ ています。これは、たとえばワイルドカード証明書の場合にCAによって作成されるか、または別 のデバイスからエクスポートされます。これはバイナリファイルであり、テキストエディタでは 表示できません。

1. PKCS12ファイルからの更新されたID証明書とCA証明書のインストール

ID証明書、CA証明書、およびキーペアを1つのPKCS12ファイルにバンドルする必要があり ます。

- a. Configuration > Device Management > Certificate Managementの順に移動し、Identity Certificatesを選択します。
- b. [Add] をクリックします。
- c. 新しいトラストポイント名を指定します。

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	assphrase:						Re-Enrol
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	local certificate authority a	nd issue dynamic ce	rtificates to TLS-F	Proxy			
				Advanced			
REnable C/	fag in basic constraints av	tension		AVUILLUIT			
L Stible C	a nag in basic constraints ex						
_							

d. [アイデンティティ証明書をファイルからインポートする(Import the identity certificate from a file)] ラジオ ボタンをクリックします。

Issued To	Issued By	Expiry D	ate	Associated	Trustpoints	Usage	Put	lic Key Type		Add
										Show Detail
📴 Add Identity Certi	ficate		L.	()	x					Delete
Trustpoint Name:	SSL-Trustpoint-F	KCS12			import ID certi	ficate file				
Import the identi	ty certificate from a file (F	PKCS12 format wit	h Certificate(s)+P	rivate Kev):	Look in:	Document	S	~	🥬 📂 🖽	•
Decryption Passp	hrase:				C.	CSR.txt				
File to Import Fro	m:		Browse		Recent Items	ypn.exan	ple.com.ptx			
O Add a new identi	ty certificate:									
Key Pair:	<default-rsa-k< td=""><td>ey> 🗸</td><td>Show</td><td>New</td><td>Desktop</td><td></td><td></td><td></td><td></td><td></td></default-rsa-k<>	ey> 🗸	Show	New	Desktop					
Certificate Subject	ct DN: CN=risavpn31		Select		4					
Generate self	f-signed certificate				Documents					
Act as loc	al certificate authority an	id issue dynamic c	ertificates to TLS-F	roxy						
				Advanced	This PC F	ile name:	vpn.example.com.p	fx	Import ID	certificate file
				Muvance0	i 🎒 F	Files of type:	All Files	~	C	ancel
Enable CA fla	g in basic constraints ext	ension			4					

e. PKCS12 ファイルの作成に使用するパスフレーズを入力します。

ssued To	Issued By	Expiry Da	te	Associated Trustpoints	Usage	Public Key Type	Add
							Show Detail
Add Identity Certif	icate			×			Delete
Trustpoint Name:	SSL-Trustpoint-PK	CS12					Export
 Import the identity 	y certificate from a file (PK	CS12 format with	Certificate(s)+Pr	ivate Key):			Install
Decryption Passph	rase: ••••						Re-Enroll
File to Import From	n: C:\Users\cisco.DE	SKTOP-R2CH8G	Browse				
O Add a new identity	y certificate:						
Key Pair:	<default-rsa-ke< td=""><td>γ> ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-ke<>	γ> ~	Show	New			
Certificate Subject	t DN: CN=risavpn31		Select				
Generate self-	signed certificate						
Act as loca	al certificate authority and	l issue dynamic cer	tificates to TLS-P	roxy			
				Advanced			
Enable CA flag	in hasic constraints exter	nsion		Novon CCO			
	in busic constraints exter						

f. [証明書の追加 (Add Certificate)] をクリックします。

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
		,				Show Details
🔁 Add Identity C	Certificate		×			Delete
Trustpoint Name:	SSL-Trustpoint-	PKCS12				Export
Import the id	entity certificate from a file (PKCS12 format with Certificate(s)+Private Key):			Install
Decryption Pa	assphrase: ••••					Re-Enroll
File to Import	From: C:\Users\cisco.0	DESKTOP-R2CH8G Browse.				
🔿 Add 🛅 Pl	ease wait		Information			×
Cert	Please wait while ASDM device	is delivering the command(s) to	the Created trustpoint WARNING: CA cer the validation-usage	s for CAs higher in the hie lificates can be used to va le of this trustpoint to limi	erarchy as the CA certificate was not s alidate VPN connections,by default. Pli It the validation scope, if necessary	ease adjust
Enable C/	A flag in basic constraints ext	tension	Import PKCS 12 opt	eration completed success	sfully.	

注:CA証明書チェーンを持つPKCS12がインポートされると、ASDMは、追加さ れた – numberサフィックスを持つ名前でアップストリームCAトラストポイント を自動的に作成します。

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. ASDMを使用したインターフェイスへの新しい証明書のバインド

指定されたインターフェイスで終端するWebVPNセッションに新しいID証明書を使用する ようにASAを設定する必要があります。

a. [構成(Configuration)] > [リモートアクセスVPN(Remote Access VPN)] > [詳細

(Advanced)] > [SSL設定(SSL Settings)]の順に移動します。

b. [証明書(Certificates)] で、WebVPN セッションの終端に使用されるインターフェイ スを選択します。この例では、外部インターフェイスが使用されています。

[Edit] をクリックします。

c. [証明書(Certificate)] ドロップダウン リストで、新しくインストールした証明書を 選択します。

Contain	OLE STRUCTURE	
ertificates Specify which certificates, if ar Interface OUTSIDE-direct inside inside-vlan management	Select SSL Certificate × edfy enrolled trustpoints to be used for SSL authentication and VPN load balancing on the ITSIDE-direct interface. To enroll a trustpoint, go to Device Management > Certificate nagement > Identity Certificates. terface: OUTSIDE-direct mary Enrolled Certificate: SSL-Trustpoint-PKCS 12:unstructuredName=FTD72-ek, u v CK Cancel Help	wn.
Fallback Certificate:	None V	

- d. [OK] をクリックします。
- e. [APPLY] をクリックします。

Certi Sp	ificates ecify which certificates, if any, should be	e 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 Key-Type					
	OUTSIDE-direct	SSL-Trustpoint-PKCS12:unstructuredName=F		Primary: RSA (2048 bits), Load Balan		

これで、新しいID証明書が使用されています。

確認

サードパーティベンダーの証明書が正常にインストールされたことを確認し、SSL VPN接続に使用するには、次の手順を使用します。

ASDM を使用してインストールされた証明書の表示

- [構成(Configuration)] > [リモートアクセスVPN(Remote Access VPN)] > [証明書の管理 (Certificate Management)]の順に移動して、[アイデンティティ証明書(Identity Certificates)]を選択します。
- 2. サードパーティベンダーによって発行されたID証明書が表示される場合があります。

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

トラブルシュート

このdebugコマンドは、SSL証明書のインストールが失敗した場合にCLIで収集されます。

· debug crypto ca 14

よく寄せられる質問(FAQ)

Q. PKCS12とは何ですか。

A.暗号化では、PKCS12は、多数の暗号化オブジェクトを1つのファイルとして保存するために作 成されるアーカイブファイル形式を定義します。通常、秘密キーをX.509証明書とバンドルした り、信頼のチェーンのすべてのメンバーをバンドルしたりするために使用されます。

Q. CSRとは何ですか。

A.Public Key Infrastructure (PKI;公開キーインフラストラクチャ)システムでは、証明書署名要 求(CSRまたは証明書要求)は、デジタルID証明書を申請するために申請者から公開キーインフ ラストラクチャの登録機関に送信されるメッセージです。通常は、証明書を発行できる公開キー 、署名付き証明書を識別するために使用される情報(サブジェクト内のドメイン名など)、およ び整合性の保護(デジタル署名など)が含まれます。

Q. PKCS12のパスワードはどこにありますか。

A.証明書とキーペアがPKCS12ファイルにエクスポートされる際に、パスワードはexportコマンド で指定されます。 pkcs12ファイルをインポートするには、CAサーバの所有者または別のデバイ スからPKCS12をエクスポートしたユーザがパスワードを提供する必要があります。

Q.ルートとアイデンティティの違いは何ですか。

A.暗号化とコンピュータセキュリティでは、ルート証明書はルート認証局(CA)を識別する公開キ ー証明書です。ルート証明書は自己署名され(証明書がクロス署名されたルートによって発行さ れたかなど、複数の信頼パスを持つことが可能です)、X.509ベースの公開キーインフラストラ クチャ(PKI)の基盤を形成します。公開鍵証明書は、デジタル証明書またはID証明書とも呼ばれ、 公開鍵の所有権を証明するために使用される電子文書です。証明書には、キーに関する情報、所 有者の身元に関する情報(サブジェクトと呼ばれます)、証明書の内容を検証したエンティティ のデジタル署名(発行者と呼ばれます)が含まれます。署名が有効で、証明書を検査するソフト ウェアが発行者を信頼する場合、そのキーを使用して証明書のサブジェクトと安全に通信できま す。

Q.証明書をインストールしましたが、なぜそれが機能しないのですか。 A.これは、次のようなさまざまな原因が考えられます。

1.証明書とトラストポイントが設定されているが、それらを使用する必要があるプロセスにバイ ンドされていない。 たとえば、使用されるトラストポイントは、Anyconnectクライアントを終 端する外部インターフェイスにバインドされません。

2. PKCS12ファイルがインストールされていますが、中間CA証明書がPKCS12ファイルにないため、エラーが発生します。中間CA証明書を信頼できる証明書として持つが、ルートCA証明書を 信頼できないクライアントは、証明書チェーン全体を検証できず、サーバID証明書を信頼できないとして報告できません。

3.誤った属性が設定された証明書は、インストール障害またはクライアント側のエラーの原因と なる可能性があります。たとえば、特定の属性が誤った形式でエンコードされている可能性があ ります。もう1つの理由は、ID証明書にサブジェクト代替名(SAN)がないか、サーバへのアクセス に使用されるドメイン名がSANとして存在しないことです。

Q.新しい証明書をインストールすると、メンテナンス期間が必要になるか、ダウンタイムが発生しますか。

A. 新しい証明書(IDまたはCA)のインストールに手間がかかることはないため、ダウンタイム が発生したり、メンテナンス期間が必要になることはありません。既存のサービスに対して新し い証明書を使用できるようにするには、変更が必要であり、変更要求/メンテナンスウィンドウが 必要になる可能性があります。

Q.証明書を追加または変更すると、接続されているユーザの接続が切断される可能性がありますか。

A.いいえ、現在接続されているユーザの接続は維持されます。証明書は接続の確立時に使用され ます。ユーザが再接続すると、新しい証明書が使用されます。

Q.ワイルドカードを使用してCSRを作成するにはどうすればよいですか。またはサブジェクトの 別名(SAN)を選択してください。

A.現在、ASA/FTDはワイルドカードを使用してCSRを作成できませんが、このプロセスは OpenSSLで実行できます。CSRとIDキーを生成するには、次のコマンドを実行します。

openssl genrsa -out id.key 2048

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

トラストポイントに完全修飾ドメイン名(FQDN)属性が設定されている場合、ASA/FTDによって 作成されるCSRには、その値を持つSANが含まれます。CSRに署名するときにCAが追加できる SAN属性が増えたり、OpenSSLでCSRを作成したりすることもできます

Q.証明書の置き換えは、すぐに有効になりますか。

A. 新しいサーバID証明書は、新しい接続にのみ使用されます。新しい証明書は、変更後すぐに使用できる状態になっていますが、実際には新しい接続で使用されます。

Q.インストールが正常に行われたかどうかを確認するには、どうすればよいですか。 A.確認するCLIコマンド:show crypto ca cert <trustpointname>

Q.ID証明書、CA証明書、および秘密キーからPKCS12を生成する方法は?

A. PKCS12は、次のコマンドを使用してOpenSSLで作成できます。 openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt Q.証明書をエクスポートして新しいASAにインストールする方法は? A.

- ・ CLIを使用する場合:コマンドcrypto ca export <trustpointname> pkcs12 <password>
- ASDMを使用:
 - a. Configuration > Device Management > Certificate Management > Identity Certificatesの順に移動し、Identity Certificateを選択します。[Export] をクリックしま す。

File View Tools Wizards Wind	ow Help					Type topic to search	Go	
Home 🖓 Configuration 🔯 Mo	nitoring 🔚 Save 🔇 Refre	sh 🔇 Back 🔘 Forwar	d 🢡 Help					cisco
Bookmarks 🗗 म 🗡	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)	S	now Details
	unstructuredName=FTD7 [asa.vpn.example.com]	CN=KrakowCA-sub1-1 Not Available	04:44:00 CEST Dec 21 2024 Pending	SSL-Trustpoint-PKCS12 SSL-Trustpoint	General Purpose Unknown	RSA (2048 bits)		Delete
								Instal
								Re-Enrol
Device Management 🗗 🖗								
Management Access Solutions Generation Solutions S								
Element Call-Home	Find:	🛇 🔘 🗌 Match Case						
Cloud Web Security	Certificate Expiration Alerts Send the first alert before	e: 60 (days) Set Def	ault					
Gertificate Management Identity Certificates	Repeat Alert Interval :	7 (days)						
	Weak Crypto Configurations -							

b. ファイルのエクスポート先を選択し、エクスポートパスワードを指定して、Export Certificateをクリックします。

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
instructuredName=asav	CN=ca.example.com, OU	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023	General Purp	oose RSA (4096 bits)	Show Detail
nstructuredName=risav	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purp	oose RSA (2048 bits)	Show Detail
nstructuredName=FTD7	CN=KrakowCA-sub1-1	04:44:00 CEST Dec 21 2024	SSL-Trustpoint-PKCS12	General Purp	oose RSA (2048 bits)	Delete
asa.vpn.example.com]	Not Available	Pending	SSL-Trustpoint	Unknown		Export
						Install
						Listai
ind: ertificate Expiration Alerts Send the first alert before	Match Case (days) Set Defa	ult				
Find: erbificate Expiration Alerts - Send the first alert before Repeat Alert Interval :	Image: Set Defa 7 (days)	Jt				
Find: ertificate Expiration Alerts - Send the first alert before Repeat Alert Interval : ak Crypto Configurations	Image: match case Image	Jt		×		
ind: ertificate Expiration Alerts Send the first alert before Repeat Alert Interval : k Crypto Configurations —] Permit Weak key sizes an	 Match Case (days) Set Defa (days) Export certificate d Ha Export to File: 	ult C:\Users\dsco.DESKTOP-1	R2CH8G5\Documents\ce] Brows	×		
Find: ertificate Expiration Alerts Send the first alert before Repeat Alert Interval : ak Crypto Configurations chypto Configurations Permit Weak key sizes an lic CA Enrollment	Match Case Match Case Match Case Go (days) Set Defa 7 (days) Export certificate dHa Export to File: Certificate Format:	ult C: {Users\cisco.DESKTOP+	R2CH8G5\Documents\ce Brows	X		
Find: ertificate Expiration Alerts Send the first alert before Repeat Alert Interval : ak Crypto Configurations Permit Weak key sizes an ic CA Enrollment et your Cisco ASA security a sting.	Match Case Match Case Match Case Go (days) Set Defa 7 (days) Gays Export certificate dHa Export to File: Certificate Format: spplie	Ult C: \Users\dsco.DESKTOP4 PKCS12 Format (Certificat PEM Format (Certificat	R2CH8G5\Documents\ce Brows ficate(s) + Private Key) te Only)	e	pecial promotional price for certificat	es and trial certificates f
Find: ertificate Expiration Alerts Send the first alert before Repeat Alert Interval : ik Crypto Configurations Permit Weak key sizes an ic CA Enrollment et your Clisco ASA security a sting.	Match Case Match Case Match Case Match Case Go (days) Set Defa Z (days) Set Defa Z (days) Export certificate dHa Export to File: Certificate Format: upple tifica Configuration Encryptio	Ut C:\Users\cisco.DESKTOP4 PKCS 12 Format (Certificat PEM Format (Certificat n Passphrase	R2CH8G5\Documents\ce Brows ficate(s) + Private Key) te Only)	e stomers a s	pecial promotional price for certificat	es and trial certificates f
Find: ertificate Expiration Alerts Send the first alert before Repeat Alert Interval : ik Crypto Configurations Permit Weak key sizes an ic CA Enrollment et your Clisco ASA security a sting. Ising a previously saved cer M Identity Cettificate Vision	Match Case Match Case Match Case Match Case Match Case Match Case Cell Certificate Certificate Format: pplic Export to File: Certificate Format: pplic Encryption Passphras	Ut C:\Users\dsco.DESKTOP4 @ PKCS12 Format (Certifcat) PEM Format (Certifcat n Passphrase 	R2CH8G5\Documents\ce Brows ficate(s) + Private Key) te Only)	e stomers a s	pecial promotional price for certificat	es and trial certificates f
Find: ertificate Expiration Alerts - Send the first alert before Repeat Alert Interval : sk Crypto Configurations Permit Weak key sizes an lic CA Enrollment	Match Case Match Case Match Case Match Case Match Case Case Certificate Certificate Format: Certificate Format: Define Certificate Format: Define Certificate Format:	ult C:\Users\disco.DESKTOP+ @ PKCS12 Format (Certificat	R2CH8G5\Documents\ce Brows ficate(s) + Private Key) te Only)	e k	pecial promotional price for certificat	ies and trial certificates f

エクスポートされた証明書は、コンピュータのディスクに保存できます。安全な場所 でパスフレーズを書き留めてください、ファイルはそれなしで役に立ちません。

Q. ECDSAキーを使用する場合、SSL証明書の生成プロセスは異なりますか。 A.設定の唯一の違いは、キーペア生成の手順です。この手順では、RSAキーペアの代わりに ECDSAキーペアを生成できます。手順のそれ以外の部分は変わりません。

Q.新しいキーペアを生成する必要は常にありますか。

A.キーペアの生成手順はオプションです。既存のキーペアを使用することも、PKCS12の場合は 証明書と一緒にキーペアをインポートすることもできます。それぞれの登録/再登録タイプについ ては、「キーペア名の選択」セクションを参照してください。

Q.新しいID証明書の新しいキーペアを生成しても安全ですか。

A.新しいキーペア名が使用されている限り、プロセスは安全です。この場合、古いキーペアは変更されません。

Q.ファイアウォールを交換する(RMAなど)際にキーを再生成する必要がありますか。

A.設計上の新しいファイアウォールには、古いファイアウォールに存在するキーペアはありません。

実行コンフィギュレーションのバックアップには、キーペアは含まれません。

ASDMで実行される完全バックアップには、キーペアを含めることができます。

ID証明書は、ASDMまたはCLIを使用して、失敗する前にASAからエクスポートできます。

フェールオーバーペアの場合、証明書とキーペアはwrite standbyコマンドを使用してスタンバイ

ユニットに同期されます。フェールオーバーペアの1つのノードが交換された場合は、基本的なフ ェールオーバーを設定し、新しいデバイスに設定をプッシュするだけで十分です。

キーペアがデバイスで失われ、バックアップがない場合は、新しいデバイスに存在するキーペア で新しい証明書に署名する必要があります。 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。