ASDM에서 관리하는 ASA에 인증서 설치 및 갱신

목차

<u>소개</u> 사전 요구 사항 요구 사항 사용되는 구성 요소 배경 정보 ASDM을 사용하여 새 ID 인증서 요청 및 설치 CSR(Certificate Signing Request)을 사용하여 새 ID 인증서 요청 및 설치 ASDM으로 CSR 생성 특정 이름으로 신뢰 지점 만들기 (<u>선택 사</u>항) 새 키 쌍 생성 키 쌍 이름 선택 인증서 주체 및 FQDN(정규화된 도메인 이름)을 구성합니다 CSR 생성 및 저장 ASDM을 사용하여 PEM 형식의 ID 인증서 설치 <u>CSR에 서명한 CA 인증서 설치</u> ID 인증서 설치 <u>새 인증서를 ASDM을 통해 인터페이스에 바인딩</u> ASDM을 사용하여 PKCS12 형식으로 받은 ID 인증서 설치 PKCS12 파일에서 ID 및 CA 인증서 설치 새 인증서를 ASDM을 통해 인터페이스에 바인딩 인증서 갱신 ASDM을 사용하여 CSR(Certificate Signing Request)로 등록된 인증서 갱신 ASDM을 사용하여 CSR 생성 특정 이름으로 새 신뢰 지점을 만듭니다. (선택사항)새키쌍생성 키 쌍 이름 선택 인증서 주체 및 FQDN(정규화된 도메인 이름)을 구성합니다 CSR 생성 및 저장 ASDM을 사용하여 PEM 형식의 ID 인증서 설치 CSR에 서명한 CA 인증서 설치 ID 인증서 설치 새 인증서를 ASDM을 통해 인터페이스에 바인딩 ASDM을 사용하여 PKCS12 파일에 등록된 인증서 갱신 PKCS12 파일에서 갱신된 ID 인증서 및 CA 인증서 설치 새 인증서를 ASDM을 통해 인터페이스에 바인딩 다음을 확인합니다. ASDM을 통해 설치된 인증서 보기 문제 해결 자주 묻는 질문(FAQ)

소개

이 문서에서는 ASDM으로 관리되는 Cisco ASA Software에서 특정 유형의 인증서를 요청, 설치, 신 뢰 및 갱신하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

- 시작하기 전에 ASA(Adaptive Security Appliance)에 올바른 클록 시간, 날짜 및 표준 시간대가 있는지 확인합니다. 인증서 인증에서는 NTP(Network Time Protocol) 서버를 사용하여 ASA의 시간을 동기화하는 것이 좋습니다. 관련 정보를 참조하십시오.
- CSR(Certificate Signing Request)을 사용하는 인증서를 요청하려면 신뢰할 수 있는 내부 또 는 서드파티 CA(Certificate Authority)에 대한 액세스 권한이 있어야 합니다. 서드파티 CA 벤 더의 예로는 Entrust, Geotrust, GoDaddy, Thawte, VeriSign 등이 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASAv 9.18.1
- PKCS12 생성에는 OpenSSL이 사용됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서의 주소 인증서 유형은 다음과 같습니다.

- 자체 서명 인증서
- 서드파티 인증 기관 또는 내부 CA에서 서명한 인증서

EAP 인증 프로토콜용 SSL(Secure Socket Layer), TLS(Transport Layer Security) 및 IKEv2 rfc7296에서는 SSL/TLS/IKEv2 서버가 클라이언트에 서버 인증을 수행할 서버 인증서를 제공하도 록 요구합니다. 이를 위해 신뢰할 수 있는 서드파티 CA를 사용하여 ASA에 SSL 인증서를 발급하는 것이 좋습니다.

Cisco에서는 사용자가 실수로 비인가 서버의 인증서를 신뢰하도록 브라우저를 구성할 수 있기 때문 에 자체 서명 인증서의 사용을 권장하지 않습니다. 사용자가 보안 게이트웨이에 연결할 때 보안 경 고에 대응해야 하는 불편도 있다.

ASDM을 사용하여 새 ID 인증서 요청 및 설치

인증서는 CA(Certificate Authority)에서 요청하고 ASA에 설치하는 두 가지 방법으로 사용할 수 있습니다.

- CSR(Certificate Signing Request)을 사용합니다. 키 쌍을 생성하고, CSR을 사용하여 CA에서 ID 인증서를 요청하며, CA에서 얻은 서명된 ID 인증서를 설치합니다.
- CA에서 가져왔거나 다른 디바이스에서 내보낸 PKCS12 파일을 사용합니다. PKCS12 파일에 는 키 쌍, ID 인증서, CA 인증서가 들어 있습니다.

CSR(Certificate Signing Request)을 사용하여 새 ID 인증서 요청 및 설치

CSR은 ID 인증서가 필요한 디바이스에 생성되며, 디바이스에 생성된 키 쌍을 사용합니다.

CSR에는 다음이 포함됩니다.

- 인증서 요청 정보 요청된 주체 및 기타 특성, 키 쌍의 공개 키,
- 서명 알고리즘 정보,
- 키 쌍의 개인 키로 서명된 인증서 요청 정보의 디지털 서명.

CSR은 CA(Certificate Authority)에 전달되므로 PKCS#10 형식으로 서명합니다.

서명된 인증서는 CA에서 PEM 형식으로 반환됩니다.

참고: CA는 CSR에 서명하고 서명된 ID 인증서를 생성할 때 신뢰 지점에 정의된 FQDN 및 주 체 이름 매개변수를 변경할 수 있습니다.

ASDM으로 CSR 생성

- 1. 특정 이름으로 신뢰 지점 만들기
 - a. Configuration(컨피그레이션) > Device Management(디바이스 관리) >Certificate Management(인증서 관리) > Identity Certificates(ID 인증서)로 이동합니다.

File View Tools Wizards Window	w Help				Type topic	to search	Go	ahaha
Home 🆓 Configuration 🔯 Monite	toring 🔚 Save 🔇 Refresh 🔇 Back 🔘	Forward 💡 Help						cisco
Device Management 🗗 🖗 🧕	Configuration > Device Management > Certif	icate Management > Identity Cer	<u>tificates</u>					
Management Access Generation	Issued To	∧ ¹ Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type		Add
System Image/Configuration Generation Generation Generation	unstructuredName=asa.example.com, L=San Jos	unstructuredName=asa.example	15:09:09 CEDT Jul 1	тр	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. Add(추가)를 클릭합니다.
- c. 신뢰 지점 이름을 정의합니다.

sued To	Issued By	Expiry Date	Associated Tro	ustpoints ^	¹ Usage	Public Key Type		Add
🛓 Add Identity C	Certificate					×	<	Show Deta
Trustpoint Name:	SSL-Trustpoint							Delete
O Import the ide	entity certificate from a file (PKCS12 format with Ce	rtificate(s)+Private Key):					Export
Decryption Pa	assphrase:							Install
File to Import	From:		Browse					Re-Enrol
Add a new ide	entity certificate:							
Key Pair:	<default-rsa-k< td=""><td>(ey> v</td><td>Show New</td><td></td><td></td><td></td><td></td><td></td></default-rsa-k<>	(ey> v	Show New					
Certificate Su	bject DN: CN=asavpn.exa	ample.com	Select					
Generate	self-signed certificate							
Act as	s local certificate authority ar	nd issue dynamic certific	ates to TLS-Proxy				-	
			Advanced					
Enable CA	A flag in basic constraints ext	ension	Auvanceu					

d. Add a New Identity Certificate(새 ID 인증서 추가) 라디오 버튼을 클릭합니다.

2. (선택 사항) 새 키 쌍 생성

참고: 기본적으로 Default-RSA-Key라는 이름과 2048의 크기를 갖는 RSA 키가 사용됩니다. 그러나 각 ID 인증서에 대해 고유한 개인/공용 키 쌍을 사용하는 것이 좋습니다.

a. New(새로 만들기)를 클릭하여 새 키 쌍을 생성합니다.

Issued To	Issued By	Expiry Date	Associated Trust	tpoints	Usage	Public Key Type	Add
Table Add Identity Cer	rtificate			×	General Purpose	RSA (4096 bits)	Show Deta
Trustnoint Name:	SSI -Trustnoint				General Purpose	RSA (2010 DIS)	Delete
Import the iden	ntity certificate from a file (PKCS12 format with Certifica	te(s)+Private Kev):				Export
Decryption Pas	sphrase:						Install
File to Import F	rom:	Brows	e				Re-Enrol
Add a new ider	ntity certificate:						
Key Pair:	<default-rsa+< td=""><td>Key> v Show</td><td>New</td><td></td><td></td><td></td><td></td></default-rsa+<>	Key> v Show	New				
Certificate Subj	ject DN: CN=asavpn.ex	ample.com Selec	t				
Generate s	elf-signed certificate						
Act as l	ocal certificate authority a	nd issue dynamic certificates	to TLS-Proxy				
			Adversed				
			Advanced				
Enable CA 1	flag in basic constraints ex	tension					

- b. Enter new Key Pair name(새 키 쌍 이름 입력) 옵션을 선택하고 새 키 쌍의 이름을 입력 합니다.
- c. Key Type(키 유형) RSA 또는 ECDSA를 선택합니다.
- d. Key Size(키 크기)를 선택합니다. RSA의 경우 General purpose for Usage(사용 용도)를 선택합니다.
- e. Generate Now(지금 생성)를 클릭합니다. 이제 키 쌍이 생성됩니다.

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	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. 키 쌍 이름 선택

CSR에 서명하고 새 인증서와 바인딩할 키 쌍을 선택합니다.

ssued To	Issued By	Expiry Date		Associated Trust	points	Usage	Public Key Type	Add
🔄 Add Identity Cer	tificate				×	General Purpose	RSA (4096 bits)	Show Deta
Trustpoint Name:	SSI -Trustmoint					General Polipose	KSA (2010 013)	Delete
Import the ident	tity certificate from a file (PKCS12 format with C	ertificate(s)+Pri	vate Kev):				Export
Decryption Pass	phrase:							Install
File to Import Fr	om:		Browse					Re-Enrol
Add a new iden	tity certificate:							
Key Pair:	SSL-Keypair	~ [Show	New				
Certificate Subje	ect DN: CN=asavpn.ex	ample.com	Select					
Generate se	If-signed certificate							
Act as lo	cal certificate authority a	nd issue dynamic certi	ficates to TLS-Pr	оху	_			
				Advanced	-			
Enable CA f	ag in basic constraints ex	tension						

4. 인증서 주체 및 FQDN(정규화된 도메인 이름)을 구성합니다

주의: FQDN 매개변수는 ID 인증서가 사용되는 ASA 인터페이스의 FQDN 또는 IP 주소 와 일치해야 합니다. 이 매개변수는 ID 인증서에 대해 요청된 SAN(Subject Alternative Name) 확장을 설정합니다. SAN 확장은 SSL/TLS/IKEv2 클라이언트에서 인증서가 연결 되는 FQDN과 일치하는지 확인하는 데 사용됩니다.

a. 선택을 클릭합니다.

ssued To	Issued By	Expiry Date	Associated Trustpoints	^1 Us	age Public Ke	y Type	Add
Add Identity Cer	rtificate				· · ·	×	Show Detail
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the iden	ntity certificate from a file (P	KCS12 format with Certificate(s))+Private Key):				Export
Decryption Pass	sphrase:						Install
File to Import Fi	rom:	Browse					Re-Enrol
Add a new iden	ntity certificate:						
Key Pair:	SSL-Keypair	v Show	New				
Certificate Subj	ject DN: CN=asavpn.exar	mple.com Select					
Generate se	elf-signed certificate						
Act as k	local certificate authority and	d issue dynamic certificates to TI	LS-Proxy				
_			Advanced				
Enable CA f	flag in basic constraints exte	nsion					
				-			
		Add Certificate	Cancel Help				

b. Certificate Subject DN(인증서 주체 DN) 창에서 인증서 특성을 구성합니다. 드롭다운 목 록에서 특성을 선택하고 값을 입력한 다음 Add(추가)를 클릭합니다.

sued To	Issued By	Expiry Date	Associated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Certificat	e					×	Show Detail
Trustpoint Name:	SSL-Trustpoint						Delete
O Import the identity ce	Certificate Subject	DN			×		Export
Decryption Passphrase	Certificate Subject	UN			~		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 cer							
Enable CA flag in t		ОК	Cancel Help				

issued To	Issued By	Expiry Date	Associated Trustpoint	s ^1 Usage	Public Key Type	Add
Add Identity Certifica	te	· · · ·			×	Show Details
Trustpoint Name:	SSL-Trustpoint					Delete
O Import the identity ce	Cartificato Subias	+ DN		~		Export
Decryption Passphras	a Certificate Subject			^		Install
File to Import From:			Attribute	Value		Re-Enroll
Add a new identity ce	DN Attribute to I	be Added	Common Nan	ne (CN) asa.vpn.exam		
Key Pair:	Attribute: Co	untry (C) 🗸 🗸	Add>>			
Certificate Subject DM	Value: Cor Dep	nmon Name (CN) partment (OU)	Delete			
Generate self-sig	n Cor	mpany Name (O)				
Act as local ce	Sta	te (St)				
	Ema	ail Address (EA)				
		ОК	Cancel Help			
Enable CA flag in	¢					

설명
방화벽에 액세스할 수 있는 이름(일반적으로 정규화된 도메인 이름(예:
vpn.example.com).
조직 내 부서 이름
합법적으로 등록된 조직/회사 이름
국가 코드(문장 부호 없는 2자 코드)
조직이 위치한 상태입니다.
조직이 위치한 도시입니다.
이메일 주소

참고: 이전 필드 값은 64자 제한을 초과할 수 없습니다. 값이 길면 ID 인증서 설치 에 문제가 발생할 수 있습니다. 또한 모든 DN 특성을 정의할 필요는 없습니다.

- 모든 특성을 추가한 후 OK를 클릭합니다.
- c. 디바이스 FQDN을 구성합니다. Advanced(고급)를 클릭합니다.

Configuration > Device Management > Certificate Management >	Identity Certificates
conquiation > bevice Hanagement > certificate Hanagement	identity certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	s ^1 Usage	Public Key Type	Add
Add Identity Certif	ficate				×	Show Detail
Trustpoint Name:	SSL-Trustpoint					Delete
O Import the identit	y certificate from a file (PK	CS12 format with Certificat	te(s) +Private Key):			Export
Decryption Passph	hrase:					Install
File to Import From	m:	Brows	e			Re-Enroll
Add a new identit	y certificate:					
Key Pair:	SSL-Keypair	~ Show	New			
Certificate Subjec	t DN: CN=asa.vpn.exar	mple.com Select	t			
Generate self	-signed certificate					
Act as loca	al certificate authority and	issue dynamic certificates f	to TLS-Proxy			
			Advanced			
Enable CA flag	g in basic constraints exter	nsion				
		Add Cartificate	Canaal			

d. FQDN 필드에 인터넷에서 디바이스에 액세스할 수 있는 정규화된 도메인 이름을 입력 합니다. OK(확인)를 클릭합니다.

ssued To	Issund Du	Evoiry Data	Accessized Trustasiate	A 1 110000	Public Key Type	Add
Add Identity Cer	rtificate	ced Options		×	×	Show Detail
Trustpoint Name:	S Certificate	mode parameters and SCEP challenge	password are not available for self-	signed certificates.		Delete
O Import the iden	tity certifica	E Parameters Enrolment Mode SCE	P Challenge Password			Export
Decryption Pass	sphrase: FQDN:	asavpn.example.com				Install
File to Import Fr	rom: E-mail:					Re-Enrol
Add a new iden	IP Addre	:55:				
Key Pair:	S Indu	de serial number of the device				
Certificate Subje	ect DN: C					
Generate se	elf-signed ce					
Act as lo	ocal certifica					
Enable CA fi	flag in basic (

5. CSR 생성 및 저장

a. Add Certificate(인증서 추가)를 클릭합니다.

Issued To	Issued By	Expiry D	ate	Associated Trustpoints	^1	Usage	Public Key Type	Add
Add Identity Certificat	e			1			×	Show Detail
Trustpoint Name:	SSL-Trustpoint							Delete
○ Import the identity cer	rtificate from a file (PK)	S12 format with	Certificate(s)+Pri	vate Kev):				Export
Decryption Passphrase	e:							Install
File to Import From:			Browse					Re-Enroll
Add a new identity cer	rtificate:							
Key Pair:	SSL-Keypair	~	Show	New				
Certificate Subject DN	: CN=asa.vpn.exam	ple.com	Select					
Generate self-sign	ed certificate							
Act as local cer	rtificate authority and i	ssue dynamic ce	rtificates to TLS-Pr	оху			-	
				dvanced				
Enable CA flag in b	oasic constraints exten	sion						
		Add Certif	icate C	ancel Help				

b. CSR을 로컬 시스템의 파일에 저장하기 위한 프롬프트가 표시됩니다.

ssued To	Issued By	Expiry Date	Associated Trustpoints	~1	Usage	Public Key Type	Add
Add Identity Cert	ificate					×	Show Details
Trustpoint Name:	SSL-Trustpoint	S12 format with Certificate(s)	I±Private Kav)•				Delete Export
Decryption Pass	ohrase:	entity Certificate Request		×			Install Re-Enroll
 Add a new identi Key Pair: Certificate Subje 	ity certificate: To c requ SSL-Keypa You ct DN: CN=asa.vp	omplete the enrollment proce uest (CSR) and send it to the will then need to install the ce ing the Install button in the Id	ss, please save the PKCS 10 enrollme CA. ertificate that is returned from the CA lentity Certificates panel.	it by			
Generate sel	f-signed certificate Savi	e CSR to File:	Cancel Help	vse		_	
Enable CA fla	ag in basic constraints extens	ion	Advanced				
				_			

Browse(찾아보기)를 클릭하고 CSR을 저장할 위치를 선택한 다음 .txt 확장자로 파일을 저장합니다.

참고: 파일을 .txt 확장자로 저장하면 PKCS#10 요청을 열고 텍스트 편집기(예: 메 모장)로 볼 수 있습니다.

c. 이제 새 신뢰 지점이 Pending(보류 중) 상태로 표시됩니다.

figuration > Device M	lanagement > Certifi	icate Management > Iden	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
						Do Encol

ASDM을 사용하여 PEM 형식의 ID 인증서 설치

설치 단계에서는 CA가 CSR에 서명하고 PEM 인코딩(.pem, .cer, .crt) ID 인증서 및 CA 인증서 번들 을 제공했다고 가정합니다.

- 1. CSR에 서명한 CA 인증서 설치
 - a. Configuration(컨피그레이션) > Device Management(디바이스 관리) >Certificate Management(인증서 관리) >로 이동하고 CA Certificates(CA 인증서)를 선택합니다. Add(추가)를 클릭합니다.

Configuration > Remote Acc	ess VPN > Certificate Mana	igement > <u>CA Certificates</u>				
le le						
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	Curt

b. 신뢰 지점 이름을 입력하고 Install From File(파일에서 설치)을 선택하고 Browse(찾아보 기) 버튼을 클릭한 다음 중간 인증서를 선택합니다. 또는 텍스트 파일의 PEM 인코딩 CA 인증서를 텍스트 필드에 붙여넣습니다.

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

참고: CSR에 서명한 CA 인증서를 설치하고 ID 인증서와 동일한 신뢰 지점 이름을 사용합니다. PKI 계층 구조의 다른 CA 인증서는 별도의 신뢰 지점에 설치할 수 있



c. Install Certificate를 클릭합니다.

issued To	Issued By	Expiry Date	Associated Trustpoin	ts ^	¹ Usage	Active		Add
denTrust Commercial Root	CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_Serv	erCA	General Purpose	No		Edit
uoVadis Root CA 2	CN=QuoVadis Root CA 2,	19:23:33 CEST Nov 24 2031	_SmartCallHome_Serv	erCA2	General Purpose	No		Lone
Install Certificate						×		Show Details
Trustpoint Name: SS	SL-Trustpoint	1.						Request CRI
O Install from a file:		Browse						Delete
Paste certificate in PEI	M format:							
VROOBBYEFESSi2abra 9HE/FS2147em9u2kah CGqeyQMRhs3RsyMD2 zskqaRijas153JV/NL8i QIRyjalH56BFlackNc7K gW8YnHOCM08svyTX dk/cox0/DRaxn413H END CERTIFICATI	9999LFV52U47em9UXaMBGGA1 AGCCSqGSbDDQEDCULAA4IBA 9M2WkAF4AY2HgN9QISYUCK 4M ESoAlatna/fQfKGV-tharacea SLUJOUCdmAY+IGO 23/WFN3MXWZO E	UdivQ1VHBaAFE 55k2sbra9b QQ4xSIFwK3h9bWo2Yh5mgT odkMQ2y4X/uhj65NDU7oFf6f tw24t5w44s4.dpp.wa wait Please wait while ASDM is delivi device	Information	: Certificate has the	following attributes:		×	
Specify source Interfa	ce: None		Finge	rprint: e9ad165c 26	73424c 6e7e0c5f b30b4	ła02		
Certificate Subject DN:	CN=risavpn31		Trust	point CA certificate	accepted.			
allow-untrusted-co	nnection							
O Use SCEP:					ОК			
Specify source Interfa	ce: None	\sim			269			
SCEP URL: http://								
Retry Period:	1	minutes						

- 2. ID 인증서 설치
 - a. CSR 생성 중에 이전에 생성 된 ID 인증서를 선택 합니다. Install(설치)을 클릭합니다.

<u>C</u>	onfiguration > Remot	te Ac	cess VPN > Certificate Ma	anagement > Identity Cert	ificates				
	Issued To	^1	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add	
	[vpn.example.com]		Not Available	Pending	SSL-Trustpoint	Unknown		Show Details	
								Delete	
								Export	
								Install	

참고: Identity Certificate(ID 인증서)에는 Issued By(발급자) 필드를 Not available(사용할 수 없음)으로 지정하고 Expiry Date(만료일) 필드를 Pending(보 류 중)으로 지정할 수 있습니다입니다.

b. CA에서 받은 PEM 인코딩 ID 인증서가 포함된 파일을 선택하거나 텍스트 편집기에서 PEM 인코딩 인증서를 열고 CA에서 제공한 ID 인증서를 복사하여 텍스트 필드에 붙여 넣습니다.

sued To	^¹ Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
n.example.com]	Not Available	Pending	SSL-Trustpoint	Unknown		Show Detail
				General Purpose	RSA (2048 bits)	Show Detail
Install identity cen	tificate		tpoint	General Purpose	RSA (2048 bits)	Delete
entity Certificate						Export
 Install from a file; 			browse			Install
						113001
O Paste the certification	ate data in base-64 form	at:				Re-Enrol
O Paste the certific	ate data in base-64 form	at:				Re-Enroll
O Paste the certific	ate data in base-64 form	at:				Re-Enroll
O Paste the certific	ate data in base-64 form	at:				Re-Enroll
O Paste the certific	ate data in base-64 form	at:				Re-Enroll
O Paste the certific	ate data in base-64 form	at:				Re-Enroll

참고: ID 인증서는 설치할 .pem, .cer, .crt 형식일 수 있습니다.

c. Install Certificate를 클릭합니다.

sued to	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
pn.example.com]	lot Available	Pending	SSL-Trustpoint	Unknown		Show Detail
loctall Identify cortificat	10		×	General Purpose	RSA (2048 bits)	
install identity certificat	te		tpoint	General Purpose	RSA (2048 bits)	Delete
dentity Certificate	🧰 Please v	vait	×			Export
O Install from a file:			Information	×		Install
Paste the certificate da	ata in ba P	lease wait while ASDM is deli levice	vering th			Re-Enroll
LnNBJz6XgDmVuQjfBE Gyer3x2GXML7MAiHBp			G Certificate im	port succeeded.		
T8y9Yia7poqMnamQka	QpcKAF					
END CERTIFICATE	DowH3					
-			OK			
<						

3. 새 인증서를 ASDM을 통해 인터페이스에 바인딩

지정된 인터페이스에서 종료되는 WebVPN 세션에 대해 새 ID 인증서를 사용하도록 ASA를 구성해야 합니다.

- a. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Advanced(고급) > SSL Settings(SSL 설정)로 이동합니다.
- b. Certificates(인증서)에서 WebVPN 세션을 종료하는 데 사용되는 인터페이스를 선택합 니다. 이 예에서는 외부 인터페이스가 사용됩니다.

Edit를 클릭합니다.

c. Certificate(인증서) 드롭다운 목록에서 새로 설치된 인증서를 선택합니다.

				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 nement > 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(확인)를 클릭합니다.
- e. 적용을 클릭합니다.

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

이제 새 ID 인증서가 사용 중입니다.

ASDM을 사용하여 PKCS12 형식으로 받은 ID 인증서 설치

PKCS12 파일(.p12 또는 .pfx 형식)에는 ID 인증서, 키 쌍 및 CA 인증서가 포함되어 있습니다. 와일 드카드 인증서의 경우처럼 CA에 의해 생성되거나 다른 디바이스에서 내보내집니다. 이진 파일이므 로 텍스트 편집기로 볼 수 없습니다.

- 1. PKCS12 파일에서 ID 및 CA 인증서 설치
 - ID 인증서, CA 인증서 및 키 쌍은 단일 PKCS12 파일에 번들로 묶어야 합니다.
 - a. Configuration(컨피그레이션) > Device Management(디바이스 관리) > Certificate Management(인증서 관리)로 이동하고 Identity Certificates(ID 인증서)를 선택합니다. b. Add(추가)를 클릭합니다.
 - c. 신뢰 지점 이름을 지정합니다.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Detai
🗧 Add Identity Certi	ficate		×			Delete
Trustpoint Name:	SSL-Trustpoint-P	KCS12				Export
Import the identit	ty certificate from a file (P	KCS12 format with Certificate	(s) +Private Key):			Install
Decryption Passp	hrase:					Re-Enrol
File to Import Fro	m:	Browse.				
O Add a new identit	ty certificate:					
Key Pair:	<default-rsa-ke< td=""><td>ey> v Show</td><td>New</td><td></td><td></td><td></td></default-rsa-ke<>	ey> v Show	New			
Certificate Subject	CN=risavpn31	Select.				
Generate self	f-signed certificate					
Act as loc	al certificate authority and	d issue dynamic certificates to	TLS-Proxy			
			Advanced			
Enable CA fla	g in basic constraints exte	ansing	Advorteeu			
L Shape CA lia	g in basic constraints exte					

d. Import The Identity Certificate from a File(파일에서 ID 인증서 가져오기) 라디오 버튼을 클릭합니다.

Issued To	Issued By	Expiry	Date	Associated	Trustpoints	Usage	Public Ke	у Туре	A	dd
									Show	Detail
Table Add Identity Ce	ertificate				×				De	ete
Trustnoint Name:	SSI -Trustpoint-f	2KC512			import ID certif	ficate file				
Import the ide	ntity certificate from a file (PKCS12 format	with Certificate(s)+F	rivate Kev):	Look in:	Document	s	~ 6) 📂 🛄 •	
Decruption Par	cobrace:	incost format			0	CSR.txt				_
Ele to Import i	From:		Browne		Passet Items	🦻 vpn.exam	ple.com.pfx			
	atibu sastification		Di Olise		Recent Items					
O Add a new ide	nuty certificate:			_						
Key Pair:	<default-rsa-k< td=""><td>iey></td><td>Show</td><td>New</td><td>Desktop</td><td></td><td></td><td></td><td></td><td></td></default-rsa-k<>	iey>	Show	New	Desktop					
Certificate Sub	oject DN: CN=risavpn31		Select							
Generate	self-signed certificate				Documents					
Act as	local certificate authority ar	nd issue dynamic	certificates to TLS-	Proxy						
					This PC F	ile name:	vpn.example.com.pfx		Import ID certificat	e file
				Advanced	- 🍙 F	iles of type:	All Files	~	Cancel	
Enable CA	flag in basic constraints ext	ension								

e. PKCS12 파일을 생성하는 데 사용되는 패스프레이즈를 입력합니다.

ssued To	Issued By E	xpiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
Add Identity Certificate	e		×			Delete
Trustpoint Name:	SSL-Trustpoint-PKCS12					Export
Import the identity cer	tificate from a file (PKCS12 for	mat with Certificate(s)+P	rivate Key):			Install
Decryption Passphrase						Re-Enroll
File to Import From:	C: \Users\cisco.DESKTOP-R	2CH8G Browse				
O Add a new identity cer	rtificate:					
Key Pair:	<default-rsa-key></default-rsa-key>	Show	New			
Certificate Subject DN	CN=risavpn31	Select				
Generate self-sign	ed certificate					
Act as local cer	rtificate authority and issue dyr	namic certificates to TLS-f	Proxy			
			Advanced			
Enable CA flag in h	assic constraints extension		Advanceu			
	asic constraints extension					
Enable CA flag in b	basic constraints extension					

f. Add Certificate를 클릭합니다.

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	lentity certificate from a file (PKCS12 format with Certificate(s)+Private Key):			Install
Decryption Pa	assphrase: ••••					Re-Enroll
File to Import	t From: C: \Users\cisco.l	DESKTOP-R2CH8G Browse				
🔿 Add 🗧 PI	lease wait					
Key I Certi	Please wait while ASDM device	is delivering the command(s) to	the Created trustpoint WARNING: CA cert the validation-usage	s for CAs higher in the hie lificates can be used to va ye of this trustpoint to limit	rarchy as the CA certificate was not s alidate VPN connections,by default. Ple the validation scope, if necessary	elf-signed.
Enable C	A flag in basic constraints ext	tension	Import PKCS 12 ope	eration completed success	fully.	

참고: CA 인증서 체인이 포함된 PKCS12를 가져오면 ASDM은 -number 접미사가 추가된 이름과 함께 업스트림 CA 신뢰 지점을 자동으로 생성합니다.

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
<pre>KrakowCA-sub1</pre>	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. 새 인증서를 ASDM을 통해 인터페이스에 바인딩

지정된 인터페이스에서 종료되는 WebVPN 세션에 대해 새 ID 인증서를 사용하도록 ASA를 구성해야 합니다.

a. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Advanced(고급) > SSL Settings(SSL 설정)로 이동합니다.

b. Certificates(인증서)에서 WebVPN 세션을 종료하는 데 사용되는 인터페이스를 선택합 니다. 이 예에서는 외부 인터페이스가 사용됩니다.

Edit를 클릭합니다.

c. Certificate(인증서) 드롭다운 목록에서 새로 설치된 인증서를 선택합니다.

ertificates	Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To enrol a trustpoint, go to Device Management > Certificate Management > Identity Certificates.	Edit Delete
Specify which certificates, if ar Interface OUTSIDE-direct inside inside-vlan management	Interface: OUTSIDE-direct Primary Enrolled Certificate: SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u v Load Balancing Enrolled Certificate: None v OK Cancel Help	rtificate of their own.
Fallback Certificate: Forced Certification Authentica	tion Timeout:	

d. OK(확인)를 클릭합니다.

e. 적용을 클릭합니다.

Cer S	tificates pecify 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-Trustpoint-PKCS12:unstructuredName=F		Primary: RSA (2048 bits), Load Balan	

이제 새 ID 인증서가 사용 중입니다.

인증서 갱신

ASDM을 사용하여 CSR(Certificate Signing Request)로 등록된 인 증서 갱신

CSR 등록 인증서의 인증서 갱신은 새 신뢰 지점을 생성하고 등록해야 합니다. 다른 이름(예: 등록 연도 접미사가 있는 이전 이름)이 있어야 합니다. 이전 인증서와 동일한 매개변수와 키 쌍을 사용하 거나 다른 매개변수를 사용할 수 있습니다.

ASDM으로 CSR 생성

1. 특정 이름으로 새 신뢰 지점을 만듭니다.

a. Configuration(컨피그레이션) > Device Management(디바이스 관리) >Certificate Management(인증서 관리) > Identity Certificates(ID 인증서)로 이동합니다.

File View Tools Wizards Wind	dow	Help					Type topic	to search	Go	ahaha
Home 🆓 Configuration 🔯 Ma	lonito	ring 🔚 Save 💽 F	tefresh 🔇 Back 🔘 Fi	orward 🢡 Help						cisco
Device Management 🗗 🖗	G	onfiguration > Device	Management > Certific	ate Management > Identity Cer	<u>tificates</u>					
Management Access Jicensing		Issued To	~	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type		Add
System Image/Configuration High Availability and Scalability		unstructuredName=asa	.example.com, L=San Jos]unstructuredName=asa.example	15:09:09 CEDT Jul 1	TP	General Purpose	RSA (2048 bits)	-1	Show Details
Logging Smart Call-Home									1	Delete
Cloud Web Security										Export
B - Service Hoddle Settings										Install
Certificate Management Certificates CA Certificates										Re-Enroll

b. Add(추가)를 클릭합니다. c. 신뢰 지점 이름을 정의합니다.

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

d. Add a New Identity Certificate(새 ID 인증서 추가) 라디오 버튼을 클릭합니다.

2. (선택 사항) 새 키 쌍 생성

참고: 기본적으로 Default-RSA-Key라는 이름과 2048의 크기를 갖는 RSA 키가 사용됩니다. 그러나 각 ID 인증서에 대해 고유한 개인/공용 키 쌍을 사용하는 것이 좋습니다.

a. New(새로 만들기)를 클릭하여 새 키 쌍을 생성합니다.

ssued To	Issued By	Expiry Date		Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName=	CN=ca.example.com, OU	15:10:00 CEST	Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🔄 Add Identity	Certificate			×			Delete
Trustpoint Name	e: SSL-Trustpoint-20	23					Export
O Import the i	identity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):			Install
Decryption I	Passphrase:						Re-Enroll
File to Impo	rt From:		Browse				
Add a new i	identity certificate:						
Key Pair:	<default-rsa-ke< td=""><td>y> ~</td><td>Show</td><td>New</td><td></td><td></td><td></td></default-rsa-ke<>	y> ~	Show	New			
Certificate S	Subject DN: CN=asavpn.exam	nple.com	Select				
Generat	te self-signed certificate						
Act	as local certificate authority and	issue dynamic cer	tificates to TL	S-Proxy			
				Advanced			
Enable (CA flag in basic constraints exter	nsion		Auvanceu			
	en nug in busic const unto exter	120011					

- b. Enter new Key Pair name(새 키 쌍 이름 입력) 옵션을 선택하고 새 키 쌍의 이름을 입력 합니다.
- c. 키 유형(RSA 또는 ECDSA)을 선택합니다.
- d. Key Size(키 크기)를 선택합니다. RSA의 경우 General purpose for Usage(사용 용도)를 선택합니다.
- e. Generate Now(지금 생성)를 클릭합니다. 이제 키 쌍이 생성됩니다.

Show Detai
Delete
Export
Install
Re-Enroll

3. 키 쌍 이름 선택

CSR에 서명하고 새 인증서와 바인딩할 키 쌍을 선택합니다.

sued To Issued By Ex		Expiry Date	y Date Associated Trustpoints		Usage	Public Key Type	Add
structuredName= CN=c	a.example.com, OU	15:10:00 CEST F	eb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Deta
Add Identity Certificat	e			×			Delete
Trustpoint Name:	SSL-Trustpoint-20	23					Export
O Import the identity ce	rtificate from a file (PK	CS12 format with (Certificate(s)	+Private Key):			Install
Decryption 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	: CN=asavpn.exam	ple.com	Select				
Generate self-sign	ed certificate						
Act as local ce	rtificate aut Srity and	issue dynamic cert	ficates to TL	S-Proxy			
				Advanced			
Enable CA flag in l	oasic constraints exter	nsion					

4. 인증서 주체 및 FQDN(정규화된 도메인 이름)을 구성합니다

주의: FQDN 매개변수는 인증서가 사용되는 ASA 인터페이스의 FQDN 또는 IP 주소와 일치해야 합니다. 이 매개변수는 인증서의 SAN(주체 대체 이름)을 설정합니다. SAN 필 드는 SSL/TLS/IKEv2 클라이언트에서 인증서가 연결되는 FQDN과 일치하는지 확인하 는 데 사용됩니다.

참고: CA는 CSR에 서명하고 서명된 ID 인증서를 생성할 때 신뢰 지점에 정의된 FQDN 및 주체 이름 매개변수를 변경할 수 있습니다.

a. 선택을 클릭합니다.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName	e= CN=ca.example.com, OU	15:10:00 CEST Feb	6 2024 SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
add Identit	y Certificate		×			Delete
Trustooint Nar	me: SSI -Trustnoint-20	23				Export
O Import the	e identity certificate from a file (PK	CS12 format with Cer	rtificate(s) +Private Key):			Install
Decryption	n Passphrase:					Re-Enroll
File to Imp	ort From:	E	Browse			
Add a new	videntity certificate:					
Key Pair:	SSL-KeyPair-2023	~	Show New			
Certificate	Subject DN: CN=asavpn.exam	ple.com	Select			
Genera	ate self-signed certificate					
Ac	t as local certificate authority and	issue dynamic certific	ates to TLS-Proxy			
			Advanced			
Enable	e CA flag in basic constraints exter	nsion	Auvanced			

b. Certificate Subject DN(인증서 주체 DN) 창의 드롭다운 목록에서 특성을 선택하여 인증 서 특성을 구성하고 값을 입력하고 Add(추가)를 클릭합니다.

ssued To	Issued By	Expiry	Date	Associated Trustpoints		Usage	Public Key Type	Add
nstructuredName	= CN=ca.example.com,	OU 15:10:0	0 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detail
🔁 Add Identit	y Certificate			×				Delete
Trustpoint Nar	ne: SSL-Trustpo	int-2023		-				Export
Certificate Subje	ct DN				×			Install
					_			Re-Enroll
			Attribute	Value				
DN Attribute to	be Added	Adds s	Common Name (CN Company Name (O	 asavpn.example.c example inc 	om			
Value: US		Add>>						
value.		Delete						
	OK	Cance	Help					
L Enable	CA flag in basic constraints	extension						

속성	설명
CN	방화벽에 액세스할 수 있는 이름(일반적으로 정규화된 도메인 이 름(예: vpn.example.com).
오우	조직 내 부서 이름
0	합법적으로 등록된 조직/회사 이름
С	국가 코드(문장 부호 없는 2자 코드)
ST	조직이 위치한 상태입니다.
L	조직이 위치한 도시입니다.
EA	이메일 주소

참고: 이전 필드는 64자 제한을 초과할 수 없습니다. 값이 길면 ID 인증서 설치에 문제가 발생할 수 있습니다. 또한 모든 DN 특성을 정의할 필요는 없습니다.

모든 특성을 추가한 후 OK를 클릭합니다.

c. 디바이스 FQDN을 구성하려면 Advanced(고급)를 클릭합니다.

ssued To	Issued By	Expiry Date		Associated Trustp	oints	Usage	Public Key Type	Add
nstructuredName=	CN=ca.example.com, OU	15:10:00 CEST	Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detail
Add Identity Cert	ificate			>	<			Delete
Trustpoint Name:	SSI -Trustmoint-20	23						Export
O Import the ident	ity certificate from a file (PK	CS12 format with	Certificate(s)	+Private Key):				Install
Decryption Pass	phrase:							Re-Enroll
File to Import Fre	om:		Browse					
Add a new ident	ity certificate:							
Key Pair:	SSL-KeyPair-2023	- v	Show	New				
Certificate Subje	ct DN: /pn.example.com,	,O=example inc	Select					
Generate sel	If-signed certificate				-			
Act as lo	cal certificate authority and	issue dynamic ce	rtificates to TL	S-Proxy	-			
				Advanced				
Enable CA fla	ag in basic constraints exter	nsion	L	Advanced				

d. FQDN 필드에 인터넷에서 디바이스에 액세스할 수 있는 정규화된 도메인 이름을 입력 합니다. OK(확인)를 클릭합니다.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
Advanced (Ontions	OU IS 10:00 CEET SALLS	X	General Purpose	RSA (2048 bits)	Show Details
Auvanceu						Delete
Certificate Para	ameters Enrollment Mode	SCEP Challenge Password	e for self-signed certificates.			Export
						Install
FQDN:	asavpn.example.com					Re-Enroll
E-mail:						
IP Address:						
	enal number of the device					
		N				
		2				

- 5. CSR 생성 및 저장
 - a. Add Certificate(인증서 추가)를 클릭합니다.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
nstructuredName=	CN=ca.example.com, OU	. 15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
🔄 Add Identity	Certificate		×			Delete
Trustpoint Name	SSL-Trustpoint-20	023				Export
O Import the id	dentity certificate from a file (PF	KCS12 format with Certificate	(s) +Private Key):			Install
Decryption P	Passphrase:					Re-Enroll
File to Impor	t From:	Browse.				
Add a new id	dentity certificate:					
Key Pair:	SSL-KeyPair-2023	3 ~ Show	. New			
Certificate S	ubject DN: /pn.example.com	,O=example inc Select.	•• m			
Generat	e self-signed certificate					
Act a	as local certificate authority and	d issue dynamic certificates to	TLS-Proxy			
			Advanced			
Enable (A flag in basic constraints exte	incioni	Auvanceu			
	A hag in basic consulaints exte					

b. 로컬 시스템의 파일에 CSR을 저장하기 위한 프롬프트가 표시됩니다.

isued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
structuredName	e= CN=ca.example.com, OU	15: 10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Detail
🗟 Add Identit	y Certificate		×			Delete
Trustooiot Na	me: SSI .Trustmoint.20	123				Export
Import the	e identity certificate from a file (PK	KCS12 format with Certificate(s))+Private Key):			Install
	atite Castificate Research		×			Re-Enroll
F	molete the enrolment process. p	leace cave the BKCS 10 encolory	ant .			
• requ	est (CSR) and send it to the CA.					
K You dicki	will then need to install the certific ng the Install button in the Identit	ate that is returned from the C ty Certificates panel.	A by			
[Save	CSR to File: C:\Users\cisco.DES	KTOP-R2CH8G5\Docun Br	owse			
	ОК С	ancel Help				
_			Advanced			
	e CA flag in basic constraints exter	nsion				
Enable	-					

Browse(찾아보기)를 클릭합니다. CSR을 저장할 위치를 선택하고 .txt 확장자로 파일을 저장합니다.

참고: 파일을 .txt 확장자로 저장하면 PKCS#10 요청을 열고 텍스트 편집기(예: 메 모장)로 볼 수 있습니다.

c. 이제 새 신뢰 지점이 Pending(보류 중) 상태로 표시됩니다.

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

ASDM을 사용하여 PEM 형식의 ID 인증서 설치

설치 단계에서는 CA가 CSR에 서명하고 PEM 인코딩(.pem, .cer, .crt)된 새 ID 인증서 및 CA 인증서 번들을 제공했다고 가정합니다.

1. CSR에 서명한 CA 인증서 설치

ID 인증서에 서명한 CA 인증서는 ID 인증서에 대해 생성된 신뢰 지점에 설치할 수 있습니다. ID 인증서가 중간 CA에 의해 서명된 경우 이 CA 인증서를 ID 인증서 신뢰 지점에 설치할 수 있습니다. 계층의 모든 업스트림 CA 인증서는 별도의 CA 신뢰 지점에 설치할 수 있습니다.

a. Configuration(컨피그레이션) > Device Management(디바이스 관리) >Certificate Management(인증서 관리) >로 이동하고 CA Certificates(CA 인증서)를 선택합니다. Add(추가)를 클릭합니다.

ssued 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
uoVadis Root CA 2	CN=QuoVadis Root CA 2,	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	Luit
lenTrust Commercial Root	. CN=IdenTrust Commercial	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	Show Deta

b. Trustpoint 이름을 입력하고 Install From File(파일에서 설치)을 선택하고 Browse(찾아보 기) 버튼을 클릭한 다음 중간 인증서를 선택합니다. 또는 텍스트 파일의 PEM 인코딩 CA 인증서를 텍스트 필드에 붙여넣습니다.

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

참고: ID 인증서가 중간 CA 인증서로 서명된 경우 ID 인증서 신뢰 지점 이름과 동 일한 신뢰 지점 이름으로 중간 인증서를 설치합니다.

c. Install Certificate를 클릭합니다.

sued To	Issued By ^1	Expiry Date	Associated Trustpoints	Usage	Active	Add
.example.com	CN=ca.example.com, OU=I	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes	Edit
Install Certificate						× Show Details
Trustpoint Name:	SSL-Trustpoint-2023]				Request CR
O Install from a file:		Browse				Delete
Paste certificate in	PEM format:					
okSeEPpH231QUV Oj9skMrCbPfg3p2 VROB8VFEFS3L2 9LEV52J47em0U cGqeyOMRhs3Rs/ 2skqaRijsx153jV/ 0RyjaH58EPladd gW8YnH0/M083y dcVcov0/PAxmAl END CERTIFIC Use EST: Specify source Intr EST URL: https:// Certificate Subject allow-untrustee Use SCEP: Specify source Intr SCEP URL: http:// Retry Period: Retry Count:	Girp/zmmzxl46/tel6ev/dojpon/tel Girp/zmmzxl46/tel6ev/dojpon/tel FeH7w3h 1K3/czAgAdBAAGJUDBOMJ bradbzLFV52U47embyxl4B68GA Lk8E90AlatnA/f07K044h7 Lk8E90AlatnA/f07K044h7	yigeHNkQdTSUkWRSX wGA1UdEwQFMMBARBARBwHQY UdIwQMBARESSK2bra9b kQArsXIEwK3INBwQsYhSmqT formation INFO: Certificate ha Fingerprint: e9ad163 Trustpoint CA certifi in inutes (Use 0 to indicate unli	D s the following attributes: 5c 2673424c 6e7e0c5f b30b4a02 cate accepted. OK			×

이 예에서 새 인증서는 이전 인증서와 동일한 CA 인증서로 서명됩니다. 동일한 CA 인증 서가 이제 두 개의 신뢰 지점과 연결됩니다.

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

- 2. ID 인증서 설치
 - a. CSR 생성으로 이전에 생성한 ID 인증서를 선택합니다. Install(설치)을 클릭합니다.

ionfiguration > Device	e Management > Certifica	ate Management > Identity	Certificates			
Issued To	Issued By	Expiry Date	Associated Trustpoints v1	Usage	Public Key Type	Add
unstructuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)	Show Details
[asavpn.example.com]	Not Available	Pending	SSL-Trustpoint-2023	Unknown		
						Delete
						Export
						Install
						Re-Enrol

참고: Identity Certificate(ID 인증서)에는 Issued By(발급자) 필드를 Not available(사용 불가)으로 지정하고 Expiry Date(만료일) 필드를 Pending(보류 중)으로 지정할 수 있습니다.

b. CA에서 받은 PEM 인코딩 ID 인증서가 포함된 파일을 선택하거나 텍스트 편집기에서 PEM 인코딩 인증서를 열고 CA에서 제공한 ID 인증서를 복사하여 텍스트 필드에 붙여

넣습니다.

ssued To	Issued By	Expiry Date	Associated Trustpoints	~1	Usage	Public Key Type	Add
nstructuredName	= CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint		General Purpose	RSA (2048 bits)	Show Detai
savpn.example.c	omj [Not Available	Pending	SSL-Trustpoint-2023		Unknown		Delete
							Export
linstall Identi	ty certificate		×				Install
lantity Cartifica	ta						Re-Enrol
Install from	na file:		Browse				
		L	browse				
O Paste the o	certificate data in base-64 format	:					

참고: ID 인증서는 설치할 .pem, .cer, .crt 형식일 수 있습니다.

c. Install Certificate를 클릭합니다.

sued To	Issued By	Expiry Date	Associated Trustpoints ~ 1	¹ Usage	Public Key Type	Add
structuredName=	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	eral Purpose RSA (2048 bits)	Show Detz
savpn.example.com]	Not Available	Pending	SSL-Trustpoint-2023	Unknown		Delete
						Export
Install Identity o	ertificate		×			Install
lentity Certificate -						Re-Enrol
	wait					
Pa	s Informa	ition	×			
	Please wait wł device		1			
6		Cartificate impact successed	d			
- -	Q	Certificate import succeede				
	•	Ceruncate import succeede				

설치 후 이전 및 새 ID 인증서가 있습니다.

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

3. 새 인증서를 ASDM을 통해 인터페이스에 바인딩

지정된 인터페이스에서 종료되는 WebVPN 세션에 대해 새 ID 인증서를 사용하도록 ASA를 구성해야 합니다.

- a. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Advanced(고급) > SSL Settings(SSL 설정)로 이동합니다.
- b. Certificates(인증서)에서 WebVPN 세션을 종료하는 데 사용되는 인터페이스를 선택합

니다. 이 예에서는 외부 인터페이스가 사용됩니다.

Edit를 클릭합니다.

c. Certificate(인증서) 드롭다운 목록에서 새로 설치된 인증서를 선택합니다.

					Edit	I
					Delete	1
	🔤 Select SSL Certificate		×			
ertificates	Specify enrolled trustpoints to be u OUTSIDE-direct interface. To enrol Management > Identity Certificate	sed for SSL authentication and VPN load balancing on the a trustpoint, go to Device Management > Certificate s.				
Specify which certificates, if an	Interface:	OUTSIDE-direct		tes not associated with a certificate of their own.		
Interface	Primary Enrolled Certificate:	SSL-Trustpoint-2023:unstructuredName=asavpn.exampl.	• ~	Кеу-Туре	Edit	
OUTSIDE-direct	Load Balancing Enrolled Certificate:	None	\sim	Primary: RSA (2048 bits), Load Balancing: n		
inside						
inside-vlan	OK	Cancel Help				

- d. OK(확인)를 클릭합니다.
- e. 적용을 클릭합니다. 이제 새 ID 인증서가 사용 중입니다.

uration > Remote Acces	s VPN > Advanced > <u>SSL Settings</u>			
icates	y, should be used for SSL authentication on ea	ch interface. The fallback certificate will be u	sed on interfaces not associated with a certificate of their own.	Edit Delete
Interface	Primary Certificate	Load Balancing Certificate	Кеу-Туре	Edit
OUTSIDE-direct	SSL-Trustpoint-2023:unstructure		Primary: RSA (4096 bits), Load Balancing: n	
nside				
anida ulan				1.33
nside-vian				

ASDM을 사용하여 PKCS12 파일에 등록된 인증서 갱신

등록된 PKCS12 인증서의 인증서 갱신 시 새 신뢰 지점을 생성하고 등록해야 합니다. 다른 이름(예: 등록 연도 접미사가 있는 이전 이름)이 있어야 합니다.

PKCS12 파일(.p12 또는 .pfx 형식)에는 ID 인증서, 키 쌍 및 CA 인증서가 포함되어 있습니다. 예를 들어 와일드카드 인증서의 경우 CA가 생성하거나 다른 디바이스에서 내보냅니다. 이진 파일이며 텍스트 편집기로 볼 수 없습니다.

- 1. PKCS12 파일에서 갱신된 ID 인증서 및 CA 인증서 설치
 - ID 인증서, CA 인증서 및 키 쌍은 단일 PKCS12 파일에 번들로 묶어야 합니다.
 - a. Configuration(컨피그레이션) > Device Management(디바이스 관리) > Certificate Management(인증서 관리)로 이동하고 Identity Certificates(ID 인증서)를 선택합니다.
 - b. Add(추가)를 클릭합니다.
 - c. 새 신뢰 지점 이름을 지정합니다.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Detai
🗧 Add Identity Certi	ficate		×			Delete
Trustpoint Name:	SSL-Trustpoint-P	KCS12				Export
Import the identit	ty certificate from a file (P	KCS12 format with Certificate	(s) +Private Key):			Install
Decryption Passp	hrase:					Re-Enrol
File to Import Fro	m:	Browse.				
O Add a new identit	ty certificate:					
Key Pair:	<default-rsa-ke< td=""><td>ey> v Show</td><td>New</td><td></td><td></td><td></td></default-rsa-ke<>	ey> v Show	New			
Certificate Subject	CN=risavpn31	Select.				
Generate self	f-signed certificate					
Act as loc	al certificate authority and	d issue dynamic certificates to	TLS-Proxy			
			Advanced			
Enable CA fla	g in basic constraints exte	ansing	Advorteeu			
L Shape CA lia	g in basic constraints exte					

d. Import The Identity Certificate from a File(파일에서 ID 인증서 가져오기) 라디오 버튼을 클릭합니다.

ssued to	Issued By	Expiry	Date	Associated	Trustpoints	Usage	Publ	с Кеу Туре		Add
										Show Detail
add Identity Cert	tificate				×					Delete
Trustnoint Name:	SSI -Trustpoint-P	KC512			import ID certif	icate file				
Import the ident	tity certificate from a file (F	KCS12 format w	ith Certificate(s)+F	Private Kev):	Look in:	😫 Document	s	~	/ 🤌 📂 🖽	•
Decryption Pass	obrase:	inco i c ioniar i		india najy.	@_ [CSR.txt				
File to Import Fr	om:		Browse		Recent Items	눩 vpn.exam	ple.com.pfx			
Add a new ident	tity 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 Subje	ect DN: CN=risavpn31		Select							
Generate se	lf-signed certificate				Documents					
Act as lo	cal certificate authority an	d issue dynamic	certificates to TLS-	Proxy						
				Advanced	This PC F	le name:	vpn.example.com.pf;	¢ .	Import ID	certificate file
Enable CA f	an in basis constraints out	ancion		Advanced	' 🎒 F	les of type:	All Files	~	C	ancel
	ag in basic collisi dints exti	CI ISION								

e. PKCS12 파일을 생성하는 데 사용되는 패스프레이즈를 입력합니다.

exp	ry Date	Associated Trustpoints	Usage	Public Key Type	Add
					Show Detai
1		×			Delete
SSL-Trustpoint-PKCS12					Export
tificate from a file (PKCS12 forma	t with Certificate(s)+P	rivate Key):			Install
••••					Re-Enroll
C: \Users\cisco.DESKTOP-R2C	H8G Browse				
tificate:					
<default-rsa-key></default-rsa-key>	Show	New			
CN=risavpn31	Select				
ed certificate					
tificate authority and issue dyna	nic certificates to TLS-f	Proxy			
		A descent and			
		Advanced			
asic constraints extension					
asic constraints extension					
	SSL-Trustpoint-PKCS12 tificate from a file (PKCS12 forma C: Users\cisco.DESKTOP-R2CI tificate: CDefault-RSA-Key> CN=risavpn31 ed certificate tificate authority and issue dynam asic constraints extension ficate Cancel	SSL-Trustpoint-PKCS12 tificate from a file (PKCS12 format with Certificate(s) +P C: Users\cisco.DESKTOP-R2CH8G Browse C:Users\cisco.DESKTOP-R2CH8G Browse C:	SSL-Trustpoint-PKCS12 SSL-Trustpoint-PKCS12 thCate from a file (PKCS12 format with Certificate(s)+Private Key): CtUsers\cisco.DESKTOP-R2CH8G Browse CtUsers\cis	SSL-Trustpoint-PKCS12 tificate from a file (PKCS12 format with Certificate(s)+Private Key): : : : : : : : : : : : : :	SSL-Trustpoint-PKCS12 tiftcate from a file (PKCS12 format with Certificate(s) +Private Key): : : : : : : : : : : : : :

f. Add Certificate를 클릭합니다.

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	lentity certificate from a file (PKCS12 format with Certificate(s)+Private Key):			Install
Decryption Pa	assphrase: ••••					Re-Enroll
File to Import	t From: C: \Users\cisco.l	DESKTOP-R2CH8G Browse				
🔿 Add 🗧 PI	lease wait					
Key I Certi	Please wait while ASDM device	is delivering the command(s) to	the Created trustpoint WARNING: CA cert the validation-usag	s for CAs higher in the hie lificates can be used to va ye of this trustpoint to limit	rarchy as the CA certificate was not s alidate VPN connections,by default. Ple the validation scope, if necessary	elf-signed.
Enable C	A flag in basic constraints ext	tension	Import PKCS 12 ope	eration completed success	fully.	

참고: CA 인증서 체인이 있는 PKCS12를 가져오면 ASDM은 -number 접미사가 추 가된 이름과 함께 업스트림 CA 신뢰 지점을 자동으로 생성합니다.

Issued To	\sim 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. 새 인증서를 ASDM을 통해 인터페이스에 바인딩

지정된 인터페이스에서 종료되는 WebVPN 세션에 대해 새 ID 인증서를 사용하도록 ASA를 구성해야 합니다.

a. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Advanced(고급) > SSL Settings(SSL 설정)로 이동합니다.

b. Certificates(인증서)에서 WebVPN 세션을 종료하는 데 사용되는 인터페이스를 선택합니다. 이 예에서는 외부 인터페이스가 사용됩니다.

Edit를 클릭합니다.

c. Certificate(인증서) 드롭다운 목록에서 새로 설치된 인증서를 선택합니다.

Demon	de vindere		Edit Delete
	Select SSL Certificate Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the OUTSIDE-direct interface. To erroll a trustpoint, go to Device Management > Certificate Management > Identity Conference	×	
rtificates Specify which certificates, if ar Interface OUTSIDE-direct inside inside-vlan management	Management > Identity Certificates. Interface: OUTSIDE-direct Primary Enrolled Certificate: SSL-Trustpoint-PKCS12:unstructuredName=FTD72-ek, u Load Balancing Enrolled Certificate: None OK Cancel	es not associated with a certificate of their own.	Edit
Fallback Certificate: Forced Certification Authentica	ion Timeout: 2 minutes		

d. OK(확인)를 클릭합니다.

e. 적용을 클릭합니다.

Certi Sp	ficates 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	

이제 새 ID 인증서가 사용 중입니다.

다음을 확인합니다.

타사 공급업체 인증서의 성공적인 설치를 확인하고 SSL VPN 연결에 을 사용하려면 다음 단계를 수 행합니다.

ASDM을 통해 설치된 인증서 보기

- 1. Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리)로 이동하고 Identity Certificates(ID 인증서)를 선택합니다.
- 2. 서드파티 벤더에서 발급한 ID 인증서가 나타날 수 있습니다.

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-Trustpoint-PKCS12:unstructuredName=F		Primary: RSA (2048 bits), Load Balan	

문제 해결

이 debug 명령은 SSL 인증서 설치 실패 시 CLI에서 수집됩니다.

• debug crypto ca 14

자주 묻는 질문(FAQ)

Q. PKCS12란 무엇입니까?

A. 암호학에서 PKCS12는 많은 암호학 객체를 하나의 파일로 저장하기 위해 만든 아카이브 파일 형 식을 정의합니다. 개인 키를 해당 X.509 인증서와 함께 번들로 묶거나 신뢰 체인의 모든 멤버를 번 들로 묶는 데 일반적으로 사용됩니다.

Q. CSR이란 무엇입니까?

A. PKI(Public Key Infrastructure) 시스템에서 인증서 서명 요청(CSR 또는 인증 요청)은 디지털 ID 인증서를 신청하기 위해 신청자가 공용 키 인프라의 등록 기관에 보내는 메시지입니다. 일반적으로 인증서를 발급할 수 있는 공개 키, 서명된 인증서를 식별하는 데 사용되는 정보(예: Subject의 도메 인 이름) 및 무결성 보호(예: 디지털 서명)가 포함됩니다.

Q. PKCS12의 비밀번호는 어디에 있습니까?

A. 인증서 및 키 쌍을 PKCS12 파일로 내보내면 비밀번호가 export 명령에 지정됩니다. pkcs12 파 일을 가져오려면 CA 서버의 소유자 또는 다른 디바이스에서 PKCS12를 내보낸 사람이 비밀번호를 전달해야 합니다.

Q. 루트와 ID의 차이점은 무엇입니까?

A.암호화 및 컴퓨터 보안에서 루트 인증서는 루트 CA(Certificate Authority)를 식별하는 공개 키 인 증서입니다. 루트 인증서는 자체 서명되며(교차 서명된 루트에서 발급한 인증서인지 여부 등) 인증 서에 여러 신뢰 경로가 있을 수 있음) X.509 기반 PKI(공개 키 인프라)의 기반을 형성합니다. 공개 키 인증서(디지털 인증서 또는 ID 인증서라고도 함)는 공개 키의 소유권을 증명하는 데 사용되는 전 자 문서입니다. 인증서에는 키에 대한 정보, 소유자(주체라고 함)의 ID에 대한 정보, 인증서의 내용 을 확인한 엔티티(발급자라고 함)의 디지털 서명이 포함됩니다. 서명이 유효하고 인증서를 검사하 는 소프트웨어가 발급자를 신뢰하는 경우 해당 키를 사용하여 인증서의 주체와 안전하게 통신할 수 있습니다.

Q. 인증서를 설치했는데 왜 작동하지 않습니까? A.다음과 같은 여러 가지 이유로 인해 발생할 수 있습니다.

1. 인증서 및 신뢰 지점이 구성되었지만 이를 사용해야 하는 프로세스에 바인딩되지 않았습니다. 예를 들어, 사용할 신뢰 지점은 Anyconnect 클라이언트를 종료하는 외부 인터페이스에 바인딩되지 않습니다.

2. PKCS12 파일이 설치되었지만 PKCS12 파일에 없는 중간 CA 인증서로 인해 오류가 발생합니다. 중간 CA 인증서를 신뢰할 수 있지만 루트 CA 인증서를 신뢰할 수 없는 클라이언트는 전체 인증서 체인을 확인하고 서버 ID 인증서를 신뢰할 수 없는 것으로 보고할 수 없습니다.

3. 잘못된 특성으로 채워진 인증서는 설치 실패 또는 클라이언트 측 오류를 일으킬 수 있습니다. 예

를 들어, 특정 특성은 잘못된 형식을 사용하여 인코딩될 수 있습니다. 또 다른 이유는 ID 인증서에 SAN(주체 대체 이름)이 없거나 서버 액세스에 사용되는 도메인 이름이 SAN으로 존재하지 않기 때 문입니다.

Q. 새 인증서를 설치하려면 유지 관리 기간이 필요합니까, 아니면 다운타임이 발생합니까? A. 새 인증서(ID 또는 CA)를 설치하는 것은 방해가 되지 않으며 다운타임을 발생시키거나 유지 보 수 기간을 필요로 하지 않습니다. 기존 서비스에 새 인증서를 사용하도록 설정하려면 변경 사항이 있으며 변경 요청/유지 관리 기간이 필요할 수 있습니다.

Q. 인증서를 추가하거나 변경하면 연결된 사용자의 연결이 끊길 수 있습니까? A.아니요. 현재 연결된 사용자는 계속 연결되어 있습니다. 인증서는 연결 설정 시 사용됩니다. 사용 자가 다시 연결하면 새 인증서가 사용됩니다.

Q: 와일드카드로 CSR을 생성하려면 어떻게 해야 합니까? 또는 SAN(Subject Alternative Name)입니까?

A.현재 ASA/FTD는 와일드카드로 CSR을 생성할 수 없습니다. 그러나 이 프로세스는 OpenSSL을 사용하여 수행할 수 있습니다. CSR 및 ID 키를 생성하려면 다음 명령을 실행할 수 있습니다. openssl genrsa -out id.key 2048

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

신뢰 지점이 FQDN(Fully Qualified Domain Name) 특성으로 구성된 경우 ASA/FTD에서 생성한 CSR에 해당 값의 SAN이 포함됩니다. CSR에 서명할 때 CA가 더 많은 SAN 특성을 추가하거나 OpenSSL을 사용하여 CSR을 생성할 수 있습니다

Q. 인증서 교체는 즉시 적용됩니까?

A. 새 서버 ID 인증서는 새 연결에 대해서만 사용됩니다. 새 인증서는 변경 직후 사용할 준비가 되었 지만 실제로 새 연결에서 사용됩니다.

Q. 설치가 제대로 되었는지 확인하려면 어떻게 해야 합니까?

A. 확인할 CLI 명령: show crypto ca cert <trustpointname>

Q. ID 인증서, CA 인증서 및 개인 키에서 PKCS12를 생성하는 방법은 무엇입니까?

A. PKCS12는 OpenSSL을 사용하여 다음 명령을 사용하여 생성할 수 있습니다. openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt

Q. 새 ASA에 설치하기 위해 인증서를 내보내는 방법은 무엇입니까? A.

- CLI에서: crypto ca export <trustpointname> pkcs12 <password> 명령을 사용합니다.
- ASDM의 경우:
 - a. Configuration(컨피그레이션) > Device Management(디바이스 관리) > Certificate Management(인증서 관리) > Identity Certificates(ID 인증서)로 이동하고 Identity Certificate(ID 인증서)를 선택합니다. Export(내보내기)를 클릭합니다.

File View Tools Wizards Window	v Help					Type topic to search	Go	ahaha
🚮 Home 🦓 Configuration 🔯 Monit	oring 🔚 Save 🔇 Refre	sh 🔇 Back 🔘 Forward	d 🧖 Help					CISCO
Bookmarks 🗗 म 🗡	Configuration > Device Ma	nagement > Certificate M	lanagement > Identity Ce	rtificates				C
o bookmark a page, right-click on a ode in the navigation tree and select	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type		Add
Go Telete	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]	Not Available	Pending	SSL-Trustpoint	Unknown	KSA (2040 Dits)		Export
								Install
								Re-Enrol
Device Management P								
B Licensing System Image/Configuration B Availability and Scalability								
Logging Smart Call-Home	Find:	💿 💿 🗌 Match Case						
Cloud Web Security Cloud Web Security Service Module Settings Cloud Settings Clo	Certificate Expiration Alerts Send the first alert before	e: 60 (days) Set Defa	ault					
Certificate Management	Repeat Alert Interval :	7 (days)						

b. 파일을 내보낼 위치를 선택하고 내보내기 비밀번호를 지정한 다음 Export Certificate(인 증서 내보내기)를 클릭합니다.

ssued To	Issued By	Expiry Date	Associated Trustpoints	Usad	ge	Public Key Type	Add
nstructuredName=asav	CN=ca.example.com, OU	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023		General Purpose	RSA (4096 bits)	Charu Datata
nstructuredName=risav	CN=ca.example.com, OU	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	(General Purpose	RSA (2048 bits)	Show Details
nstructuredName=FTD7	CN=KrakowCA-sub1-1	04:44:00 CEST Dec 21 2024	SSL-Trustpoint-PKCS12		General Purpose	RSA (2048 bits)	Delete
sa.vpn.example.com]	Not Available	Pending	SSL-Trustpoint		Unknown		Emert
							Export
							Install
							Re-Enroll
ind: rtificate Expiration Alerts Send the first alert before	Image: Match Case e: 60 (days) Set Defr	sult					
ind: rtificate Expiration Alerts Send the first alert before Repeat Alert Interval :	 Match Case (days) Set Defa (days) 	sult					
ind: ertificate Expiration Alerts Send the first alert before Repeat Alert Interval : k Crypto Configurations —	 Match Case (days) Set Defa (days) Export certificate 	sult		×			
ind: rtificate Expiration Alerts Send the first alert before Repeat Alert Interval : k Crypto Configurations — Permit Weak key sizes an	 Match Case 60 (days) Set Definition 7 (days) Export certificate 	sult		×	}		
nd: rtificate Expiration Alerts Send the first alert before Repeat Alert Interval : c Crypto Configurations —] Permit Weak key sizes an	 Match Case 60 (days) Set Defa 7 (days) 7 Export certificate d Ha Export to File: 	ault C:\Users\cisco.DESKTOP4	R2CH8G5\Documents\ce	×	-		
nd: tificate Expiration Alerts Send the first alert befor Repeat Alert Interval : : Crypto Configurations — Permit Weak key sizes an : CA Enrollment —	Match Case Match Case Go (days) Set Defr (days) Export certificate d Ha Export to File: Certificate Format:	ault C: \Users\cisco.DESKTOP4	R2CH8G5\Documents\ce	×			
nd: tificate Expiration Alerts Send the first alert before Repeat Alert Interval : Crypto Configurations — Permit Weak key sizes an CA Enrollment — t your Cisco ASA security ;	Match Case Match Case (days) Set Defa 7 (days) Export certificate d Ha Export to File: Certificate Format: applie	C:\Users\cisco.DESKTOP-4	R2CH8G5\Documents\ce Browse	×	stomers a special	promotional price for certificat	es and trial certificates fo
nd: tificate Expiration Alerts Send the first alert before Repeat Alert Interval : (Crypto Configurations —] Permit Weak key sizes an : CA Enrollment — tyour Cisco ASA security : ting.	 Match Case (days) Set Defi (days) Export certificate d Ha Export to File: Certificate Format: appliz 	C:\Users\cisco.DESKTOP4	R2CH8G5\Documents\ce Browse icate(s) + Private Key)	×	stomers a special	promotional price for certificat	es and trial certificates fo
nd: tificate Expiration Alerts Send the first alert before Repeat Alert Interval : : Crypto Configurations — Permit Weak key sizes an : CA Enrollment — t your Cisco ASA security a ting.	Match Case Match Case Match Case Go (days) Set Defi (days) Export certificate d Ha Export to File: Certificate Format: applie	C:\Users\cisco.DESKTOP+ () PKCS12 Format (Certif () PEM Format (Certificat	R2CH8G5\Documents\ce Browse icate(s) + Private Key) e Only)	:: ×	stomers a special	promotional price for certificat	es and trial certificates fo
ind: trificate Expiration Alerts Send the first alert before Repeat Alert Interval : k Crypto Configurations — Permit Weak key sizes an CA Enrollment — t your Cisco ASA security a ting.	Match Case Match Case Match Case Go (days) Set Defi 7 (days) Export certificate dHa Export to File: Certificate Format: applia	eult C:\Users\cisco.DESKTOP4 PKCS12 Format (Certificat PEM Format (Certificat	R2CH8G5\Documents\ce Browse icate(s) + Private Key) e Only)	×	stomers a special	promotional price for certificat	es and trial certificates fo
ind: rtificate Expiration Alerts Send the first alert before Repeat Alert Interval : k Crypto Configurations] Permit Weak key sizes an c CA Enrollment	Match Case Match Case Match Case Match Case (days) Set Defi (days) Export certificate dHa Export to File: Certificate Format: pplic tifica Configuration Encryption	eult C:\Users\cisco.DESKTOP+ PKCS12 Format (Certificat PEM Format (Certificat on Passphrase	R2CH8G5\Documents\ce Browse icate(s) + Private Key) e Only)	×	stomers a special	promotional price for certificat	es and trial certificates fo
ind: rtificate Expiration Alerts Send the first alert before Repeat Alert Interval : k Crypto Configurations —] Permit Weak key sizes an c CA Enrollment — t your Cisco ASA security : sting. sing a previously saved cer 4 Identity Certificate Wizar	Match Case Match Case Match Case (days) Set Defa 7 (days) Export certificate d Ha Export to File: Certificate Format: pplic tifica Configuration Encryptio d —	C:\Users\cisco.DESKTOP-4 © PKCS 12 Format (Certif O PEM Format (Certificat on Passphrase se:	R2CH8G5\Documents\ce Browse icate(s) + Private Key) e Only)	×	stomers a special	promotional price for certificat	es and trial certificates fo
nd: tificate Expiration Alerts Send the first alert before Repeat Alert Interval : (Crypto Configurations —] Permit Weak key sizes an : CA Enrollment — tyour Cisco ASA security : ting. ing a previously saved cer 1 Identity Certificate Wizar e Cisco ASDM Identity Cer	Match Case Match Case Match Case Go (days) Set Defa 7 (days) Export certificate d Ha Export to File: Certificate Format: applic tifica Configuration Encryption Passphrase	C:\Users\cisco.DESKTOP+ PKCS 12 Format (Certificat PEM Format (Certificat on Passphrase se:	R2CH8G5\Documents\ce Browse icate(s) + Private Key) e Only)	 	stomers a special cher.	promotional price for certificat	es and trial certificates fo

내보낸 인증서는 컴퓨터 디스크에 있을 수 있습니다. 안전한 곳에 암호를 적어 두십시오 . 파일이 없으면 무용지물입니다.

Q. ECDSA 키를 사용하는 경우 SSL 인증서 생성 프로세스가 다릅니까? A.컨피그레이션의 유일한 차이점은 키 쌍 생성 단계로, 여기서 RSA 키 쌍 대신 ECDSA 키 쌍을 생 성할 수 있습니다. 나머지 단계는 동일하게 유지됩니다.

Q. 항상 새 키 쌍을 생성해야 합니까? A.키 쌍 생성 단계는 선택 사항입니다. 기존 키 쌍을 사용할 수 있습니다. 또는 PKCS12의 경우 키 쌍을 인증서와 함께 가져옵니다. 해당 등록/재등록 유형에 대한 키 쌍 이름 선택 섹션을 참조하십시 오.

Q. 새 ID 인증서에 대한 새 키 쌍을 생성해도 안전합니까? A.새 키 쌍 이름을 사용하는 한 프로세스는 안전합니다. 이 경우 이전 키 쌍은 변경되지 않습니다.

Q. 방화벽을 교체할 때(예: RMA) 키를 다시 생성해야 합니까?

A.새로운 방화벽은 설계상 기존 방화벽에 키 쌍이 없습니다.

실행 중인 컨피그레이션의 백업에는 키 쌍이 포함되어 있지 않습니다.

ASDM을 사용하여 수행한 전체 백업에는 키 쌍이 포함될 수 있습니다.

ASA에서 ASDM 또는 CLI를 사용하여 ID 인증서를 내보냈다가 실패할 수 있습니다.

장애 조치 쌍의 경우 인증서 및 키 쌍은 write standby 명령을 사용하여 스탠바이 유닛에 동기화됩니 다. 장애 조치 쌍의 노드 하나를 교체하는 경우 기본 장애 조치를 구성하고 새 디바이스에 컨피그레 이션을 푸시하는 데 충분합니다.

디바이스에서 키 쌍이 손실되고 백업이 없는 경우, 새 디바이스에 키 쌍이 있는 상태에서 새 인증서 를 서명해야 합니다. 이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.