# ISE에 타사 CA 서명 인증서 설치

## 목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 구성 1단계. CSR(Certificate Signing Request)을 생성합니다. 2단계. 새 인증서 체인을 가져옵니다. 다음을 확인합니다. 문제 해결 dot1x 인증 중에 신청자가 ISE 로컬 서버 인증서를 신뢰하지 않음 ISE 인증서 체인이 올바르지만 엔드포인트가 인증 중에 ISE의 서버 인증서를 거부함 관련 정보

## 소개

이 문서에서는 Cisco ISE(Identity Services Engine)에서 서드파티 CA 서명 인증서 설치에 대해 설 명합니다. 이 프로세스는 최종 인증서 역할(EAP 인증, 포털, 관리 및 pxGrid)과 상관없이 동일합니 다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 기본 공개 키 인프라에 대한 지식을 보유하고 있는 것이 좋습니다.

### 사용되는 구성 요소

이 문서의 정보는 Cisco ISE(Identity Services Engine) 릴리스 3.0을 기반으로 합니다. 릴리스 2.X에 도 동일한 구성이 적용됩니다.

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

### 구성

### 1단계. CSR(Certificate Signing Request)을 생성합니다.

CSR을 생성하려면 Administration(관리) > Certificates(인증서) > Certificate Signing Requests(인증 서서명요청)로 이동하고 Generate Certificate Signing Requests (CSR)(CSR(Generate Certificate Signing Requests)를 클릭합니다.

Certificate Management $\checkmark$ System Certificates	Certificate Signing Requests			
Trusted Certificates	Generate Certificate Signing Requests (CSR)			
OCSP Client Profile	A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Clic			
Certificate Signing Requests	request has been signed, click "bind" to bind the request to the signed certificate issued by that			
Certificate Periodic Check Se	Q View ⚠ Export			
Certificate Authority >	Friendly Name Certificate Subject			

- 1. Usage 섹션의 드롭다운 메뉴에서 사용할 역할을 선택합니다.인증서가 여러 역할에 사용되는 경우 다중 사용을 선택할 수 있습니다.인증서가 생성되면 필요한 경우 역할을 변경할 수 있습 니다.
- 2. 인증서를 생성할 노드를 선택합니다.
- 3. 필요에 따라 정보를 입력합니다(조직 단위, 조직, 도시, 주 및 국가).

**참고:**CN(Common Name) 필드 아래에서 ISE는 노드의 FQDN(Fully Qualified Domain Name)을 자동으로 채웁니다.

와일드카드:

- 와일드카드 인증서를 생성하려는 경우 Allow Wildcard Certificates 상자를 선택합니다.
- 인증서가 EAP 인증에 사용되는 경우 Windows 신청자가 서버 인증서를 거부하므로 \* 기호가 Subject CN 필드에 없어야 합니다.
- 서 플리 컨 트에서 Validate Server Identity(서버 ID 검증)가 비활성화된 경우에도 \*가 CN 필드 에 있는 경우 SSL 핸드셰이크가 실패할 수 있습니다.
- 대신 CN 필드에서 일반 FQDN을 사용할 수 있으며, 그런 다음 **\*.domain.com을** SAN(Subject Alternative Name) DNS Name 필드에 사용할 수 있습니다.

**참고:**일부 CA(Certificate Authorities)는 CSR에 없는 경우에도 인증서의 CN에 와일드카드 (\*)를 자동으로 추가할 수 있습니다.이 시나리오에서는 이 작업을 방지하기 위해 특별한 요청 을 제기해야 합니다.

개별 서버 인증서 CSR 예:

#### Usage

Certificate(s) will be used for	Multi-Use	~	You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).
Allow Wildcard Certificates	()		
Node(s)			
Generate CSR's for these Nodes:			
Node	CSR Friendly Name		
✓ abtomar30	abtomar30#Multi-Use		
Subject			
Common Name (CN) \$FQDN\$		(j)	
Organizational Unit (OU) Cisco TAC		<b>(</b> )	
Organization (O) Cisco		<u>(</u> )	
City (L) Bangalore			
State (ST) Karnataka			
Country (C)			
Subject Alternative Name (SAN)			
IP Address	∨ 10.106.120.87		- + 0
* Key type			
RSA	× ()		

와일드카드 CSR 예:

Isage			~
Certificate(s) will be used for	Multi-Use	~ 🔺	You can use a single certificate for multiple services, but doing so is not a recommended
			practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).
Allow Wildcard Certificates	()		
Subject			
Mycluster.mydomain,com		(i)	
Organizational Unit (OU) Cisco TAC		<u>(</u> )	
Organization (O) Cisco		(j)	
City (L) Bangalore			
State (ST) Karnataka			
Country (C) IN			
Subject Alternative Name (SAN)			
IP Address	✓ 10.106.120.87		- +
DNS Name	✓ *.mydomain.com		- + ()
* Key type			
RSA	× (i)		

**참고:**IP 주소를 통해 서버에 액세스할 때 인증서 경고를 피하기 위해 각 구축 노드의 IP 주소를 SAN 필드에 추가할 수 있습니다.

CSR이 생성되면 ISE는 내보내기 옵션이 있는 팝업 창을 표시합니다. 내보낸 후에는 서명을 위해 이 파일을 CA로 전송해야 합니다. Successfully generated CSR(s) 🔽

Certificate Signing request(s) generated:

abtomar30.abtomar.local#Multi-Use

Click Export to download CSR(s) or OK to return to list of CSR(s) screen



### 2단계. 새 인증서 체인을 가져옵니다.

인증 기관은 전체 인증서 체인(루트/중간)과 함께 서명된 서버 인증서를 반환합니다. 수신되면 다음 단계에 따라 ISE 서버로 인증서를 가져옵니다.

- 1. CA에서 제공하는 루트 및 중간 인증서를 가져오려면 Administration(관리) > Certificates(인증 서) > Trusted Certificates(신뢰할 수 있는 인증서)로 이동합니다.
- 2. Import(**가져오기)**를 클릭한 다음 Root(루트) 및/또는 Intermediate(중간) 인증서를 선택하고 제 출할 관련 확인란을 선택합니다.
- 3. 서버 인증서를 가져오려면 Administration(관리) > Certificates(인증서) > Certificate Signing Requests(인증서 서명 요청)로 이동합니다.
- 4. 이전에 생성한 CSR을 선택하고 Bind Certificate(인증서 바인딩)를 클릭합니다.
- 5. 새 인증서 위치를 선택하고 ISE는 데이터베이스에 생성 및 저장 된 개인 키에 인증서를 바인딩 합니다.

**참고:**이 인증서에 대해 Admin Role(관리 역할)을 선택한 경우 특정 ISE 서버 서비스가 다시 시 작됩니다.

**주의:**가져온 인증서가 구축의 기본 관리 노드에 대한 것이며 관리 역할이 선택된 경우 모든 노 드의 서비스는 차례로 재시작됩니다.이 작업은 예상되며 이 작업을 수행하려면 다운타임이 권 장됩니다.

## 다음을 확인합니다.

인증서 가져오기 중에 관리 역할을 선택한 경우 브라우저에서 관리 페이지를 로드하여 새 인증서가

제자리에 있는지 확인할 수 있습니다. 체인이 올바르게 빌드되고 브라우저에서 인증서 체인을 신 뢰할 수 있는 경우 브라우저는 새 관리자 인증서를 신뢰해야 합니다.

Certificate ×	
abtomar-WIN-231PNBS4IPH-CA	
	Identity Services Engine
	Intuitive network security
	Username
View Certificate	
Certificate status: This certificate is OK.	Password
	Login
ОК	English   日本語
	Problems logging in?

© 2020 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc. and/or its affiliates in the U.S and certain other countries. Cisco ISE View third-party licenses and notices

추가 확인을 위해 브라우저에서 잠금 기호를 선택하고 인증서 경로 아래에서 컴퓨터에서 전체 체인 이 존재하고 신뢰할 수 있는지 확인합니다.이는 전체 체인이 서버에 의해 올바르게 전달되었음을 나타내는 직접적인 표시기가 아니라 로컬 트러스트 저장소를 기반으로 서버 인증서를 신뢰할 수 있 는 브라우저의 표시기입니다.

## 문제 해결

### dot1x 인증 중에 신청자가 ISE 로컬 서버 인증서를 신뢰하지 않음

SSL 핸드셰이크 프로세스 중에 ISE가 전체 인증서 체인을 전달하는지 확인합니다.

서버 인증서(예: PEAP)가 필요한 EAP 방법 및 **서버 ID 확인**이 선택된 경우 신청자는 인증 프로세스 의 일부로 로컬 신뢰 저장소에 있는 인증서를 사용하여 인증서 체인을 검증합니다.SSL 핸드셰이크 프로세스의 일부로 ISE는 해당 인증서 및 체인에 있는 루트 및 중간 인증서를 나타냅니다.체인이 불 완전한 경우 신청자가 서버 ID를 검증할 수 없습니다.인증서 체인이 클라이언트로 다시 전달되었는 지 확인하려면 다음 단계를 수행할 수 있습니다.

1. 인증 중에 ISE(TCPDump)에서 캡처를 가져오려면 Operations(작업) > Diagnostic Tools(진단 **둘) > General Tools(일반 툴) > TCP Dump(TCP 덤프)로 이동합니다**.

- 2. 캡처를 다운로드/열고 Wireshark에서 **ssl.handshake.certificates** 필터를 적용하고 액세스 챌린 지를 찾습니다.
- 3. Expand Radius Protocol(RADIUS 프로토콜) > Attribute Value Pairs(특성 값 쌍) > EAP-Message Last segment(EAP-메시지 마지막 세그먼트) > Extensible Authentication Protocol(확장 가능한 인증 프로토콜) > Secure Sockets Layer(SSL 소켓 레이어) > Certificate(인증서) > Certificates(인증서)로 이동합니다.

캡처에서 인증서 체인.

Eile Edit	jile Edit View Go Capture Analyze Statistics Telephony Tools Internals Help					
● ● ∡ ▲ = _ = = = = = = = = = = = = = = = = =						
Filter	ssLhandshake.certificates	Expression	Clear Apply	Save		
No	Time	Source	Destination	Protocol Length Toto		
334	13:59:41.137274	14, 36, 157, 20	14, 36, 157, 21	TLSv1.2 992 Server	Hello, Certificate, Server Hello Done	
857	13:59:53,158063	14, 36, 157, 21	14, 36, 154, 5	RADIUS 1178 Access-	Challenge(11) (id=198, 1=1136)	
860	13:59:53,193912	14, 36, 157, 21	14.36.154.5	RADIUS 1174 Access	Challenge(11) (id=199, ]=1132)	
862	13:59:53.213715	14, 36, 157, 21	14.36.154.5	RADIUS 1174 Access-	Challenge(11) (id=200, 1=1132)	
864	13:59:53.231653	14.36.157.21	14.36.154.5	RADIUS 301 Access=	Challenge(11) (id=201, 1=259)	
1265	14:00:01.253698	14.36.157.20	14.36.157.21	TLSv1.2 992 Server	Hello, Certificate, Server Hello Done	
4				11		
21 A\	P: 1-255 t-EAP-Message(/	9) Segment[1]				
B A1	P: 1=255 t=EAP-Message(7	9) Segment[2]				
A\	P: 1=255 t=EAP-Message(7	9) Segment[3]				
8 A1	P: 1=255 t=EAP-Message(7	<ol><li>Last Segment[4]</li></ol>				
	EAP fragment					
8	Extensible Authentication	n Protocol				
	Code: Request (1)					
	Id: 41					
	Length: 1012					
	Type: Protected EAP (EA	₽-PEAP) (25)				
	EAP-TLS Flags: 0xc0					
	EAP-TLS Length: 3141					
	# [4 EAP-TLS Fragments (3)	141 bytes): #857(1002), #86	0(1002), #862(1002)	, #864(135)]		
	Secure Sockets Layer					
	I TLSv1 Record Layer: H	andshake Protocol: Server He	110			
	⊟ TLSV1 Record Layer: H	andshake Protocol: Certifica	te			
	Content Type: Handsh	take (22)				
	Version: TLS 1.0 (0)	(0301)				
	Length: 3048					
	Handshake Protocol:	Certificate				
	Handshake Type: Certificate (11)					
	Length: 3044					
	Certificates Length: 3041					
	Certificates (3041	bytes)				
	Certificate Leng	th: 1656				
	E Certificate (id-	at-commonwane=TORISE20A.rtpa	aa.net,1d-at-organ	zationalunitname=RTPAAA,1d-	at-organizationName=CISCO,1d-at-localityName=	rRT
	Certificate Leng	th: 13/9				
	E Certificate (id-	at-commonName=rtpaaa-ca,dc=r	tpaaa,dc=net)			
	ILSVI Record Layer: H	andshake Protocol: Server He	TTO Done			

체인이 불완전한 경우 ISE Administration(ISE 관리) > Certificates(인증서) > Trusted Certificates(신 뢰할 수 있는 인증서)로 이동하고 루트 및 (또는) Intermediate 인증서가 있는지 확인합니다.인증서 체인이 성공적으로 전달된 경우 여기에 설명된 방법을 사용하여 체인 자체를 유효한 것으로 확인해 야 합니다.

각 인증서(서버, 중간 및 루트)를 열고 각 인증서의 SKI(Subject Key Identifier)를 체인의 다음 인증 서의 AKI(Authority Key Identifier)에 매칭하여 신뢰 체인을 확인합니다.

인증서 체인의 예.

Certificate 26	Certificate 25	Certificate 25
General Details Certification Path	General Details Certification Path	General Details Certification Path
Show <all></all>	Show <ai></ai>	Show
Field Value A	Field Value ^	Field Value *
Public key RSA (2048 8#s)	CA Version V0.0	Public key RSA (4096 Bits)
E Subject Key Identifier da 39 a3 ee 5e 6b 4b 0d 32 55 bf ef 95 6	Subject Key Identifier fe 34 ca 8d 22 9b 6e d7 a6 86 11 cl 18 1.	🛛 🚛 Key Usage Digital Signature, Certificate Signing, Off-II
Enhanced Key Usage Server Authentication (1.3.6.1.5.5.7.3.1)	Certificate Templat SubCA	Subject Key Ident 52 2e e5 2c 38 29 d6 da 81 19 11 70 74 00
E Subject Alternative IP Address=14.36.157.21	Authority Key Identif KeyID=52 2e e5 2c 38 29 d6 da 81 19 11	CA Version V0.0
Authority Key Identi KeyID=fe 34 ca 8d 22 9b 6e d7 a6 86 11	CRL Distribution Pol [1]CRL Distribution Point: Distribution Pol	Basic Constraints Subject Type=CA, Path Length Constraint= ::
CRL Distribution Pol [1]CRL Distribution Point: Distribution Pol	Authority Informatio [1] Authority Info Access: Access Method	Thumbprint algori sha1
Authority Informati [1] Authority Info Access: Access Method +	Key Usage Digital Signature, Certificate Signing, Off-L -	Thumbprint cb 24 48 a5 30 11 72 a3 da 9e 31 d1 f3 f6 +
•	★	K
V3	V3	V3
	H	
Edit Properties Copy to File	Edit Properties Copy to File	Edit Properties Copy to File
Learn more about certificate details	Learn more about certificate details	Learn more about certificate details
OK	OK	OK

### ISE 인증서 체인이 올바르지만 엔드포인트가 인증 중에 ISE의 서버 인증서를 거부함

SSL 핸드셰이크 중에 ISE가 전체 인증서 체인을 제공하고 서 플리 컨 트가 여전히 인증서 체인을 거부 중인 경우다음 단계는 루트 및 중간 인증서가 클라이언트 로컬 트러스트 저장소에 있는지 확 인하는 것입니다.

Windows 장치에서 이를 확인하려면 mmc.exe 파일 > 스냅인 추가-제거 로 이동합니다.사용 가능한 스냅인 열에서 인증서를 선택하고 추가를 클릭합니다.사용 중인 인증 유형(사용자 또는 시스템)에 따라 **내 사용자 계정** 또는 컴퓨터 계정을 선택한 다음 확인을 클릭합니다.

콘솔 보기에서 Trusted Root Certification Authorities 및 Intermediate Certification Authorities를 선 택하여 로컬 트러스트 저장소에 루트 및 중간 인증서가 있는지 확인합니다.

Console1 - [Console Root\Certificates - Current User\Tru:	sted Root Certification Authorities\0	.ertificates]				
💊 File Action View Favorites Window Help						
◆ ⇒   2 🗊 🗓   9 🕞 월 🗊						
Console Root	Issued To	Issued By	Expiration	Intended Purpo	Friendly Name	Sta
A 🕼 Certificates - Current User	AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenti	USERTrust	
Personal	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenti	Baltimore Cybe	
Trusted Root Certification Authorities	Certum CA	Certum CA	6/11/2027	Server Authenti	Certum	
Certificates	Gisco Root CA 2048	Cisco Root CA 2048	5/14/2029	<all></all>	<none></none>	
Enterprise Trust Intermediate Certification Authorities	GCisco Root CA M1	Cisco Root CA M1	11/18/2033	<all></all>	<none></none>	
Certificate Revocation List	Class 2 Primary CA	Class 2 Primary CA	7/6/2019	Secure Email, S.,	CertPlus Class 2	
Certificates	Glass 3 Public Primary Ce	Class 3 Public Primary Certi	8/1/2028	Secure Email, C	VeriSign Class 3	
Active Directory User Object	COMODO RSA Certificati	COMODO RSA Certificatio	1/18/2038	Server Authenti	COMODO	
Trusted Publishers	Copyright (c) 1997 Micro	Copyright (c) 1997 Microso	12/30/1999	Time Stamping	Microsoft Time	
Untrusted Certificates	DigiCert Assured ID Root	DigiCert Assured ID Root C	11/9/2031	Server Authenti	DigiCert	
Third-Party Root Certification Authorities	DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenti	DigiCert	
Trusted People	DigiCert High Assurance	DigiCert High Assurance E.,	11/9/2031	Server Authenti	DigiCert	
Display the second s	DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, S	DST Root CA X3	
Certificate Enrollment Requests	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></none>	
Smart Card Trusted Roots	E Fataut Boot Cartification	Entrust Print Castification	11/07/0006	Course Authorst'	Entrant	

서버 ID 확인 문제인지 쉽게 확인할 수 있는 방법은 서 플리 컨 트 프로필 컨피그레이션 아래 Validate Server Certificate(서버 인증서 검증)를 선택 취소하고 다시 테스트하십시오.

Connection Security	When connecting:
Security type: WPA2-Enterprise	Connect to these servers:
Encryption type: AES	Trusted Root Certification Authorities:
	AddTrust External CA Root
	Baltimore CyberTrust Root
Choose a network authentication method:	Certum CA
Microsoft: Protected EAP (PEAP)	Cisco Root CA 2048
	Cisco Root CA M1
Remember my credentials for this connection each	Class 2 Primary CA
time I'm logged on	Class 3 Public Primary Certification Authority
	COMODO DOL CUMPLINA A Abusta

## 관련 정보

- <u>Cisco Identity Services Engine 관리자 가이드, 릴리스 3.0</u>
- <u>기술 지원 및 문서 Cisco Systems</u>