

ISE에서 TLS/SSL 인증서 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[서버 인증서](#)

[ISE 인증서](#)

[시스템 인증서](#)

[신뢰할 수 있는 인증서 저장소](#)

[기본 작업](#)

[자체 서명 인증서 생성](#)

[자체 서명 인증서 갱신](#)

[신뢰할 수 있는 인증서 설치](#)

[CA 서명 인증서 설치](#)

[인증서 및 개인 키 백업](#)

[문제 해결](#)

[인증서 유효성 검사](#)

[인증서 삭제](#)

[신청자가 802.1x 인증에서 ISE 서버 인증서를 신뢰하지 않음](#)

[ISE 인증서 체인이 올바르지만 엔드포인트가 인증 중에 ISE 서버 인증서를 거부합니다.](#)

[자주 묻는 질문\(FAQ\)](#)

[ISE에서 인증서가 이미 존재한다는 경고를 보낼 때 수행할 작업](#)

[브라우저에서 ISE의 포털 페이지가 신뢰할 수 없는 서버에 의해 표시된다는 경고를 보내는 이유는 무엇입니까?](#)

[유효하지 않은 인증서로 인해 업그레이드가 실패할 경우 어떻게 해야 합니까?](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ISE의 TLS/SSL 인증서, ISE 인증서의 종류 및 역할, 일반적인 작업 수행 방법 및 문제 해결, FAQ에 대한 답변을 제공합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

1. Cisco ISE(Identity Services Engine)
2. 서로 다른 유형의 ISE 및 AAA 구축을 설명하는 데 사용되는 용어.
3. RADIUS 프로토콜 및 AAA 기본 사항
4. SSL/TLS 및 x509 인증서

5. PKI(Public Key Infrastructure) 기본

사용되는 구성 요소

이 문서의 정보는 Cisco ISE, 릴리스 2.4 - 2.7 소프트웨어 및 하드웨어 버전을 기반으로 합니다. 버전 2.4에서 2.7까지의 ISE를 지원하지만 달리 명시되지 않는 한 다른 ISE 2.x 소프트웨어 릴리스와 유사하거나 동일해야 합니다.

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

서버 인증서

서버 인증서는 서버에서 신뢰성을 위해 클라이언트에 서버의 ID를 제시하고 통신을 위한 보안 채널을 제공하는 데 사용됩니다. 이러한 인증서는 자체 서명(서버가 자신에게 인증서를 발급하는 경우) 또는 인증 기관(조직 내부 또는 유명 공급업체에서 발급)에 의해 발급될 수 있습니다.

서버 인증서는 일반적으로 서버의 호스트 이름 또는 FQDN(Fully Qualified Domain Name)에 발급되거나 와일드카드 인증서(*.domain.com). 발급된 호스트, 도메인 또는 하위 도메인은 일반적으로 CN(Common Name) 또는 SAN(Subject Alternative Name) 필드에 언급됩니다.

와일드카드 인증서는 와일드카드 표기법(호스트 이름 대신 별표)을 사용하여 조직의 여러 호스트 간에 동일한 인증서를 공유할 수 있도록 하는 SSL 인증서입니다. 예를 들어 와일드카드 인증서에 대한 CN 또는 SAN 값 주체 이름은 다음과 비슷할 수 있습니다 *.company.com 이 도메인의 모든 호스트(예: server1.com, server2.com 등).

인증서는 일반적으로 공개 키 암호화 또는 비대칭 암호화를 사용합니다.

- 공개 키: 공개 키는 필드 중 하나의 인증서에 있으며, 디바이스에서 통신을 시도할 때 시스템에서 공개적으로 공유합니다.
- 개인 키: 개인 키는 엔드 시스템의 개인이며 공개 키와 쌍을 이룹니다. 공개 키로 암호화된 데이터는 쌍을 이룬 특정 개인 키에서만 해독할 수 있으며 그 반대의 경우도 마찬가지입니다.

ISE 인증서

Cisco ISE는 PKI(Public Key Infrastructure)에 의존하여 엔드포인트, 사용자, 관리자 등과의 보안 통신 및 다중 노드 구축의 Cisco ISE 노드 간 보안 통신을 제공합니다. PKI는 x.509 디지털 인증서를 사용하여 메시지의 암호화 및 해독을 위한 공개 키를 전송하고 사용자 및 디바이스에서 제공하는 다른 인증서의 신뢰성을 확인합니다. Cisco ISE에는 일반적으로 사용되는 두 가지 인증서 범주가 있습니다.

- 시스템 인증서: 클라이언트에 대한 Cisco ISE 노드를 식별 하는 서버 인증서입니다. 모든 Cisco ISE 노드에는 자체 로컬 인증서가 있으며, 각 인증서는 해당 개인 키와 함께 노드에 저장됩니다.

- 신뢰할 수 있는 인증서 저장 인증서: 이는 다양한 용도로 ISE에 제공된 인증서를 검증하는 데 사용되는 CA(Certificate Authority) 인증서입니다. 인증서 저장소의 이러한 인증서는 1 기본 관리 노드에서 관리 되고 분산 된 Cisco ISE 구축의 모든 다른 노드에 복제 됩니다. 인증서 저장에는 BYOD를 위해 ISE의 내부 인증 기관에서 ISE 노드에 대해 생성된 인증서도 포함되어 있습니다.

시스템 인증서

시스템 인증서는 하나 이상의 역할에 사용할 수 있습니다. 각 역할은 서로 다른 목적을 수행하며 여기에서 설명합니다.

- Admin(관리): 443(관리 GUI)을 통한 모든 통신, 복제 및 여기에 나열되지 않은 모든 포트/사용에 대해 보안을 설정하는 데 사용됩니다.
- 포털: CWA(Centralized Web Authentication) 포털, 게스트, BYOD, 클라이언트 프로비저닝, Native Supplicant Provisioning 포털 등의 포털을 통한 HTTP 통신을 보호하는 데 사용됩니다. 각 포털은 특별히 태그가 지정된 인증서의 포털에 사용할 것을 지시하는 포털 그룹 태그(기본값: Portal Group Tag)에 매핑되어야 합니다. 인증서의 Edit(수정) 옵션에 있는 Portal Group Tag name(포털 그룹 태그 이름) 드롭다운 메뉴를 사용하면 새 태그를 생성하거나 기존 태그를 선택할 수 있습니다.
- EAP: 802.1x 인증을 위해 클라이언트에 제공되는 인증서를 지정하는 역할입니다. 인증서는 EAP-TLS, PEAP, EAP-FAST 등 가능한 거의 모든 EAP 방법과 함께 사용됩니다. PEAP 및 FAST와 같은 터널링된 EAP 방법에서는 TLS(Transport Layer Security)를 사용하여 자격 증명 교환을 보호합니다. 보안 교환을 위해 이 터널이 설정될 때까지 클라이언트 자격 증명이 서버로 전송되지 않습니다.
- RADIUS DTLS: 이 역할은 NAD(Network Access Device)와 ISE 간의 RADIUS 트래픽을 암호화하는 DTLS 연결(UDP를 통한 TLS 연결)에 사용할 인증서를 지정합니다. 이 기능이 작동하려면 NAD가 DTLS 암호화가 가능해야 합니다.
- SAML: 서버 인증서는 SAML IdP(Identity Provider)와의 통신을 보호하는 데 사용됩니다. SAML 사용을 위해 지정된 인증서는 Admin(관리), EAP Authentication(EAP 인증) 등의 다른 서비스에 사용할 수 없습니다.
- ISE 메시징 서비스: 2.6부터 ISE는 데이터를 로깅하기 위해 레거시 Syslog 프로토콜 대신 ISE 메시징 서비스를 사용합니다. 이 통신은 이 통신을 암호화하는 데 사용됩니다.
- PxGrid: 이 인증서는 ISE의 PxGrid 서비스에 사용됩니다.

ISE를 설치하면 Default Self-Signed Server Certificate. 이는 기본적으로 EAP 인증, 관리, 포털 및 RADIUS DTLS에 할당됩니다. 이러한 역할은 내부 CA 또는 잘 알려진 CA 서명 인증서로 이동하는 것이 좋습니다.

Friendly Name	Used By	Portal group tag	Valid From	Expiration Date
OU=Certificate Services System Certificate, CN=hongkongise.riverdale.local#Certificate Services Endpoint Sub CA - hongkongise#00002	pxGrid	hongkongise.riverdale.local	Mon, 13 Apr 2020	Sun, 14 Apr 2030
OU=ISE Messaging Service, CN=hongkongise.riverdale.local#Certificate Services Endpoint Sub CA - hongkongise#00001	ISE Messaging Services	hongkongise.riverdale.local	Mon, 13 Apr 2020	Sun, 14 Apr 2030
Default self-signed saml server certificate - CN=SAML_hongkongise.riverdale.local	SAML	SAML_hongkongise.riverdale.local	Tue, 14 Apr 2020	Wed, 14 Apr 2021
Default self-signed server certificate	Default Portal Certificate Group	hongkongise.riverdale.local	Tue, 14 Apr 2020	Wed, 14 Apr 2021

팁: ISE 서버의 FQDN 및 IP 주소를 모두 ISE 시스템 인증서의 SAN 필드에 추가하는 것이 좋습니다. 일반적으로 Cisco ISE의 인증서 인증이 인증서 기반 확인 기능의 사소한 차이에 의해 영향을 받지 않도록 하려면 네트워크에 구축된 모든 Cisco ISE 노드에 대해 소문자 호스트 이름을 사용합니다.

참고: ISE 인증서의 형식은 PEM(Privacy Enhanced Mail) 또는 DER(Distinguished Encoding Rules)여야 합니다.

신뢰할 수 있는 인증서 저장소

인증 기관 인증서는 Administration > System > Certificates > Certificate Store Cisco의 IT 조직이 Trust for client authentication use-case를 사용하여 ISE가 엔드포인트, 디바이스 또는 기타 ISE 노드에서 제공한 인증서를 검증하는 데 이러한 인증서를 사용하는지 확인합니다.

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Mon, 12 May 2025
Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00 ...	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 2029
Cisco ECC Root CA	Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 2053
Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 2038
Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA ...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037
Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54 ...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029
Cisco Root CA 2099	Enabled	Cisco Services	01 9A 33 58 78 CE ...	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016	Sun, 9 Aug 2099
Cisco Root CA M1	Enabled	Cisco Services	2E D2 0E 73 47 D3...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 2033
Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037
Cisco RXC-R2	Enabled	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034
Default self-signed server certificate	Enabled	Endpoints Infrastructure	5E 95 93 55 00 00 ...	hongkongise.riverdale.local	hongkongise.riverdale.local	Tue, 14 Apr 2020	Wed, 14 Apr 2021
DigCert Global Root CA	Enabled	Cisco Services	08 3B E0 56 90 42 ...	DigCert Global Root CA	DigCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov 2031
DigCert root CA	Enabled	Endpoints Infrastructure	02 AC 5C 26 6A 0B...	DigCert High Assurance ...	DigCert High Assurance ...	Fri, 10 Nov 2006	Mon, 10 Nov 2031
DigCert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure	04 E1 E7 A4 DC 5C...	DigCert SHA2 High Assu...	DigCert High Assurance ...	Tue, 22 Oct 2013	Sun, 22 Oct 2028
DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A3...	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2006	Thu, 30 Sep 2021
HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 D0 ...	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 2023
QuoVadis Root CA 2	Enabled	Cisco Services	05 09	QuoVadis Root CA 2	QuoVadis Root CA 2	Fri, 24 Nov 2006	Mon, 24 Nov 2031
Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5...	thawte Primary Root CA	thawte Primary Root CA	Fri, 17 Nov 2006	Wed, 16 Jul 2036
VerSign Class 3 Public Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D...	VerSign Class 3 Public Pr...	VerSign Class 3 Public Pr...	Wed, 8 Nov 2006	Wed, 16 Jul 2036
VerSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03...	VerSign Class 3 Secure ...	VerSign Class 3 Public Pr...	Mon, 8 Feb 2010	Fri, 7 Feb 2020

기본 작업

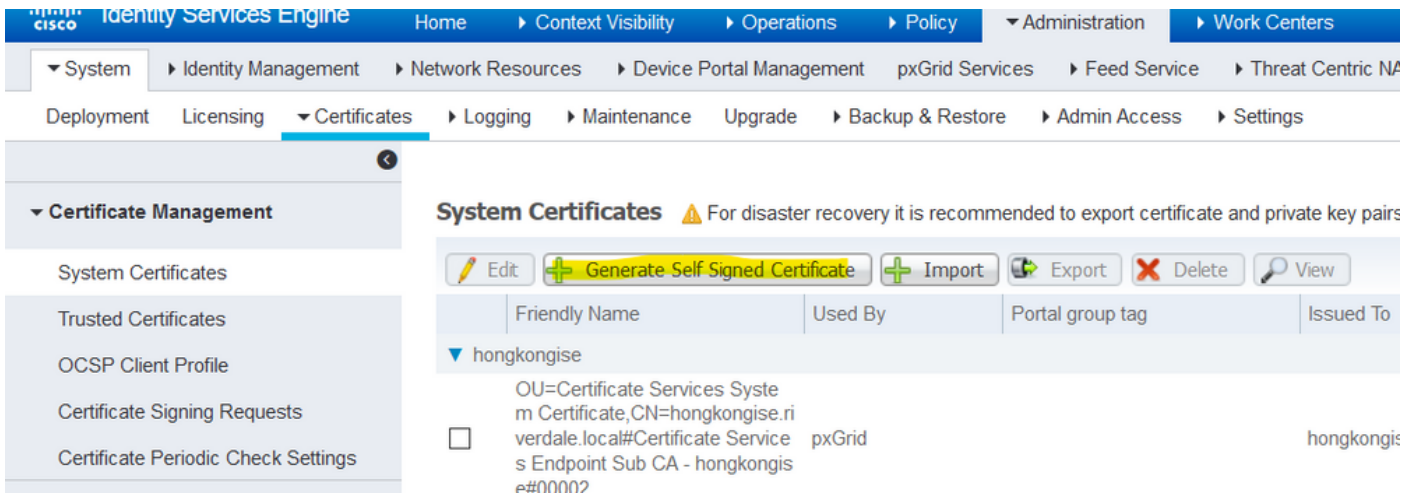
인증서는 만료 날짜가 있으므로 취소하거나 특정 시점에 교체해야 할 수 있습니다. ISE 서버 인증서

가 만료되면 새로운 유효한 인증서로 대체되지 않는 한 심각한 문제가 발생할 수 있습니다.

참고: EAP(Extensible Authentication Protocol)에 사용되는 인증서가 만료되면 클라이언트가 더 이상 ISE 인증서를 신뢰하지 않으므로 클라이언트 인증이 실패할 수 있습니다. 포털에 사용되는 인증서가 만료되면 클라이언트 및 브라우저에서 포털에 대한 연결을 거부할 수 있습니다. 관리자 사용 인증서가 만료되면 위험은 더욱 커지므로 관리자가 더 이상 ISE에 로그인할 수 없으며 분산 구축이 정상적으로 작동하지 않을 수 있습니다.

자체 서명 인증서 생성

새 자체 서명 인증서를 생성하려면 Administration > System > Certificates > System Certificates. 다음을 클릭합니다. Generate Self Signed Certificate.



이 목록에서는 Generate Self Signed Certificate(자체 서명 인증서 생성) 페이지의 필드에 대해 설명합니다.

자체 서명 인증서 설정 필드 이름 사용 지침:

- 노드 선택: (필수) 시스템 인증서를 생성하는 데 필요한 노드입니다.
- CN: (SAN이 지정되지 않은 경우 필수) 기본적으로 CN은 자체 서명 인증서가 생성되는 ISE 노드의 FQDN입니다.
- OU(조직 단위): 조직 단위 이름(예: Engineering).
- Organization (O)(조직(O)): Cisco와 같은 조직 이름입니다.
- 구/군/시(L): (약어 사용 안 함) 구/군/시 이름(예: San Jose).
- 주(ST): (약어 사용 안 함) 주 이름(예: California).
- 국가(C): 국가 이름 두 글자로 된 ISO 국가 코드가 필요합니다. 예를 들면 미국입니다.
- SAN: 인증서와 연결된 IP 주소, DNS 이름 또는 URI(Uniform Resource Identifier)입니다.
- Key Type(키 유형): 공개 키를 만드는 데 사용할 알고리즘을 지정합니다(RSA 또는 ECDSA).
- Key Length(키 길이): 공개 키의 비트 크기를 지정합니다. 이러한 옵션은 RSA: 512 1024 2048 4096에 사용할 수 있으며 ECDSA: 256 384에 사용할 수 있습니다.
- Digest to Sign With(다음으로 서명할 다이제스트): SHA-1 또는 SHA-256 해시 알고리즘 중 하나를 선택합니다.
- 인증서 정책: 인증서가 준수해야 하는 인증서 정책 OID 또는 OID 목록을 입력합니다. 쉼표나 공백을 사용하여 OID를 구분합니다.
- Expiration TTL(만료 TTL): 인증서가 만료될 때까지의 일 수를 지정합니다.

- Friendly Name(친숙한 이름): 인증서의 친숙한 이름을 입력합니다. 이름을 지정하지 않으면 Cisco ISE는 자동으로 형식의 이름을 생성합니다 위치 고유한 5자리 숫자입니다.
- Allow Wildcard Certificates(와일드카드 인증서 허용): Subject(주체)의 CN 및/또는 SAN의 DNS 이름에 별표(*)가 포함된 자체 서명 와일드카드 인증서(인증서)를 생성하려면 이 확인란을 선택합니다. 예를 들어 SAN에 할당된 DNS 이름은 *.domain.com.
- Usage(사용): 이 시스템 인증서를 사용해야 하는 서비스를 선택합니다. 사용 가능한 옵션은 다음과 같습니다.

관리자EAP 인증RADIUS DTLSPxGridSAML포털

The screenshot displays the 'Generate Self Signed Certificate' configuration interface in Cisco ISE. The left sidebar shows the navigation menu with 'Certificate Management' expanded. The main content area includes the following fields and settings:

- * Select Node:** hongkongse
- Subject:**
 - Common Name (CN): SFODNS
 - Organizational Unit (OU): Security
 - Organization (O): IT
 - City (L): Kokata
 - State (ST): West Bengal
 - Country (C): IN
- Subject Alternative Name (SAN):** IP Address, 10.127.196.248
- * Key type:** RSA
- * Key Length:** 2048
- * Digest to Sign With:** SHA-256
- Certificate Policies:** (Empty field)

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

System Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Settings

Certificate Authority

Subject Alternative Name (SAN) IP Address 10.127.196.248

* Key type RSA

* Key Length 2048

* Digest to Sign With SHA-256

Certificate Policies

* Expiration TTL 10 years

Friendly Name

Allow Wildcard Certificates

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- SAML: Use certificate for SAML Signing
- Portal: Use for portal

Submit Cancel

참고: RSA 및 ECDSA 공개 키는 동일한 보안 수준에 대해 서로 다른 키 길이를 가질 수 있습니다. 공용 CA 서명 인증서를 얻거나 FIPS 호환 정책 관리 시스템으로 Cisco ISE를 구축하려는 경우 2048을 선택합니다.

자체 서명 인증서 갱신

존재하는 자체 서명 인증서를 보려면 Administration > System > Certificates > System Certificates ISE 콘솔에 있습니다. 동일한 ISE 서버 FQDN에서 언급되는 경우 'Issued To' 및 'Issued By'가 있는 인증서는 자체 서명 인증서입니다. 이 인증서를 선택하고 Edit.

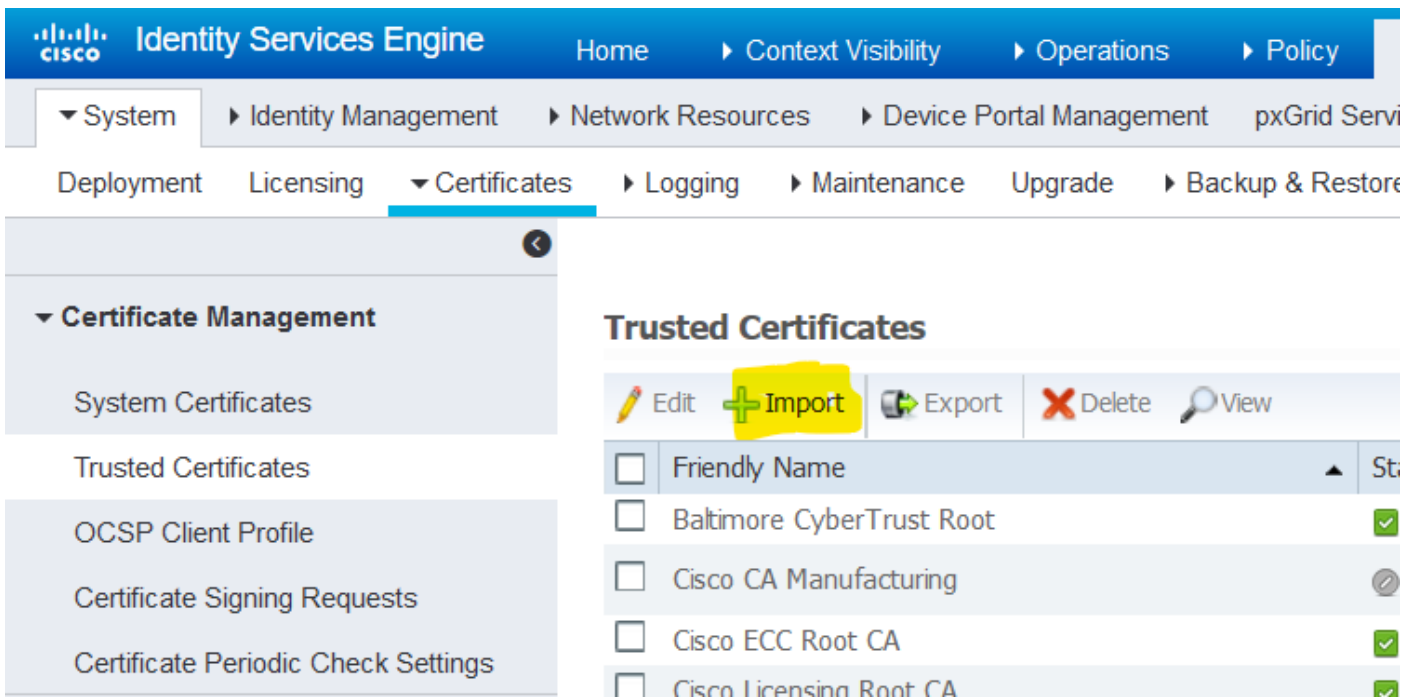
아래 Renew Self Signed Certificate을(를) 선택합니다. Renewal Period Expiration TTL(만료 TTL)을 설정합니다. 마지막으로 Save.

신뢰할 수 있는 인증서 설치

루트 CA, 중간 CA 및/또는 신뢰해야 하는 호스트에서 Base 64 인코딩 인증서를 가져옵니다.

1. ISE 노드에 로그인하고 Administration > System > Certificate > Certificate Management > Trusted Certificates 을 클릭

릭하고 Import이 그림에 나와 있는 것처럼.

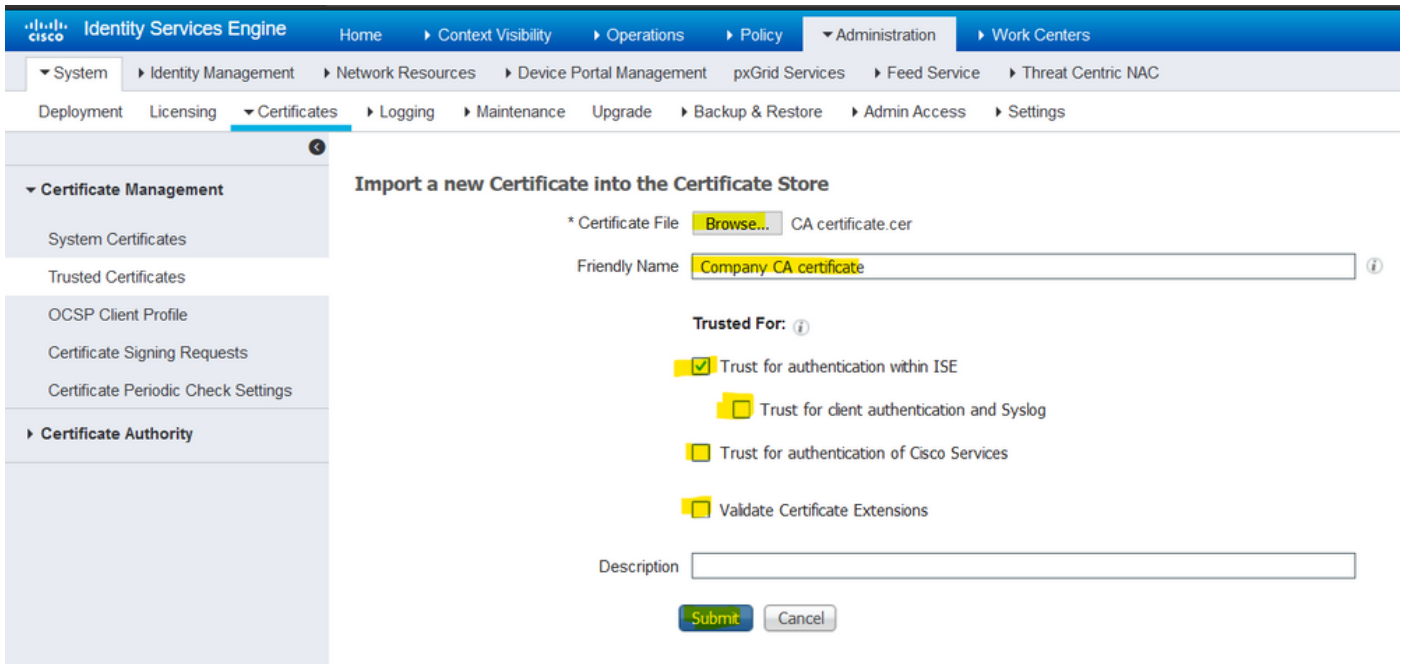


2. 다음 페이지에서 가져온(앞에서 설명한 것과 같은 순서로) CA 인증서를 업로드합니다. 사용자에게 친숙한 이름 및 인증서 용도를 설명하는 설명을 할당하여 계속 추적합니다.

사용 요구에 따라 다음 옆에 있는 상자를 선택합니다.

- Trust for authentication within ISE(ISE 내 인증 신뢰) - 동일한 신뢰받는 CA 인증서가 신뢰받는 인증서 저장소에 로드된 경우 새 ISE 노드를 추가하기 위한 것입니다.
- Trust for client authentication and Syslog(클라이언트 인증 및 Syslog 신뢰) - 인증서를 사용하여 EAP를 통해 ISE에 연결하는 엔드포인트를 인증하거나 보안 Syslog 서버를 신뢰하려면 이 옵션을 활성화합니다.
- Cisco Services의 인증 신뢰 - 피드 서비스와 같은 외부 Cisco 서비스를 신뢰하는 경우에만 필요합니다.

3. 마지막으로 Submit. 이제 인증서가 신뢰할 수 있는 저장소에 표시되고 모든 보조 ISE 노드(구축에 있는 경우)와 동기화되어야 합니다.



CA 서명 인증서 설치

루트 및 중간 CA 인증서가 신뢰할 수 있는 인증서 저장소에 추가되면 CSR(Certificate Signing Request)이 발행되고 CSR을 기반으로 서명된 인증서가 ISE 노드에 바인딩될 수 있습니다.

1. 이렇게 하려면 다음으로 이동합니다. Administration > System > Certificates > Certificate Signing Requests 클릭 하여 **Generate Certificate Signing Requests (CSR)** CSR을 생성합니다

2. 표시되는 페이지의 사용 섹션에 있는 드롭다운 메뉴에서 사용할 역할을 선택합니다.

인증서가 여러 역할에 사용되는 경우 Multi-Use를 선택합니다. 인증서가 생성되면 필요한 경우 역할을 변경할 수 있습니다. 대부분의 경우 인증서는 Used For(용도) 드롭다운에서 Multi-use(다중 사용)에 사용하도록 설정할 수 있습니다. 이렇게 하면 모든 ISE 웹 포털에서 인증서를 사용할 수 있습니다.

3. ISE 노드 옆의 확인란을 선택하여 인증서가 생성되는 노드를 선택합니다.

4. 와일드카드 인증서를 설치/생성하려면 Allow Wildcard Certificates 상자를 클릭합니다.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

Certificate Authority

Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:


ISE Identity Certificates:

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate
- ISE Messaging Service - This is not a signing request, but an ability to generate a brand new Messaging certificate.

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for  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
<input type="checkbox"/> hongkongise	hongkongise#Multi-Use

Usage

Certificate(s) will be used for  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
<input type="checkbox"/> hongkongise	hongkongise#Multi-Use

5. 주최자 또는 조직(조직 단위, 조직, 시, 도, 국가)에 대한 내용을 바탕으로 주제 정보를 입력합니다

6. 이 작업을 완료하려면 다음을 클릭하십시오. Generate을 클릭한 다음 Export 표시되는 팝업입니다.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

▼ Certificate Management

- System Certificates
- Trusted Certificates
- OCSF Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

▶ Certificate Authority

hongkongise hongkongise#Multi-Use

Subject

Common Name (CN) \$FQDN\$ ⓘ

Organizational Unit (OU) Security ⓘ

Organization (O) IT ⓘ

City (L) Kolkata

State (ST) West Bengal

Country (C) IN

Subject Alternative Name (SAN) IP Address 10.127.196.248 - + ⓘ

* Key type RSA ⓘ

* Key Length 2048 ⓘ

* Digest to Sign With SHA-256

Certificate Policies

Generate Cancel

Country (C) IN

Subject Alternative Name (SAN) | - + ⓘ

- DNS Name
- IP Address
- Uniform Resource Identifier
- Directory Name

* Key type RS

* Key Length 2048 ⓘ

* Digest to Sign With SHA 256

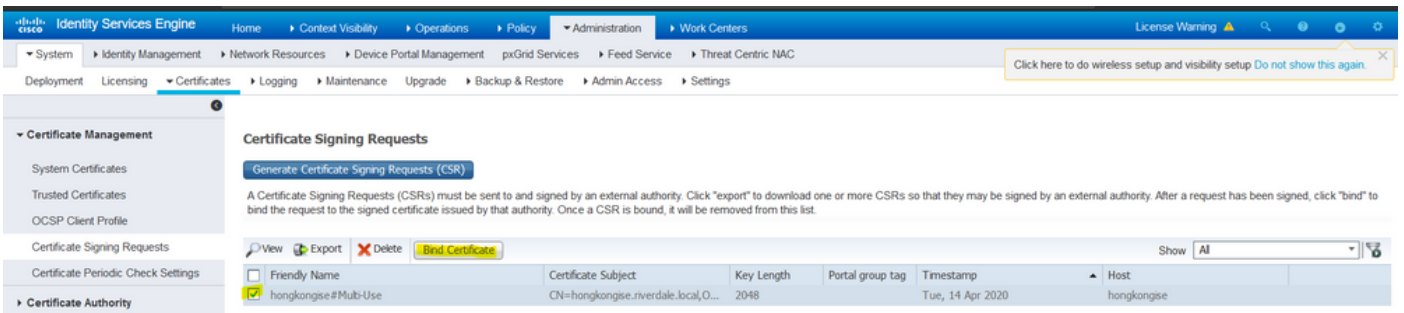
방금 생성한 Base64 인코딩 인증서 요청 요청을 다운로드합니다. 이 PEM 파일은 서명을 위해 CA로 전송되어야 하며, 그 결과로 서명된 인증서 CER 파일(Base64 인코딩)을 얻어야 합니다.

참고: CN 필드 아래에서 ISE는 노드 FQDN을 자동으로 채웁니다.

참고: ISE 1.3 및 1.4에서는 pxGrid를 사용하려면 적어도 두 개의 CSR을 발급해야 했습니다. 하나는 pxGrid 전용이고, 다른 하나는 나머지 서비스에 사용됩니다. 2.0 이상 버전부터는 이 모든 것이 하나의 CSR에 포함되어 있습니다.

참고: 인증서가 EAP 인증에 사용되는 경우 Windows 신청자가 서버 인증서를 거부하므로 '*' 기호가 Subject CN 필드에 없어야 합니다. 서 플리 컨 트에서 서버 ID를 확인 할 수 없는 경우 에도 SSL 핸드셰이크는 CN 필드에 '*'가 있는 경우 실패 할 수 있습니다. 대신 일반 FQDN을 CN 필드에 사용할 수 있으며 *.domain.com SAN DNS Name(SAN DNS 이름) 필드에서 사용할 수 있습니다. 일부 CA(Certificate Authorities)는 CSR에 없는 경우에도 인증서의 CN에 와일드 카드(*)를 자동으로 추가할 수 있습니다. 이 시나리오에서는 이 작업을 방지하기 위해 특별한 요청이 제기되어야 합니다.

7. CA가 인증서를 서명하면(비디오에 표시된 대로 CSR에서 생성한 경우 [여기서](#) Microsoft CA가 사용되는 경우) ISE GUI로 돌아가서 **Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Management(인증서 관리) > Certificate Signing Request(인증서 서명 요청)**로 이동합니다. 앞서 생성한 CSR 옆에 있는 상자를 선택하고 Bind Certificate(인증서 바인딩) 버튼을 클릭합니다.



8. 그런 다음 방금 받은 서명된 인증서를 업로드하고 ISE의 이름을 지정합니다. 그런 다음 인증서 (예: Admin 및 EAP 인증, Portal 등)에 대한 필요에 따라 사용 옆에 있는 상자를 선택하고 Submit, 이 이미지에 표시된 대로

Identity Services Engine Administration > Work Centers > Certificates > Bind CA Signed Certificate

* Certificate File:

Friendly Name:

Validate Certificate Extensions:

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- Portal: Use for portal

* Portal group tag:

Portal(s) using this tag

BYOD Portal (default)	Blacklist Portal (default)
Certificate Provisioning Portal (default)	Client Provisioning Portal (default)
Hotspot Guest Portal (default)	MDM Portal (default)
My Devices Portal (default)	Self-Registered Guest Portal (default)
Sponsor Portal (default)	Sponsored Guest Portal (default)

이 인증서에 대해 Admin Role(관리자 역할)을 선택한 경우 ISE 노드는 서비스를 다시 시작해야 합니다. VM에 할당된 버전 및 리소스에 따라 이 작업에는 10~15분이 걸릴 수 있습니다. 애플리케이션의 상태를 확인하려면 ISE 명령줄을 열고 `show application status ise` 명령을 실행합니다.

Warning: Enabling Admin role for this certificate will cause an application server restart on the selected node.

Note: Make sure required Certificate Chain is imported under Trusted Certificates

Warning: The Portal tag is already assigned to the following certificate(s). If you proceed, it will be removed from the existing certificates, and affected portals will be restarted. Do you want to proceed?

- Default self-signed server certificate

인증서 가져오기에서 관리자 또는 포털 역할을 선택한 경우, 브라우저의 관리자 또는 포털 페이지에 액세스할 때 새 인증서가 사용되고 있는지 확인할 수 있습니다. 브라우저에서 잠금 기호를 선택하고 인증서에서 경로를 통해 전체 체인이 존재하고 시스템에서 신뢰할 수 있는지 확인합니다. 체인이 올바르게 구축되었고 브라우저에서 인증서 체인을 신뢰할 수 있는 경우 브라우저는 새 관리자 또는 포털 인증서를 신뢰해야 합니다.

참고: 현재 CA 서명 시스템 인증서를 갱신하려면 새 CSR을 생성하고 동일한 옵션으로 서명 인증서를 바인딩합니다. 활성 상태가 되기 전에 ISE에 새 인증서를 설치할 수 있으므로, 기존 인증서가 만료되기 전에 새 인증서를 설치할 계획입니다. 기존 인증서 만료 날짜와 새 인증서 시작 날짜 사이에 이 기간이 겹치면 인증서를 갱신하고 다운타임 없이 스왑을 계획할 수 있습니다. 시작 날짜가 이전 인증서 만료일 이전인 새 인증서를 가져옵니다. 이 두 날짜 사이의 기간은 변경 기간입니다. 새 인증서가 유효한 날짜 범위를 입력한 후, 필요한 프로토콜 (Admin/EAP/Portal) 를 활성화 합니다. 관리자 사용이 활성화된 경우 서비스가 다시 시작됩니다.

팁: 관리 및 EAP 인증서에는 회사 내부 CA를 사용하고 게스트/스폰서/핫스팟/기타 포털에는 공개적으로 서명된 인증서를 사용하는 것이 좋습니다. 그 이유는 사용자 또는 게스트가 네트워크에 접속하고 ISE 포털이 게스트 포털에 개인 서명 인증서를 사용하는 경우 인증서 오류가 발생하거나 브라우저가 포털 페이지에서 이들을 차단하게 될 수 있습니다. 이 모든 것을 방지하려면 더 나은 사용자 경험을 보장하기 위해 포털에서 사용할 공개 서명 인증서를 사용합니다. 또한 IP 주소를 통해 서버에 액세스할 때 인증서 경고가 발생하지 않도록 각 구축 노드 IP 주소를 SAN 필드에 추가해야 합니다.

인증서 및 개인 키 백업

내보내는 것이 좋습니다.

1. 모든 시스템 인증서(구축의 모든 노드에서)와 개인 키(재설치를 위해 필요)를 안전한 위치에 설치합니다. 인증서 컨피그레이션(인증서가 어떤 서비스에 사용되었는지)을 기록해 둡니다.
2. 기본 관리 노드의 신뢰할 수 있는 인증서 저장소의 모든 인증서 인증서 컨피그레이션(인증서가 어떤 서비스에 사용되었는지)을 기록해 둡니다.
3. 모든 인증기관 인증서

그러기 위해서는

1. 탐색 Administration > System > Certificates > Certificate Management > System Certificates. 인증서를 선택하고 Export. 선택 Export Certificates 및 개인 키 라디오 버튼. 개인 키 비밀번호를 입력하고 비밀번호를 확인합니다. 클릭 Export.
2. 탐색 Administration > System > Certificates > Certificate Management > Trusted Certificates. 인증서를 선택하고 Export. 클릭 Save File 인증서를 내보냅니다.
3. 탐색 Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates. 인증서를 선택하고 Export. 선택 Export Certificates 및 개인 키 라디오 버튼. 개인 키 비밀번호와 비밀번호 확인을 입력합니다. 클릭 Export. 클릭 Save File 인증서를 내보냅니다.

문제 해결

인증서 유효성 검사

Cisco ISE 신뢰할 수 있는 인증서 또는 시스템 인증서 저장소의 인증서가 만료되면 업그레이드 프로세스가 실패합니다. Trusted Certificates(신뢰할 수 있는 인증서) 및 System Certificates(시스템 인증서) 창의 Expiration Date(만료일) 필드에서 유효성을 확인합니다(Administration > System > Certificates > Certificate Management)를 다운로드하고 필요한 경우 업그레이드 전에 갱신하십시오.

또한 CA Certificates(CA 인증서) 창에서 인증서의 Expiration Date(만료일) 필드에서 유효성을 확인합니다(Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates)를 다운로드하고 필요한 경우 업그레이드 전에 갱신하십시오.

인증서 삭제

ISE의 인증서가 만료되거나 사용되지 않는 경우 이를 제거해야 합니다. 삭제하기 전에 인증서를 내 보내도록 합니다(해당하는 경우 개인 키 사용).

만료된 인증서를 삭제하려면 Administration > System > Certificates > Certificate Management. 다음을 클릭합니다 . System Certificates Store. 만료된 인증서를 선택하고 Delete. 신뢰할 수 있는 인증서 및 인증 기관 인증서 저장소에 대해 동일한 항목을 참조하십시오.

신청자가 802.1x 인증에서 ISE 서버 인증서를 신뢰하지 않음

ISE가 SSL 핸드셰이크 프로세스에 대한 전체 인증서 체인을 전송하는지 확인합니다.

클라이언트 OS 설정에서 서버 인증서(즉, PEAP) 및 서버 ID 검증을 필요로 하는 EAP 방법을 선택 하면 신청자는 인증 프로세스의 일부로 로컬 신뢰 저장소에 있는 인증서로 인증서 체인을 검증합니다. SSL 핸드셰이크 프로세스의 일부로서 ISE는 해당 인증서 및 체인에 있는 모든 루트 및/또는 중간 인증서를 제공합니다. 체인이 불완전하거나 신뢰 저장소에 이 체인이 없는 경우 서플리컨트가 서버 ID를 확인할 수 없습니다.

인증서 체인이 클라이언트로 다시 전달되었는지 확인하려면 ISE에서 패킷 캡처를 가져옵니다 (Operations > Diagnostic Tools > General Tools > TCP Dump 또는 인증 시 엔드포인트에서 Wireshark 캡처. 캡처를 열고 필터를 적용합니다. ssl.handshake.certificates Wireshark에서 액세스 과제를 찾습니다.

선택한 다음 Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates.

체인이 불완전한 경우 ISE로 이동합니다 Administration > Certificates > Trusted Certificates 루트 및/또는 중간 인증서가 있는지 확인합니다. 인증서 체인이 성공적으로 통과되면 여기에 설명된 방법으로 체인 자체가 유효한 것으로 검증되어야 합니다.

각 인증서(서버, 중간 및 루트)를 열고 각 인증서의 SKI(Subject Key Identifier)와 체인에 있는 다음 인증서의 AKI(Authority Key Identifier)가 일치하도록 신뢰 체인을 확인합니다.

ISE 인증서 체인이 올바르지만 엔드포인트가 인증 중에 ISE 서버 인증서를 거부합니다.

ISE가 SSL 핸드셰이크에 대한 전체 인증서 체인을 표시하고 신청자가 여전히 인증서 체인을 거부한 경우 다음 단계는 루트 및/또는 중간 인증서가 클라이언트 로컬 신뢰 저장소에 있는지 확인하는 것입니다.

Windows 디바이스에서 이를 확인하려면 을(를) 실행하십시오. mmc.exe(Microsoft Management Console), 다음으로 이동 File > Add-Remove Snap-in. 사용 가능한 스냅인 열에서 Certificates 을 클릭하고 Add. 다음 중 하나를 선택합니다. My user account 또는 Computer account 사용 중인 인증 유형(사용자 또는 머신)에 따라 OK .

콘솔 보기에서 신뢰할 수 있는 루트 인증 기관 및 중간 인증 기관을 선택하여 로컬 신뢰 저장소에 루트 및 중간 인증서가 있는지 확인합니다.

이 문제가 서버 ID 확인 문제인지 쉽게 확인할 수 있는 방법은 신청자 프로필 컨피그레이션에서 Validate Server Certificate(서버 인증서 검증)의 선택을 취소하고 다시 테스트하는 것입니다.

자주 묻는 질문(FAQ)

ISE에서 인증서가 이미 존재한다는 경고를 보내는 경우 어떻게 해야 하나요?

이 메시지는 ISE가 정확히 동일한 OU 매개변수를 사용하는 시스템 인증서를 탐지했으며 중복 인증서를 설치하려고 시도했음을 의미합니다. 중복 시스템 인증서는 지원되지 않으므로 새 인증서가 다르도록 시/도/부서 값을 약간 다른 값으로 변경하는 것이 좋습니다.

브라우저에서 ISE의 포털 페이지가 신뢰할 수 없는 서버에 의해 표시된다는 경고를 보내는 이유는 무엇입니까?

브라우저가 서버의 ID 인증서를 신뢰하지 않는 경우 이러한 현상이 발생합니다.

먼저, 브라우저에 표시되는 포털 인증서가 포털에 대해 ISE에서 예상되고 구성된 인증서인지 확인합니다.

둘째, FQDN을 통해 포털에 액세스해야 합니다. 사용 중인 IP 주소의 경우 인증서의 SAN 및/또는 CN 필드에 FQDN과 IP 주소가 모두 있어야 합니다.

마지막으로, 포털 인증서 체인(ISE 포털, 중간 CA, 루트 CA 인증서)을 클라이언트 OS/브라우저 소프트웨어에서 가져오거나 신뢰할 수 있는지 확인합니다.

참고: 일부 이후 버전의 iOS, Android OS 및 Chrome/Firefox 브라우저는 인증서에 대한 엄격한 보안 기대를 가지고 있습니다. 이러한 포인트가 충족되더라도 포털 및 중간 CA가 SHA-256 미만인 경우 연결을 거부할 수 있습니다.

유효하지 않은 인증서로 인해 업그레이드가 실패할 경우 어떻게 해야 하나요?

Cisco ISE 신뢰할 수 있는 인증서 또는 시스템 인증서 저장소의 인증서가 만료되면 업그레이드 프로세스가 실패합니다. Trusted Certificates(신뢰할 수 있는 인증서) 및 System Certificates(시스템 인증서) 창의 Expiration Date(만료일) 필드에서 유효성을 확인합니다(Administration > System > Certificates > Certificate Management)를 다운로드하고 필요한 경우 업그레이드 전에 갱신하십시오.

또한 CA Certificates(CA 인증서) 창에서 인증서의 Expiration Date(만료일) 필드에서 유효성을 확인합니다(Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates)를 다운로드하고 필요한 경우 업그레이드 전에 갱신하십시오.

ISE를 업그레이드하기 전에 내부 CA 인증서 체인이 유효한지 확인합니다.

탐색 Administration > System > Certificates > Certificate Authority Certificates. 구축의 각 노드에 대해 Friendly Name(친숙한 이름) 열에서 Certificate Services Endpoint Sub CA가 있는 인증서를 선택합니다. 클릭 View Certificate Status(인증서 상태)가 좋은 메시지이고 표시되는지 확인합니다.

인증서 체인이 깨진 경우 Cisco ISE 업그레이드 프로세스가 시작되기 전에 문제를 해결해야 합니다. 문제를 해결하려면 다음으로 이동하십시오. Administration > System > Certificates > Certificate Management > Certificate Signing Requests 및 ISE Root CA 옵션에 대해 하나를 생성합니다.

관련 정보

- [ISE 2.7 인증서 및 인증서 저장소 설정 관리](#)
- [ISE에서 디지털 인증서 구현](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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 번역 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.