Cisco Secure Firewall Impact of the Public CA Client Authentication EKU Changes Starting to Secure Communications(보안 통신을 위해 2026년 5월부터 시작되는 Cisco 보안 방화벽 영향)

소개

이 문서에서는 Chrome Root Certificate 프로그램을 준수하는 인증 기관에서, 특히 Cisco Secure Firewall 제품과 관련된 인증서 발급 기준에 대한 제한이 미치는 영향에 대해 설명합니다.

배경 정보

공개적으로 신뢰할 수 있는 TLS 인증서는 인증서 발급 및 사용을 제어하는 업계 정책을 준수해야 하는 CA에 의해 발급됩니다.

Google에서 운영하는 Chrome Root Program Policy는 Google Chrome 브라우저에서 인증서를 신뢰하기 위해 CA가 따라야 하는 요구 사항을 정의합니다. 이러한 요구 사항은 업계에서 공개적으로 신뢰할 수 있는 인증서를 발급하는 방법에 영향을 미칩니다. Chrome Root Program은 진화하는 보안 관행의 일환으로 인증서 사용에 대한 보다 엄격한 지침을 도입하고 있습니다.

따라서 많은 공용 CA가 클라이언트 인증 EKU를 포함하는 인증서 발급에서 벗어나 서버 인증만을 위한 인증서 발급으로 전환되고 있습니다. 따라서 많은 공용 CA에서 새로 발급된 인증서에는 서버 인증 EKU만 포함될 것으로 예상됩니다.

EKU(Extended Key Usage)는 디지털 인증서 내의 공개 키의 의도된 기능을 정의하는 인증서 확장입니다. 이 기능은 특정 암호화 작업에만 키가 사용되도록 허용된 응용 프로그램의 구조화된 집합을 설정합니다. 이 기능은 OID(Object Identifiers)(코드 서명, 서버 인증, 클라이언트 인증 또는 보안 전자 메일과 같은 허용된 각 사용을 분류하는 고유 숫자 식별자)에 의해 제어됩니다.

인증이 인증서를 기반으로 하는 경우 확인 엔티티가 인증서를 검토하여 EKU 내의 OID(Object Identifier)를 식별합니다. CA(Certificate Authority)는 EKU 확장을 포함시킴으로써 인증서의 범위를 미리 정의된 역할로 제한하며, 각각의 지정된 용도는 OID에 명시적으로 매핑됩니다.

EKU 특성의 용도

· 용도 정의: EKU 특성은 인증서가 수행할 수 있는 인증 또는 암호화 유형을 명확히 합니다.

· 보안 강화: EKU는 인증서를 특정 용도로 제한하여 오용되거나 의도하지 않은 애플리케이션(예: 클라이언트 인증에 서버 인증서를 사용할 수 없음)을 방지합니다.

· 규정 준수: 보안 정책 및 업계 표준에 따라 인증서가 사용되는지 확인합니다.

EKU 특성의 주요 용도

1. TLS 웹 클라이언트 인증

· 인증서를 사용하여 사용자 또는 장치를 식별하여 서버에 인증할 수 있습니다.

· OID: 1.3.6.1.5.5.7.3.2

· VPN, 상호 TLS 및 보안 로그인 시나리오에서 사용됩니다.

2. TLS 웹 서버 인증

· 클라이언트에서 인증서를 사용하여 ID를 확인할 수 있습니다.

· OID: 1.3.6.1.5.5.7.3.1

· HTTPS, SSL/TLS 웹 서버 및 보안 API 엔드포인트에서 사용

3. 코드 서명

· 인증서를 사용하여 소프트웨어 또는 실행 파일에 서명할 수 있음을 나타냅니다.

· OID: 1.3.6.1.5.5.7.3.3

· 소프트웨어 배포 및 무결성 검사에 사용됩니다.

4. 이메일 보호

· 인증서를 사용하여 이메일 메시지를 서명 및 암호화할 수 있습니다.

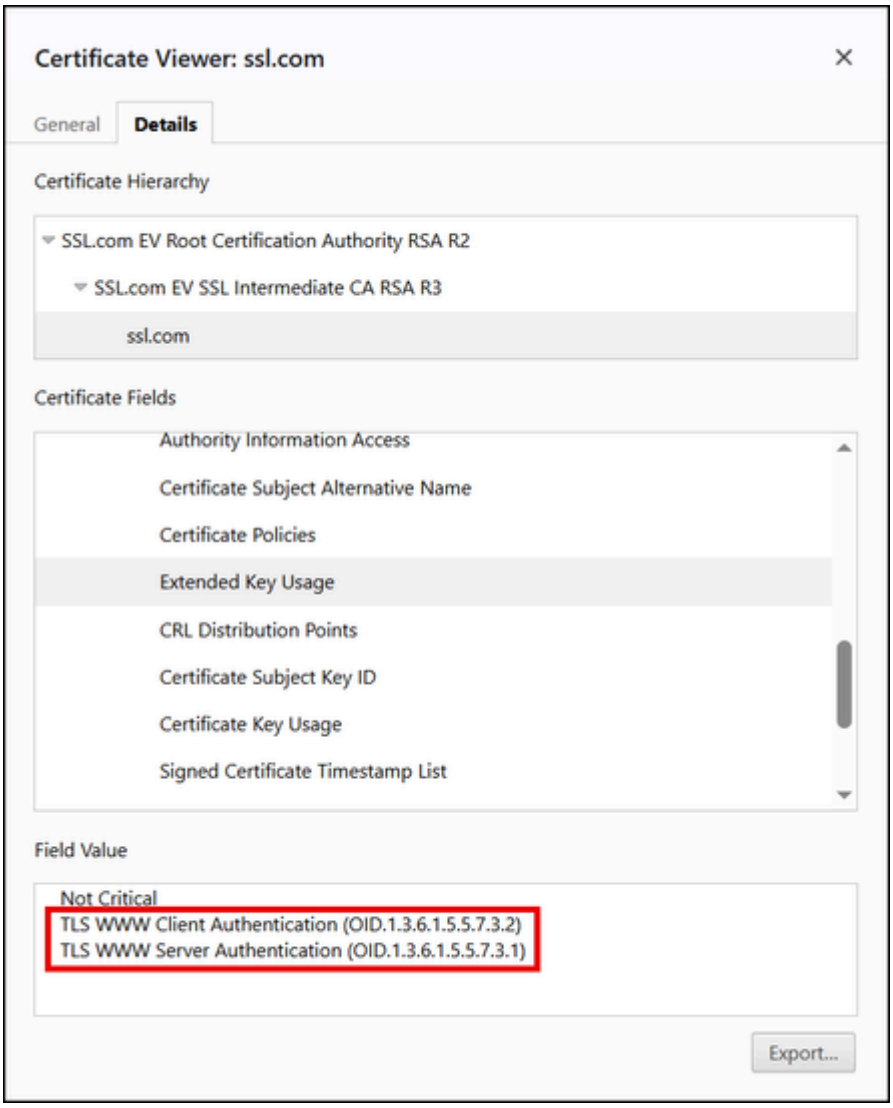
· OID: 1.3.6.1.5.5.7.3.4

· S/MIME 이메일 보안에 사용됩니다.

5. 그 밖의 용도

· 각각 고유 OID가 있는 문서 서명, 타임스탬프, 스마트 카드 로그온 등

브라우저와 서버는 HTTPS에 대한 보안 연결을 설정하기 위해 serverAuth EKU만 필요하지만, 역사적으로 많은 TLS 서버 인증서는 serverAuth와 clientAuthEKU를 모두 포함했습니다.



서버 인증서에서 클라이언트 인증 EKU를 제거하는 이유

- 보안 및 범위: 공용 TLS 인증서는 웹에서 서버를 인증하는 데만 사용됩니다. 이 제거 작업을 수행하면 서버와 클라이언트 기능이 명확하게 분리됩니다. ClientAuth EKU는 mTLS(Mutual TLS) 및 기타 인증 시나리오를 사용하여 머신 및 사용자를 인증하는 데 사용됩니다.

- 잘못된 컨피그레이션 방지: 일부 시스템은 EKU가 있는 경우 클라이언트 인증을 위해 공용 CA의 인증서를 신뢰할 수 있으며, 이는 보안 위험이 될 수 있습니다.

- 브라우저 요구 사항: 주요 브라우저는 웹 사이트의 인증서에서 clientAuth EKU를 요구하거나 확인하지 않습니다.

- 간소화된 PKI 아키텍처: CA는 사용을 분리하여 서버 TLS와 다른 용도를 위해 서로 다른 인증서 계층을 유지할 수 있습니다.

이는 Cisco Secure ASA(Firewall Adaptive Security Appliance), Cisco FTD(Secure Firewall Threat Defense), Cisco FDM(Secure Firewall Device Manager), Cisco FMC(Secure Firewall Management Center)와 같은 제품에서 특히 중요하며, 사용 사례에 따라 TLS 인증 중에 서버 또는 클라이언트 역할을 할 수 있습니다.

서버 환경에 미치는 영향

대부분의 서버 구축에서 이러한 변경은 영향이 적거나 없습니다. 예상되는 내용은 다음과 같습니다.

- 표준 웹 서버(HTTPS): 영향 없음. 업데이트된 인증서는 계속 정상적으로 작동합니다.

- 기존 인증서: 컷오프 전에 발급된 인증서는 만료될 때까지 계속 작동합니다.

- 상호 TLS(mTLS) 및 클라이언트 인증서 시나리오:클라이언트 인증에 TLS 서버 인증서를 사용하는 경우 다른 소스에서 clientAuth EKU로 별도의 인증서를 가져와야 합니다.

- 두 EKU가 모두 필요한 엔터프라이즈 시스템: 일부 레거시 또는 엔터프라이즈 시스템에는 두 EKU가 모두 필요합니다. 새 규칙을 준수하기 위해 업데이트가 필요한지 확인해야 합니다.

문제/장애 설명

2026년 5월부터 많은 공개 CA(인증 기관)가 클라이언트 EKU(Authentication Extended Key Usage)가 포함된 TLS(Transport Layer Security) 인증서 발급을 중지합니다. 새로 발급된 인증서에는 일반적으로 서버 인증 EKU만 포함됩니다.

그 결과, 공용 CA에서 발급한 인증서가 업데이트된 CA 정책에 따라 갱신되고 Cisco Secure Firewall 제품에 구축된 경우,

클라이언트 인증 EKU가 필요한 서비스가 실패합니다. 영향을 받는 특정 서비스는 다음과 같습니다.

- ASA, FTD, FDM 또는 FMC가 클라이언트 역할을 하는 경우(예: ISE(pxGrid), RADIUS, LDAPS 또는 Active Directory와 같은 인증 서버나 ID 공급자에 연결하는 경우), 클라이언트 인증서가 공용 CA에 의해 생성되었지만 클라이언트 인증 EKU가 없는 경우 인증서 기반 인증이 실패할 수 있습니다. 이러한 시나리오에서 인증 서버가 필수 EKU 없이 인증서를 거부하는 경우 연결 실패가 발생할 수 있습니다.

- Cisco Secure Client(이전의 AnyConnect)는 인증서를 사용하여 ASA 또는 FTD 서버에 인증할 수 있습니다. 그러나 클라이언트 인증서가 공용 CA에 의해 생성되었고 클라이언트 인증 EKU가 없는 경우 RAVPN(Remote Access VPN) 연결이 실패합니다.

- 인증서 인증(RSA 또는 ECDSA)을 사용하여 FTD 또는 ASA가 다른 FTD, ASA, Cisco 라우터 또는 서드파티 VPN 피어에 관계 없이 사이트 대 사이트 VPN 터널을 설정하는 경우, 공용 CA에서 생성된 ID 인증서에 클라이언트 인증 EKU 특성이 없으면 터널이 실패합니다. 이는 원격 VPN 피어에서 ID 인증서에 클라이언트 인증 EKU가 있어야 하기 때문에 발생합니다.

Chrome 루트 프로그램 정책 변경

EKU의 구현은 CA 서명 인증서에 따라 달라집니다. 서버 인증과 클라이언트 인증 EKU를 모두 사용하는 것은 일반적인 관례였습니다. 그러나 Chrome 루트 프로그램 정책 변경 CA의 일부로 이 인증서 발급 기준에 맞게 정렬되어 클라이언트 인증 EKU(확장 키 사용)가 포함된 TLS 인증서의 서명이 중단되고 있습니다. 새로 발급된 인증서에는 서버 인증 EKU만 포함됩니다.

주요 정책 요구 사항

- 공용 루트 CA는 서버 인증(id-kp-serverAuth)에 대해서만 EKU(Extended Key Usage)를 어설션해야 합니다.

- 인증서에는 서버 인증 EKU만 포함되어야 합니다.

- 이러한 인증서에 클라이언트 인증 EKU를 포함하는 것은 금지됩니다

- 클라이언트 인증 EKU를 사용하여 인증서를 계속 발급하는 루트 CA는 결국 Chrome 루트 저장소에서 제거되어 Chrome 브라우저에서 "신뢰할 수 없음"과 같은 인증서의 플래그를 지정합니다

일정

- 2025년 9월, SSL.com은 서버 인증서에 대해 ServerAuth EKU만 포함하는(ClientAuth는 포함하지 않는) TLS 인증

서를 발급합니다. 즉, 웹 사이트 또는 서버에 대한 새 SSL/TLS 인증서는 명시적으로 "서버 인증"에만 사용됩니다.

- 2025년 10월: 프로그램에 맞게 조정된 CA(예: DigiCert, Sectigo 등)가 기본적으로 서버 전용 인증서를 발급하기 시작했습니다.
- 2026년 5월: 프로그램에 맞춰진 CA가 클라이언트 인증 EKU 인증서 발급을 중지합니다.
- 2027년 3월: Chrome Root Program Policy가 완전히 유효해짐

Cisco Secure Firewall 제품에 미치는 영향

공용 CA가 발급된 인증서에 서버 인증 EKU만 포함하기 시작하면 이는 다음 Cisco Secure Firewall 제품 시나리오에 다음과 같은 영향을 미칠 수 있습니다.

- ASA, FTD, FDM 또는 FMC가 클라이언트 역할을 하는 경우(예: ISE(pxGrid), RADIUS, LDAPS 또는 Active Directory와 같은 인증 서버나 ID 공급자에 연결하는 경우), 클라이언트 인증서가 공용 CA에 의해 생성되었지만 클라이언트 인증 EKU가 없는 경우 인증서 기반 인증이 실패할 수 있습니다. 이러한 시나리오에서 인증 서버가 필수 EKU 없이 인증서를 거부하는 경우 연결 실패가 발생할 수 있습니다.
- Cisco Secure Client(이전의 AnyConnect)는 인증서를 사용하여 ASA 또는 FTD 서버에 인증할 수 있습니다. 그러나 클라이언트 인증서가 공용 CA에 의해 생성되었고 클라이언트 인증 EKU가 없는 경우 RAVPN(Remote Access VPN) 연결이 실패합니다.
- 인증서 인증(RSA 또는 ECDSA)을 사용하여 FTD 또는 ASA가 다른 FTD, ASA, Cisco 라우터 또는 서드파티 VPN 피어에 관계 없이 사이트 대 사이트 VPN 터널을 설정하는 경우, 공용 CA에서 생성된 ID 인증서에 클라이언트 인증 EKU 특성이 없으면 터널이 실패합니다. 이는 원격 VPN 피어에서 ID 인증서에 클라이언트 인증 EKU가 있어야 하기 때문에 발생합니다.

참고: pxGrid를 통해 ISE와 FMC 또는 FDM을 통합하는 경우 FMC/FDM에 설치된 인증서에 클라이언트 인증 EKU 특성이 없으면 이 문서에서 제안하는 해결 방법 및 다음 ISE 참조를 검토하십시오. FN74392 및 Prepare Identity Services Engine for Extended Key Usage Restrictions in Issued Public Certification Authorities.

참고: TLS 서버 인증서에서 clientAuth EKU를 제거하는 것은 보안을 강화하고 오용을 방지하는 업계 전반의 정책 변경입니다. 대부분의 사용자들에게 눈에 띄는 영향은 없을 것이다. 그러나 ClientAuth EKU에 의존하는 경우 사전 대응적 단계를 수행하여 요구 사항에 맞는 올바른 유형의 인증서를 얻어야 합니다.

영향을 받는 제품

Cisco Secure Firewall 제품	소프트웨어 버전	영향 받는 시나리오	교정
FTD	모든 버전	클라이언트 역할을 하는 경우(예: ISE(pxGrid), RADIUS, LDAPS 또는 Active Directory와 같은 인증 서버나 ID 공급자에 연결할 때), 클라이언트 인증서가 공용 CA에 의해 생성되었지만 클라이언트 인증 EKU가 없는 경우 인증서 기반 인증이 실패할 수 있습니다. 이 시나리오에서 인증 서버가 필수 EKU 없이 인증서를 거부하는 경우 연결 실패가 발생할 수 있습니다.	옵션 1. 클라이언트 인증에 TLS 서버 인증서를 사용하는 경우 다른 소스에서 ClientAuth EKU를 사용하는 인증서를 얻어야 합니다. 또는 옵션2. 통합된 EKU(ClientAuth 및 ServerAuth) 인증서를 제공하는 공용 루트 CA(Certificate Authorities)로 전환합니다. 참고: 추가 옵션은 이 문서의 해결 방법 섹션을 참조하십시오.
FDM	모든 버전		
FMC	모든 버전		
ASA	모든 버전		
Cisco Secure Client(이전의 AnyConnect)	모든 버전	Cisco Secure Client는 인증서를 사용하여 ASA 또는 FTD 서버에 인증할 수 있습니다. 그러나 클라이언트 인증서가 공용 CA에 의해 생성되었고 클라이언트 인증 EKU가 없는 경우 RAVPN(Remote Access VPN) 연결이 실패합니다.	
FTD 또는 ASA	모든 버전	인증서 인증(RSA	

		또는 ECDSA)을 사용하여 FTD 또는 ASA가 다른 FTD, ASA, Cisco 라우터 또는 서드파티 VPN 피어에 관계 없이 사이트 대 사이트 VPN 터널을 설정하면 공용 CA에서 생성된 ID 인증서에 클라이언트 인증 EKU 특성이 없으면 VPN 터널이 실패합니다. 이는 원격 VPN 피어에서 ID 인증서에 클라이언트 인증 EKU가 있어야 하기 때문에 발생합니다.	

참고: pxGrid를 통해 ISE와 FMC 또는 FDM을 통합하는 경우 FMC/FDM에 설치된 인증서에 클라이언트 인증 EKU 특성이 없으면 이 문서에서 제안하는 해결 방법 및 다음 ISE 참조를 검토하십시오. FN74392 및 Prepare Identity Services Engine for Extended Key Usage Restrictions in Issued Public Certification Authorities.

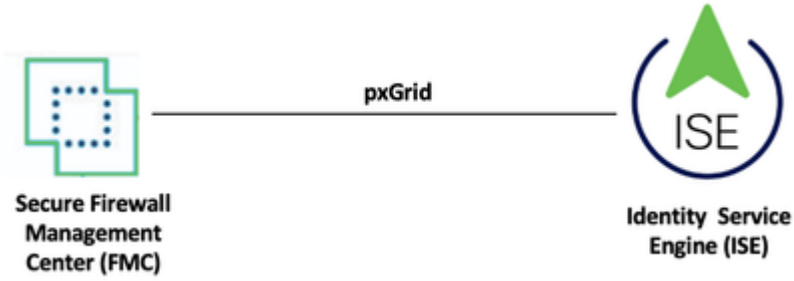
참고: TLS 서버 인증서에서 clientAuth EKU를 제거하는 것은 보안을 강화하고 오용을 방지하는 업계 전반의 정책 변경입니다. 대부분의 사용자들에게 눈에 띄는 영향은 없을 것이다. 그러나 ClientAuth EKU에 의존하는 경우 사전 대응적 단계를 수행하여 요구 사항에 맞는 올바른 유형의 인증서를 얻어야 합니다.

주의: 프로덕션 환경에서는 적절한 EKU 특성이 있는 인증서를 사용하는 것이 좋습니다. 이러한 방식을 통해 보안, 호환성, 업계 표준 및 모범 사례 준수를 보장합니다. EKU 속성이 없는 인증서는 임시적인 해결 방법으로만 간주해야 하며 관련 위험에 대한 명확한 이해가 있어야 합니다.

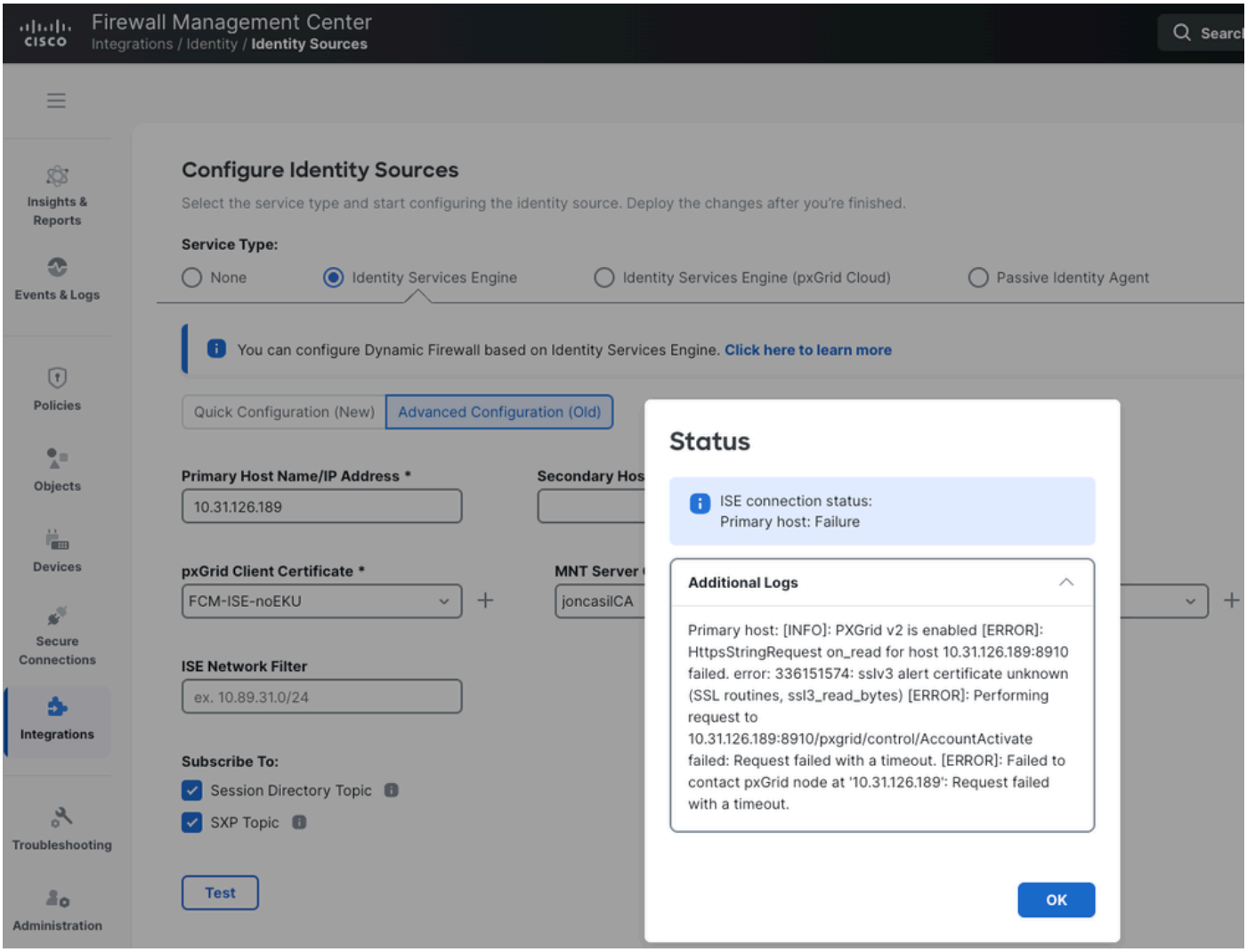
문제 1. FMC 인증서에 클라이언트 인증 EKU 특성이 없는 경우 FMC와 ISE 간의 pxGrid 통합 문제

이 시나리오에서 FMC에서 ISE와의 pxGrid 통합을 위해 사용하는 인증서에는 클라이언트 인증 EKU 특성이 없습니다. 따라서 ISE 서버는 FMC에서 제공한 인증서에 이 특성이 있을 것으로 예상하므로 pxGrid 통합이 실패합니다.

토폴로지



FMC UI 오류: FMC에서 사용하는 인증서에 ISE와의 pxGrid 통합에 대한 클라이언트 인증 EKU 특성이 없는 경우 FMC에 표시되는 오류 메시지입니다.



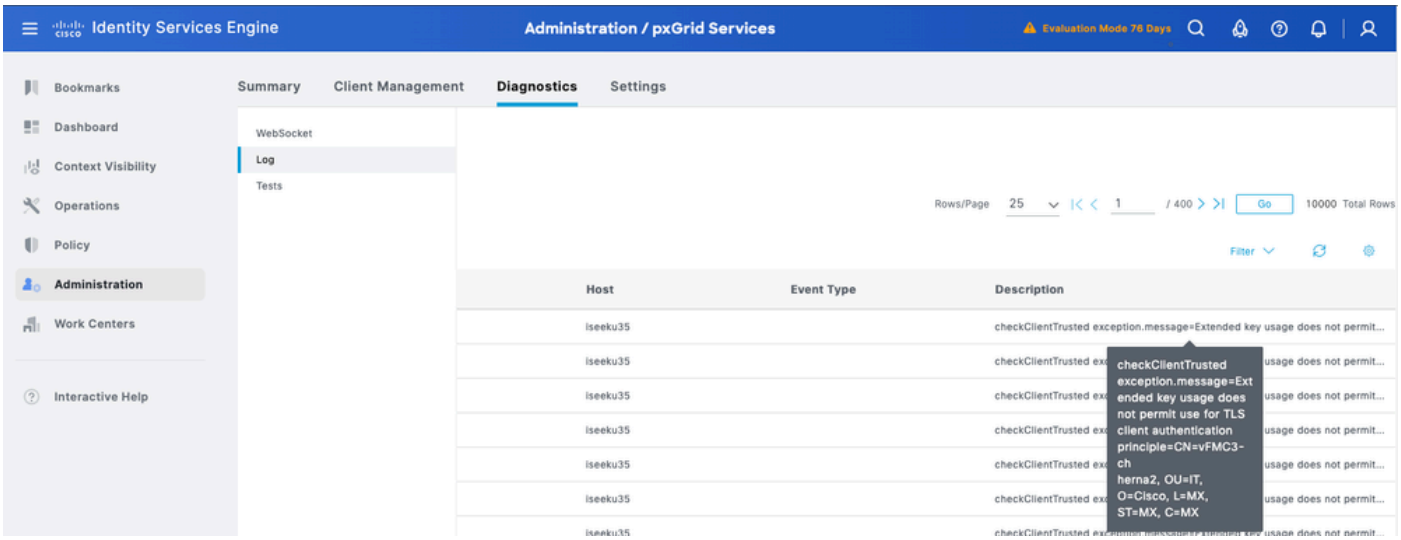
FMC CLI 오류: FMC /var/log/messages 디렉토리에도 동일한 오류 메시지가 있습니다.

<#root>

```
HttpsStringRequest on_read for host 10.31.126.189:8910 failed. error: 336151574:

sslv3 alert certificate unknown
```

```
(SSL routines, ssl3_read_bytes)

Mar 27 23:17:17 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:HttpsEndpoint

[ERROR] Performing request to 10.31.126.189:8910/pxgrid/control/AccountActivate failed: Request failed w

Mar 27 23:17:17 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService

[ERROR] pxgrid2_service was not created for 10.31.126.189. Reason - Request failed with a timeout.

Mar 27 23:17:47 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService [I
Mar 27 23:17:47 vFMC3-chherna2 SF-IMS[8074]: [7514] ADI:ise_connector.PXGrid2ThreadedService [I
```

ISE 오류: ISE에 표시되는 오류 메시지입니다. "checkClientTrusted exception.message=Extended key usage does not permit use for TLS client authentication principle=CN=vFMC3-chherna2, OU=IT, O=Cisco, L=MX, ST=MX, C=MX".



해결 방법: pxGrid를 통해 ISE와 FMC 또는 FDM을 통합하려는 경우 FMC/FDM에 설치된 인증서에 클라이언트 인증 EKU 특성이 없으면 이 문서에서 제안하는 내용과 다음 ISE 참조 FN74392를 검토하고 pxGrid 통합의 성공을 위해 Public Certification Authorities Issued에서 Prepare Identity Services Engine for Extended Key Usage Restrictions를 준비하십시오.

참고: FMC pxGrid 클라이언트 인증서는 ClientAuth EKU 특성을 포함하거나 클라이언트 또는 서버 EKU 특성을 전혀 포함하지 않아야 합니다.

참고: IMS에서는 공용 CA 서명 인증서 사용이 지원되지만 이 통신은 내부 트랜잭션용이므로 ISE 내부 CA 인증서

를 사용하는 것이 좋습니다.

문제 2. 제공된 인증서에 클라이언트 인증 EKU 특성이 없는 경우 LDAPS 서버와의 FTD 또는 ASA 통합 문제

이 시나리오에서 FTD 또는 ASA는 인증서 인증을 사용하여 LDAPS 서버와 통합하는 클라이언트 역할을 합니다. FTD 또는 ASA에서 사용하는 인증서에 클라이언트 인증 EKU 특성이 없으면 LDAPS 서버에서 이 특성이 인증서에 있어야 하므로 통합이 실패합니다.

토폴로지

LDAP 서버 오류: 'TLS 인증서 확인: 오류, 지원되지 않는 인증서 용도 ' 및 'TLS 추적: SSL3 경고 쓰기:치명적:지원되지 않는 인증서'

```
69ceb4f5.157b4993 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 write server cer
tificate verify
69ceb4f5.157c01a4 0x7ff553fff700 TLS trace: SSL_accept:SSLv3/TLS write finished
69ceb4f5.157c458a 0x7ff553fff700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.157c6685 0x7ff553fff700 TLS trace: SSL_accept:error in TLSv1.3 early d
ata
69ceb4f5.15b17eaa 0x7ff5522fc700 connection_get(15): got connid=1004
69ceb4f5.15b1b73f 0x7ff5522fc700 connection_read(15): checking for input on id=
1004
69ceb4f5.15b2bf05 0x7ff5522fc700 TLS trace: SSL_accept:TLSv1.3 early data
69ceb4f5.15b4c6c3 0x7ff5522fc700 TLS certificate verification: depth: 0, err: 2
6, subject: /CN=asa-server-only,69ceb4f5.15b4e8de 0x7ff5522fc700  issuer: /CN=T
est-CA
69ceb4f5.15b4f367 0x7ff5522fc700 TLS certificate verification: Error, unsupport
ed certificate purpose
69ceb4f5.15b57df8 0x7ff5522fc700 TLS trace: SSL3 alert write:fatal:unsupported
certificate
69ceb4f5.15b5b557 0x7ff5522fc700 TLS trace: SSL_accept:error in error
69ceb4f5.15b66c36 0x7ff5522fc700 TLS: can't accept: error:1417C086:SSL routines
:tls_process_client_certificate:certificate verify failed (unsupported certific
ate purpose).
69ceb4f5.15b70391 0x7ff5522fc700 connection_read(15): TLS accept failure error=
-1 id=1004, closing
69ceb4f5.15b747ae 0x7ff5522fc700 connection_close: conn=1004 sd=15
```

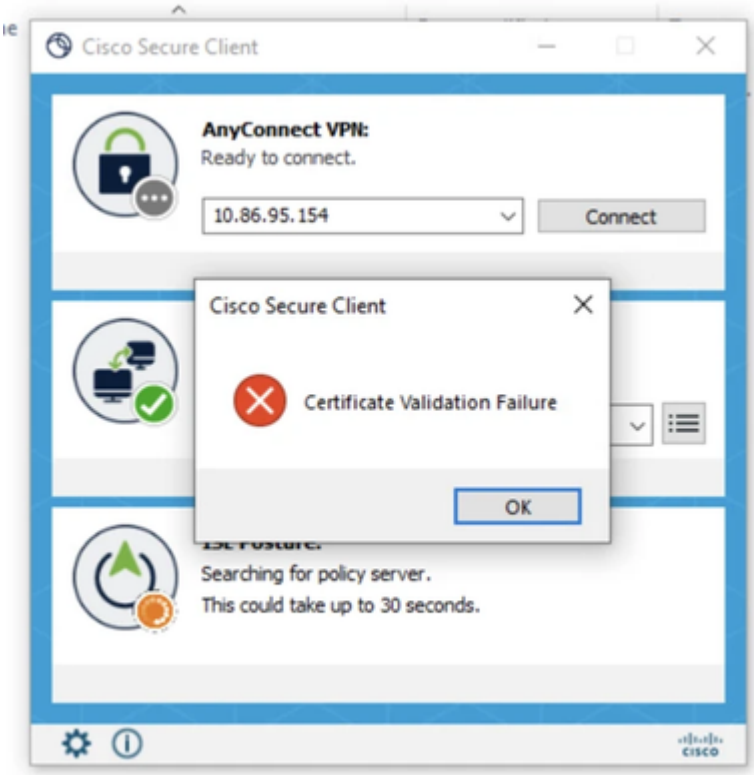
해결 방법: LDAPS 서버에서 인증서 기반 인증을 성공적으로 수행하려면 FTD 또는 ASA에서 올바른 ID 인증서(클라이언트 인증 EKU 특성 포함)를 사용하는지 확인하십시오.

문제 3. 클라이언트 인증서에 클라이언트 인증 EKU 특성이 없는 경우 Cisco Secure Client(이전의 AnyConnect)에서 FTD 또는 ASA에 연결 문제가 발생할 수 있습니다

이 시나리오에서 Cisco Secure Client는 인증서 인증을 사용하여 FTD 또는 ASA에 대한 RAVPN 터널을 설정합니다. 그러나 클라이언트 인증서에 클라이언트 인증 EKU 특성이 없는 경우 ASA 또는 FTD에서 이 특성이 클라이언트 인증서에 있어야 하므로 RAVPN 세션이 실패합니다.

토폴로지

Cisco Secure Client 오류: '인증서 검증 실패'



Cisco Secure Client DART 오류: DART 번들의 AnyConnectVPN.txt 파일의 다음 로그에서는 Cisco Secure Client가 RAVPN 인증서 기반 인증에 사용되는 인증서를 거부했는지 확인합니다. 클라이언트 인증 EKU 특성이 없습니다(DART 번들에서 AnyConnectVPN.txt 파일을 찾으려면 Cisco Secure Client > AnyConnect VPN > Logs > AnyConnectVPN.txt.로 이동합니다).

<#root>

```
****************************************

Date : 04/07/2026
Time : 03:35:22
Type : Error
Source : csc_vpnapi


Description : Function: CVerifyExtKeyUsage::compareEKUs


File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\CommonCrypt\Certificates\VerifyEx
Line: 330

EKU not found in certificate: 1.3.6.1.5.5.7.3.2



****************************************

Date : 04/07/2026
Time : 03:35:22
Type : Information
```

```
Source : csc_vpnapi


Description : Function: CCertStore::GetCertificates


File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\CommonCrypt\Certificates\CertStor
Line: 225

Ignoring client certificate because it does not contain the required EKU extension.

 Certificate details:
Store: [Omitted Output]

*****************************************
```

해결 방법: Cisco Secure Client가 FTD 또는 ASA를 사용한 인증서 기반 인증에 올바른 인증서(클라이언트 인증 EKU 특성 포함)를 사용하는지 확인하려면 이 문서의 제안서를 검토하십시오.

참고: 위의 DART 번들 오류에서 'EKU를 인증서에서 찾을 수 없음: 1.3.6.1.5.5.7.3.2', 이 번호 '1.3.6.1.5.5.7.3.2'는 클라이언트 인증 EKU OID에 해당합니다.

문제 4. ID 인증서에 클라이언트 인증 EKU 특성이 없는 경우 인증서 기반 인증을 사용하는 사이트 대 사이트 VPN 터널이 실패합니다

IKEv2 사이트 대 사이트 VPN 터널에 대한 인증서 기반 인증을 포함하는 이 시나리오에서는 FTD/ASA(1)에서 FTD/ASA 피어에 대한 터널을 설정하기 위해 사용하는 ID 인증서에 클라이언트 인증 EKU 특성이 없습니다. 따라서 원격 피어인 FTD/ASA (2)에 이 특성이 인증서에 있어야 하므로 VPN 터널을 설정할 수 없습니다.

토폴로지

FTD 또는 ASA CLI 오류: 클라이언트 인증 EKU 특성이 없는 FTD/ASA(1) ID 인증서를 거부하는 경우 IKEv2 인증서 기반 인증 중에 FTD/ASA(2)에서 관찰된 오류입니다.

<#root>

```
Apr 09 2026 15:59:50:

%ASA-3-717027: Certificate chain failed validation. Certi. Peer certificate key usage is invalid,

 subject name: CN=ASAv3.cisco.com,OU=IT,O=Cisco,C=US,unstructuredName=ASAv3.cisco.com.
Apr 09 2026 15:59:50:

%ASA-3-717027: Certificate chain failed validation. Certificate chain is either invalid or not authorize

Apr 09 2026 15:59:50: %ASA-3-751006: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:10.3.3.5

IKEv2 Certificate authentication failed.  Error: Certificate authentication failed

Apr 09 2026 15:59:50: %ASA-4-750003: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:10.3.3.5

IKEv2 Negotiation aborted due to ERROR: Auth exchange failed

Apr 09 2026 15:59:50: %ASA-4-752012: IKEv2 was unsuccessful at setting up a tunnel.  Map Tag = CMAP.  M
Apr 09 2026 15:59:50: %ASA-3-752015: Tunnel Manager has failed to establish an L2L SA.  All configured
Apr 09 2026 15:59:55: %ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.  Map Ta
Apr 09 2026 15:59:55: %ASA-5-750001: Local:10.3.3.6:500 Remote:10.3.3.5:500 Username:Unknown IKEv2 Rece
```

참고: 위의 예에서 FTD/ASA(2)는 ClientAuth 및 ServerAuth EKU 특성을 모두 포함하는 ID 인증서를 사용하고 있었습니다.

참고: 위의 예에서 FTD/ASA(2)는 라우터 또는 서드파티 물리적 또는 클라우드 기반 VPN Concentrator로 대체될 수도 있습니다. 그러면 VPN 피어에서 성공적인 인증서 기반 인증을 위해 FTD/ASA에서 사용하는 인증서에 클라이언트 인증 EKU 특성이 있어야 하므로 동일한 문제가 유지됩니다(1).

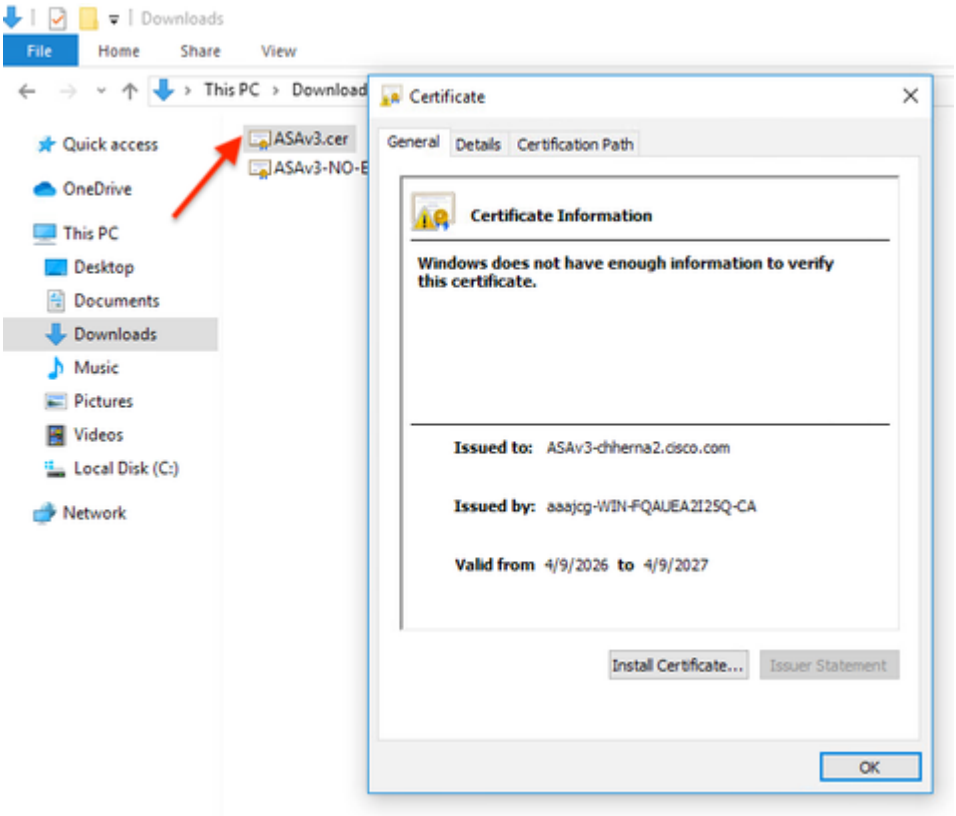
해결 방법: 이 문서에서 제안된 내용을 검토하여 FTD/ASA(1)가 올바른 ID 인증서(클라이언트 인증 EKU 특성 포함)를 사용하여 인증서 기반 인증을 사용하는 성공적인 사이트 대 사이트 VPN 터널을 지원하는지 확인합니다.

인증서에 클라이언트 인증 EKU 특성이 없는지 확인하는 지침

Windows 인증서 관리자를 사용하여 .cer 인증서의 EKU 특성 확인

다음 단계에 따라 Windows 인증서 관리자를 사용하여 .cer 인증서의 EKU 특성을 확인합니다.

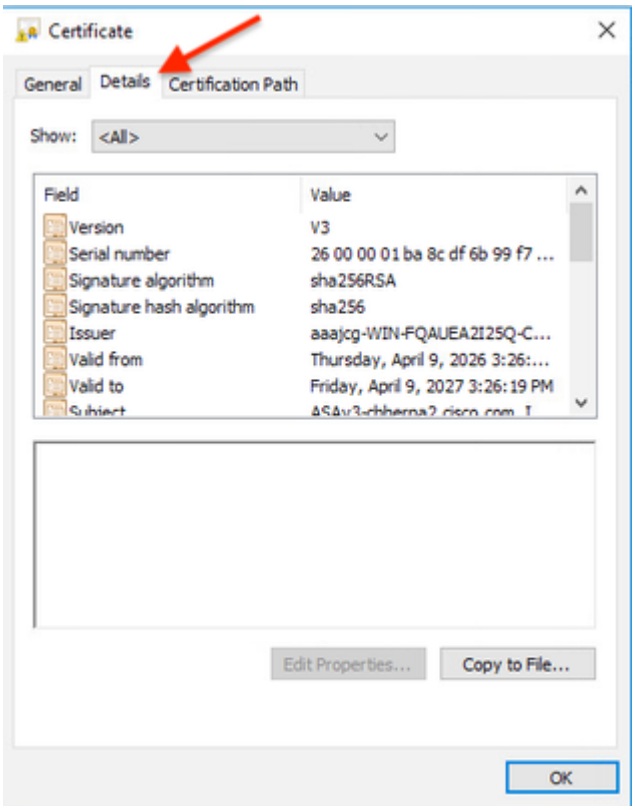
1단계. .cer 파일을 두 번 클릭하여 Windows Certificate Manager에서 엽니다.



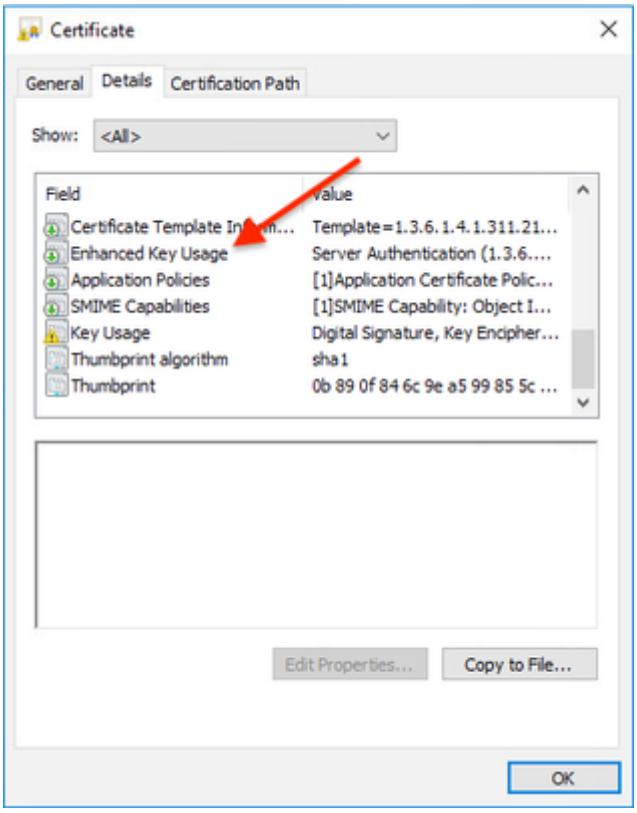
참고: .cer 파일만 이 방법으로 직접 열립니다. 인증서의 확장명이 .pem인 경우 먼저 이름을 .cer 또는 .crt로 변경합니다.

2단계. Handle Security Warning (if any)(보안 경고 처리(있는 경우)), 보안 경고 프롬프트가 나타나면 Open(열기)을 클릭하여 계속합니다.

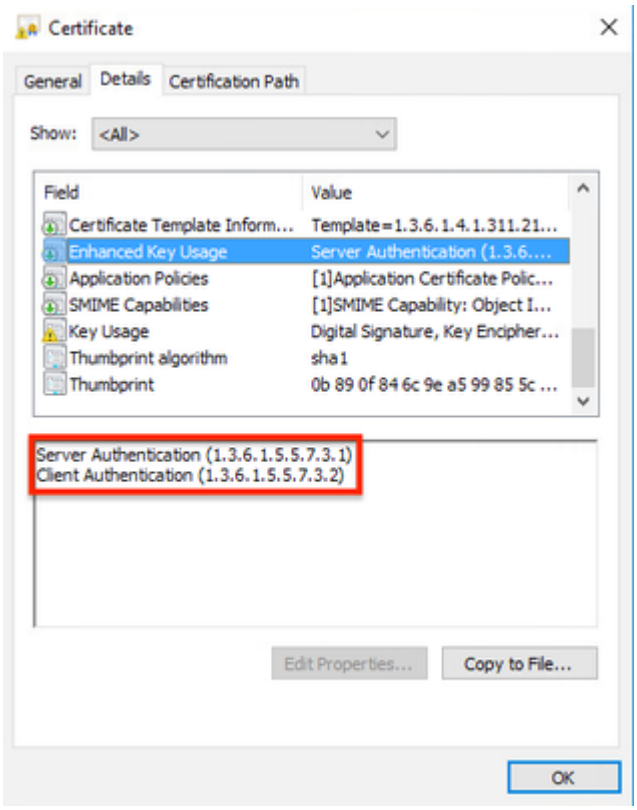
3단계. 인증서 창에서 Details(세부사항) 탭을 클릭합니다.



4단계. 필드 목록을 스크롤하여 "Enhanced Key Usage"(또는 Extended Key Usage)를 선택합니다.

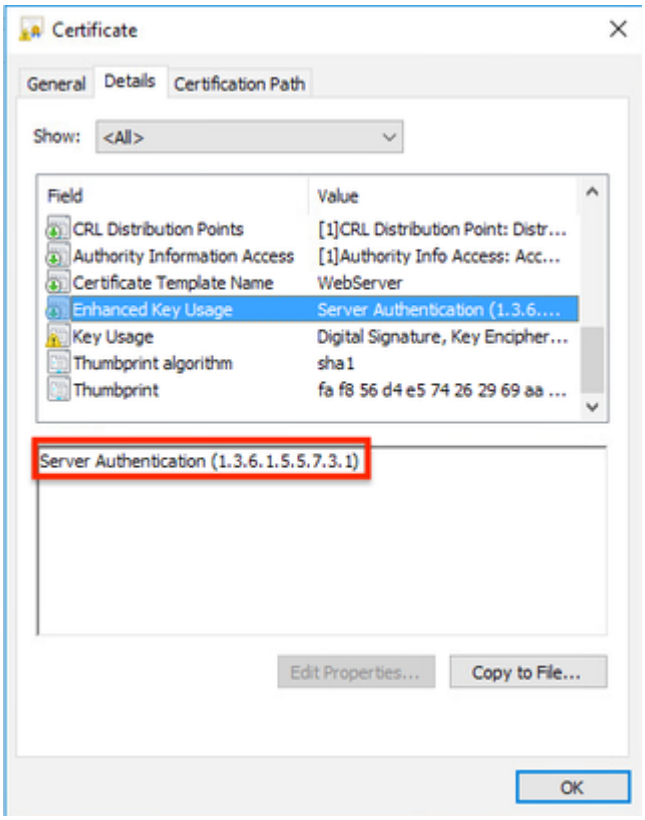


5단계. EKU 특성을 확인합니다. 인증서에 있는 EKU 값을 나타내는 "Server Authentication(서버 인증)" 및 "Client Authentication(클라이언트 인증)"과 같은 항목이 표시될 수 있습니다.

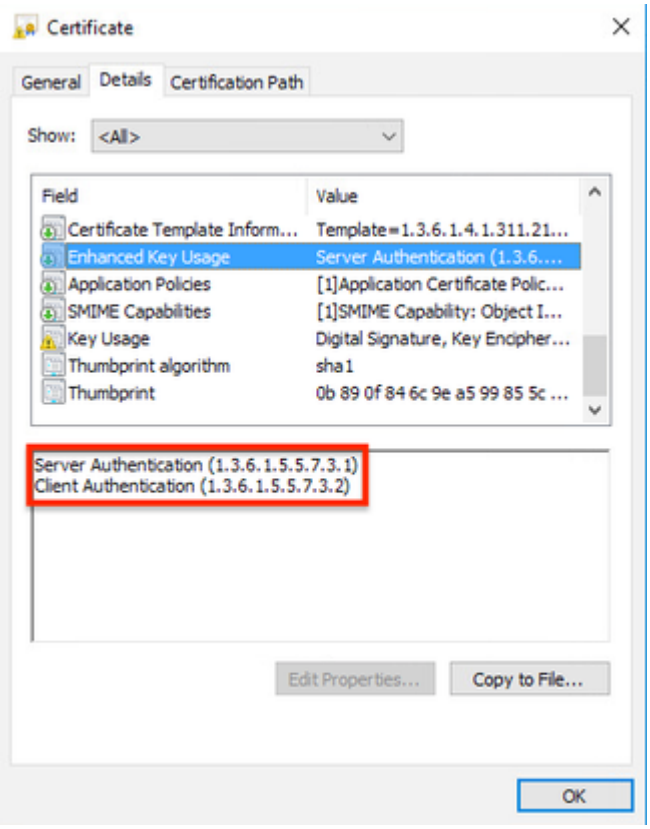


6단계. 확인 후 OK(확인)를 클릭하여 인증서 창을 닫습니다.

예 1: 이 .cer 인증서에는 클라이언트 인증 EKU 특성이 없고 서버 인증 EKU 특성만 포함되어 있습니다.



예 2: 이 .cer 인증서에는 서버 및 클라이언트 인증 EKU 특성이 모두 포함됩니다.



OpenSSL을 사용하여 PKCS#12, PEM 및 .cer 인증서에서 EKU 특성 확인

다음 단계에 따라 .p12(PKCS#12), .pem(PEM) 및 .cer 인증서에서 EKU 특성을 확인합니다.

1단계. 확인해야 할 인증서를 찾아 .p12(PKCS#12), .pem(PEM) 또는 .cer 형식으로 내보냅니다.

.p12(PKCS#12) 인증서의 경우 openssl을 사용하여 .p12(PKCS#12) 파일에서 인증서를 추출하면 .p12(PKCS#12) 파일에 개인 키, 인증서 및 CA 인증서가 포함될 수 있습니다.

다음 명령을 사용하여 .p12(PKCS#12) 파일의 인증서를 .pem(PEM) 파일로 추출합니다(개인 키 또는 CA 체인 없음).

```
openssl pkcs12 -in yourfile.p12 -nokeys -clcerts -out cert.pem
```

- yourfile.p12: 실제 파일 이름으로 대체합니다.
- .p12 파일의 암호를 입력해야 할 수 있습니다.
- cert.pem: 개인 키 또는 CA 체인 없이 .pem(PEM) 형식으로 인증서를 추출합니까?

2단계. 다음 openssl 명령을 사용하여 인증서 세부사항 및 EKU 특성을 표시합니다.

a) .pem 파일의 경우 다음 openssl 명령을 사용하여 인증서 세부사항 및 EKU 특성을 표시합니다.

```
openssl x509 -in cert.pem -text -noout
```

- cert.pem: 실제 파일 이름으로 대체합니다.

b) .cer 파일의 경우 다음 openssl 명령을 사용하여 인증서 세부사항 및 EKU 특성을 표시합니다.

```
openssl x509 -in yourfile.cer -text -noout
```

- yourfile.cer: 실제 파일 이름으로 대체합니다.

3단계. 그런 다음 출력에서 X509v3 Extended Key Usage(X509v3 확장 키 사용) 섹션을 찾습니다. 인증서에 있는 EKU 값을 나타내는 "TLS Web Server Authentication(TLS 웹 서버 인증)" 및 "TLS Web Client Authentication(TLS 웹 클라이언트 인증)"과 같은 항목이 표시될 수 있습니다.

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
```

또는 EKU 특성 OID(Object Identifiers):

```
X509v3 Extended Key Usage:
1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2
```

- 서버 인증 EKU OID: 1.3.6.1.5.5.7.3.1
- 클라이언트 인증 EKU OID: 1.3.6.1.5.5.7.3.2

예 1: 이 .pem(PEM) 인증서에는 클라이언트 인증 EKU 특성이 없으며 서버 인증 EKU 특성만 포함됩니다.

<#root>

```
MyHost$ openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            26:00:00:01:b7:e7:90:48:d6:f9:41:d3:54:00:01:00:00:01:b7
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=aaajcg, CN=aaajcg-WIN-FQAUEA2I25Q-CA
        Validity
            Not Before: Mar 27 00:31:40 2026 GMT
            Not After : Mar 26 00:31:40 2028 GMT
        Subject: C=MX, ST=MX, L=MX, O=Cisco, OU=IT, CN=vFMC3-chherna2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:cf:a8:a0:ff:dd:34:73:7d:46:86:85:05:b6:0c:
                    5e:32:8c:6f:6f:88:52:03:58:63:c6:89:d8:fc:55:
                    c5:58:ba:eb:45:88:b2:21:9e:c5:d8:67:57:39:0f:
                    91:a5:41:61:fa:94:b1:ad:9e:71:26:87:b6:30:ae:
                    a7:f6:89:b1:6d:61:ce:fa:47:7f:2a:d8:e8:4d:26:
                    4f:a7:d3:eb:5a:69:16:46:71:c7:55:cf:87:b4:10:
                    96:f2:10:6b:c0:a7:3d:3c:49:9d:ee:77:8c:b5:95:
                    9b:69:81:e0:2d:a0:6e:5c:78:73:22:5a:38:d0:74:
                    38:b2:ba:e0:ab:c5:44:eb:e1:3c:52:86:b8:2a:4e:
                    37:44:9c:34:d8:d8:6c:ae:3e:df:12:57:0e:28:52:
                    57:dc:6d:62:ea:b6:ec:19:4e:90:8f:3f:2c:23:1b:
                    e2:39:f0:ba:07:08:9a:0b:97:96:05:2e:69:fe:9a:
                    b2:b2:74:9a:ba:06:25:bc:38:1c:94:87:8e:2a:dc:
                    2f:0b:a6:31:6c:bf:11:96:2a:71:b3:87:e5:f5:cb:
                    88:f1:73:cf:88:d7:30:78:24:77:7c:b7:2c:7c:83:
                    6d:69:5b:bd:d4:21:b9:ee:19:c4:02:be:7b:44:a2:
                    55:d6:b2:95:11:46:bf:db:3e:4f:9a:8c:d4:ad:8d:
                    82:f5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                0D:8E:DA:07:6D:49:EA:51:D2:C7:EF:50:CE:CE:2B:8E:7C:DF:A6:8D
            X509v3 Authority Key Identifier:
                keyid:3A:45:60:22:F7:C8:2C:0D:D2:98:5A:BC:E0:98:D4:91:1D:67:32:22

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=WIN-FQAUEA2I25Q,CN=CDP,CN=Public%20Key%20

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=AIA,CN=Public%20Key%20Services

            1.3.6.1.4.1.311.20.2:
                ...W.e.b.S.e.r.v.e.r
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment


X509v3 Extended Key Usage:

        <-------- "EKU SECTION"
```

TLS Web Server Authentication

```
  <-------- "Server Authentication EKU Attribute Included"
    Signature Algorithm: sha256WithRSAEncryption
         2f:27:cd:95:7d:5c:40:fa:29:64:df:75:7d:7a:87:9b:b0:94:
         0e:6b:07:4d:d2:7e:83:da:03:08:f3:50:0d:5b:05:8c:1f:54:
         46:fe:53:f3:e2:d4:0a:ba:37:4f:cd:a4:49:04:74:79:09:23:
         d6:06:af:69:d2:7b:f5:bc:ec:fe:ce:e4:c9:07:31:d7:85:45:
         55:78:d3:42:45:f9:ce:cd:bf:43:53:b4:8e:4c:af:64:4b:a6:
         dc:47:d0:16:4e:73:62:fd:c8:5e:37:74:cb:68:48:29:7d:f9:
         41:b3:d1:46:56:24:83:23:5c:bd:b0:e3:7c:f9:8a:af:da:09:
         d0:c2:7d:4a:e6:24:0f:e6:fc:6e:0d:65:8c:96:8c:af:21:b2:
         7f:4b:bb:1c:17:33:b1:db:00:f3:12:e3:53:39:d0:e7:6a:48:
         4c:c6:4f:29:6f:74:ff:2d:a7:e5:ea:e8:89:fe:a4:2b:cd:e3:
         61:6a:9e:11:52:15:57:f2:b8:e8:fa:78:31:20:49:d9:50:f9:
         70:3f:1e:aa:9c:1a:bb:0b:59:66:1e:85:bd:76:e7:73:6f:ec:
         86:30:b0:dd:86:3c:b3:a0:7b:fb:b7:74:5d:38:88:82:3d:a3:
         2d:8c:a5:e4:db:37:eb:be:7f:62:bc:87:7c:35:17:32:fc:52:
         c5:d3:c5:8f
```

예 2: 이 .pem(PEM) 인증서에는 클라이언트 및 서버 인증 EKU 특성이 모두 포함됩니다.

<#root>

```
MyHost$ openssl x509 -in cert.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            26:00:00:01:b6:74:fc:b4:1e:99:be:7a:10:00:01:00:00:01:b6
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=aaajcg, CN=aaajcg-WIN-FQAUEA2I25Q-CA
        Validity
            Not Before: Mar 26 23:44:58 2026 GMT
            Not After : Mar 26 23:44:58 2027 GMT
        Subject: C=MX, ST=AD, L=AD, O=Cisco, OU=IT, CN=vFMC3-chherna2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ab:aa:67:4e:55:19:3b:38:6c:33:2e:ba:fd:19:
                    56:e7:68:f8:f7:e9:53:95:1f:53:b4:f1:ce:94:c8:
                    ca:41:f1:52:15:eb:a5:35:9f:07:95:9f:c3:8a:5e:
                    62:d6:e1:5c:04:c5:c0:27:1c:84:ed:3d:1b:42:50:
                    91:4a:a6:86:90:e0:6e:26:7e:37:fd:17:0c:2f:bb:
                    fe:58:81:ec:3b:9d:0b:fc:dd:8c:6b:dd:ab:d3:96:
                    74:23:0d:78:d7:09:53:61:f9:b0:29:c6:7c:e2:9c:
                    2f:74:30:42:0f:45:47:cd:16:59:ed:53:62:8f:60:
                    75:f8:24:f5:1f:77:fb:89:85:4b:49:ad:93:43:04:
                    6e:4a:b3:59:fc:eb:75:70:39:67:71:60:be:b3:b7:
                    86:f7:c5:53:28:1e:bf:8f:b2:52:ec:79:d6:12:b0:
                    33:9c:6d:46:7a:9c:5d:53:a5:44:24:da:4b:36:7d:
                    c2:ec:61:d7:a0:01:c3:d2:bc:0a:df:a8:f6:0c:82:
                    48:30:fb:c6:3e:4a:48:a9:01:13:f5:4e:f2:03:24:
                    38:ee:aa:d9:60:78:30:45:ed:3b:76:16:fd:7a:d3:
```

```
                    b0:16:10:28:75:fc:41:32:e6:6d:cb:c3:96:58:77:
                    9e:11:0a:9b:33:c7:92:8d:75:1f:e5:30:29:a4:a5:
                    ba:7d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D2:DF:62:25:17:DB:72:31:D8:D2:D0:41:CB:FB:DD:00:FF:38:BD:BB
            X509v3 Authority Key Identifier:
                keyid:3A:45:60:22:F7:C8:2C:0D:D2:98:5A:BC:E0:98:D4:91:1D:67:32:22

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=WIN-FQAUEA2I25Q,CN=CDP,CN=Public%20Key%20

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=aaajcg-WIN-FQAUEA2I25Q-CA,CN=AIA,CN=Public%20Key%20Services

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            1.3.6.1.4.1.311.21.7:
                0-.%+.....7.....^..9...
...b.../ ...R...Z..d...


X509v3 Extended Key Usage:

          <-------- "EKU SECTION"


TLS Web Server Authentication, TLS Web Client Authentication


  <----- "Server & Client EKU Attributes Included"
            1.3.6.1.4.1.311.21.10:
                0.0
..+.......0
..+.......
            S/MIME Capabilities:
......0...+....0050...*.H..
..*.H..
    Signature Algorithm: sha256WithRSAEncryption
         3f:66:b1:35:7e:05:b4:69:f1:81:95:b8:18:90:f2:20:bd:8d:
         ff:03:5a:59:ca:02:ba:2d:1d:e0:8d:3f:63:e9:fe:71:3c:9a:
         11:15:5c:3b:fc:62:e4:cf:15:25:4c:74:5e:ad:3f:09:e9:3b:
         d5:08:95:7d:97:7a:ef:c1:16:6d:e0:7a:0b:21:81:46:bc:15:
         c3:76:8c:fe:fb:14:94:36:92:0d:3b:4a:c9:8f:6a:bd:dc:4b:
         0b:24:c3:32:35:27:e7:aa:23:95:85:e4:a9:64:71:f0:98:9e:
         33:aa:6e:bd:7c:dd:dc:4b:cf:dd:0e:a7:ea:e8:aa:61:8f:67:
         84:da:5b:be:8e:05:75:c8:eb:46:13:6f:14:4d:fe:4e:57:3c:
         29:27:cc:0b:5b:25:87:37:24:12:79:b1:c3:78:c8:94:fe:df:
         3c:77:aa:fc:f2:ee:ae:9b:ab:88:29:f9:ee:04:c2:48:5f:21:
         9e:1c:25:cc:c9:c5:9c:23:8f:af:87:76:5e:46:74:ac:73:57:
         01:ba:71:ae:46:e1:87:3c:94:6c:19:f7:fe:8e:66:9d:c7:1f:
         b0:87:4b:65:e2:fc:d6:10:7c:44:57:56:5d:68:bb:df:f0:36:
         0e:07:c5:8a:be:56:86:97:3d:a7:1c:8b:86:df:0b:51:b5:97:
         cc:67:09:8e
```

해결 방법

관리자는 다음 해결 옵션 중 하나를 선택할 수 있습니다.

옵션 1. 통합된 EKU 인증서를 제공하는 공용 루트 CA로 전환

DigiCert 및 IdenTrust와 같은 일부 공용 루트 CA는 대체 루트에서 통합된 EKU 유형(서버 및 클라이언트 인증서)을 가진 인증서를 발급하며, 이는 Chrome 루트 저장소에 포함될 수 없습니다. CA 공급자와 협력하여 이러한 인증서의 가용성을 확인하고, 인증서를 배포하기 전에 인증서를 제공하는 서버와 인증서를 사용하는 클라이언트가 모두 해당 루트 CA를 신뢰하는지 확인합니다.

이 접근 방식을 사용하면 Chrome 루트 프로그램 정책에 의해 시행되는 클라이언트 인증 EKU의 일몰을 완화하기 위해 서버 소프트웨어를 업그레이드할 필요가 없습니다.

공용 루트 CA 및 EKU 유형의 예를 보여 주는 다음 표는 완전한 목록이 아니며 예시 목적으로만 사용됩니다.

CA 벤더	EKU 유형	루트 CA	발급/하위 CA
아이덴트러스트	클라이언트 인증 + 서버 인증	IdenTrust 공공 부문 루트 CA 1	IdenTrust 공공 부문 서버 CA 1
아이덴트러스트	클라이언트 인증	IdenTrust 공공 부문 루트 CA 1	TrustID RSA ClientAuth CA 2
아이덴트러스트	serverAuth(브라우저에서 신뢰함)	IdenTrust 상용 루트 CA 1	HydrantID 서버 CA O1
디지인증서	클라이언트 인증 + 서버 인증	DigiCert Assured ID Root G2	DigiCert Assured ID CA G2
디지인증서	클라이언트 인증	DigiCert Assured ID Root G2	DigiCert Assured ID Client CA G2
디지인증서	serverAuth(브라우저에서 신뢰함)	DigiCert 전역 루트 G2	DigiCert 전역 G2 TLS RSA SHA256

옵션 2. 현재 인증서를 갱신하여 유효 기간 연장

서버 및 클라이언트 인증 EKU가 모두 있는 공용 루트 CA에서 2026년 5월 이전에 발급한 인증서는 해당 기간이 만료될 때까지 계속 유효합니다. 그러나 정책 설정 전에 통합 EKU 인증서를 갱신하는 것이 좋습니다.

- 퍼블릭 CA 정책 및 구현 날짜는 벤더에 따라 다를 수 있습니다.
- CA에 확인하고 그에 따라 인증서 갱신을 계획합니다.

- 2026년 3월 15일 이후에는 공개 CA 발급 인증서가 200일 동안만 유효합니다.
- 일부 공용 CA가 통합된 EKU 인증서 발급을 중지했음을 고려하십시오.

옵션 3. 사설 PKI로 마이그레이션하여 결합된 EKU(서버 및 클라이언트) 인증서 발급

PKI(Private Public Key Infrastructure)로의 전환 가능성을 평가한 다음 사설 CA를 설정하여 통합된 EKU(필요한 EKU가 있는 서버 및 클라이언트 인증서)로 단일 인증서를 발급합니다.

인증서를 발급하거나 배포하기 전에 인증서를 제공하는 서버와 인증서를 사용하는 모든 클라이언트가 해당 루트 CA를 신뢰하는지 확인하십시오.

옵션 4. 클라이언트 인증 EKU만 있는 공개적으로 신뢰할 수 있는 인증서 가져오기

SSL.com과 같은 일부 CA는 전용 클라이언트 인증 인증서를 제공합니다. 이러한 인증서는 TLS 인증서와 별개이며 일반적으로 엔터프라이즈 인증에 사용됩니다.

⚠ 주의: 프로덕션 환경에서는 적절한 EKU 특성이 있는 인증서를 사용하는 것이 좋습니다. 이러한 방식을 통해 보안, 호환성, 업계 표준 및 모범 사례 준수를 보장합니다. EKU 속성이 없는 인증서는 임시적인 해결 방법으로만 간주해야 하며 관련 위험에 대한 명확한 이해가 있어야 합니다.

FAQ(자주 묻는 질문)

Q1. 개인 PKI를 사용할 경우 이에 대해 우려해야 합니까?

A: 프라이빗 CA에 의해 시행되는 정책은 각 조직에 의해 결정됩니다. 프라이빗 CA가 인증서에서 클라이언트 인증 EKU 특성 제거와 같은 동일한 발급 기준을 채택하는 경우 이 문서에서 설명하는 지침을 적용할 수 있습니다.

Q2. 기존 인증서를 계속 사용할 수 있습니까?

A : 예. 결합된 EKU가 있는 유효한 인증서를 만료 시간까지 사용할 수 있습니다.

Q3. FMC/FDM에 설치된 인증서에 클라이언트 인증 EKU 특성이 없는 경우 pxGrid를 통해 ISE와 FMC 또는 FDM을 통합하는 데 사용할 수 있는 옵션은 무엇입니까?

A : 이 문서에서 제안한 해결 방법 외에 다음 ISE 참조를 확인하는 것이 좋습니다.

- 필드 알림: FN74392 - Cisco Identity Services Engine: 2026년 5월부터 시작되는 공용 CA 클라이언트 인증 EKU 변경으로 인한 보안 통신에 미치는 영향 - 해결 방법 제공

- 공용 인증 기관에서 발급한 인증서의 확장된 키 사용 제한에 대한 Identity Services Engine 준비

참고: IMS에서는 공용 CA 서명 인증서 사용이 지원되지만 이 통신은 내부 트랜잭션용이므로 ISE 내부 CA 인증서를 사용하는 것이 좋습니다.

Q4. "클라이언트 인증" EKU란 무엇이며, 내 인증서에 해당 EKU가 포함된 이유는 무엇입니까?

A: "클라이언트 인증" EKU는 클라이언트가 인증서를 사용하여 서버에 인증할 수 있음을 나타냅니다. 일부 CA는 기본적으로 TLS 인증서에 포함되었지만, 정상적인 웹 사이트 보안에는 필요하지 않았습니다.

Q5. 현재 TLS 인증서의 확장 키 사용 아래에 "클라이언트 인증"이 표시됩니다. 이제 무효가 된 건가요?

A: 아니요, 유효합니다. 즉시 교체할 필요는 없습니다. 갱신하면 새 인증서에 clientAuth EKU가 포함되지 않습니다.

Q6. 인증서에 clientAuth EKU가 있는지 확인하려면 어떻게 해야 합니까?

A : OpenSSL, PowerShell 또는 GUI 툴을 사용하여 인증서 세부사항을 검사하여 Extended Key Usage(확장 키 사용) 확장을 확인할 수 있습니다.

Q7. 클라이언트 인증 EKU만 있는 공개적으로 신뢰할 수 있는 인증서를 계속 받을 수 있습니까?

A : SSL.com과 같은 일부 CA는 전용 클라이언트 인증 인증서를 제공합니다. 이러한 인증서는 TLS 인증서와 별개이며 일반적으로 엔터프라이즈 인증에 사용됩니다.

Q8. 다른 EKU 또는 인증서 유형(코드 서명, 전자 메일 등)에 영향을 줍니까?

A : 아니요. 이 변경은 TLS 서버 인증서에만 적용됩니다. 코드 서명 및 이메일 인증서에는 고유한 EKU 요구 사항이 있습니다.

Q9. 이 변경에 대한 공식 요구 사항은 어디에서 확인할 수 있습니까?

A : Google Chrome 루트 프로그램 정책은 TLS 서버 인증서에서 clientAuth EKU를 금지하는 것에

대한 지침을 제공합니다.

Q10. 프로덕션 환경에서 클라이언트 및 서버 EKU 특성 없이 인증서를 사용해도 안전합니까?

A: 프로덕션 환경에서는 적절한 EKU 특성이 있는 인증서를 사용하는 것이 좋습니다. 이러한 방식을 통해 보안, 호환성, 업계 표준 및 모범 사례 준수를 보장합니다. EKU 속성이 없는 인증서는 임시적인 해결 방법으로만 간주해야 하며 관련 위험에 대한 명확한 이해가 있어야 합니다.

관련 정보

- 추가 지원이 필요한 경우 Cisco Technical Assistance Center(TAC)에 문의하십시오. 유효한 지원 계약이 필요합니다. Cisco Worldwide Support 연락처
- Cisco 지원 및 다운로드: Cisco 기술 지원 및 다운로드

관련 버그

- CSCwt94492 ENH: FMC는 pxGrid 통합에 사용된 클라이언트 인증서에 클라이언트 인증 EKU 특성이 있는지 검증해야 합니다.
- CSCwt94509 ENH: FMC는 pxGrid 통합에 사용되는 클라이언트 인증서에 클라이언트 인증 EKU 특성이 필요하다는 메시지를 표시해야 합니다
- CSCwt61767 2026년 5월 EKU 서버 전용 변경 - EKU가 부적절한 경우 ASA 컨피그레이션 경고 발행
- CSCws83036 EKU: ISE에서 ClientAuth EKU 시행의 영향 평가

Cisco ISE 참조

- 필드 알림: FN74392 - Cisco Identity Services Engine: 2026년 5월부터 시작되는 공용 CA 클라이언트 인증 EKU 변경으로 인한 보안 통신에 미치는 영향 - 해결 방법 제공
- 공용 인증 기관에서 발급한 인증서의 확장된 키 사용 제한에 대한 Identity Services Engine 준비

외부 참조

- Chrome 루트 프로그램 정책
- IdenTrust 포털
- SSL - TLS 서버 인증서에서 클라이언트 인증 EKU 제거 - 알아야 할 사항

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.