공용 CA 인증서에서 클라이언트 인증 EKU 일몰을 위한 Cisco ISE 준비

목차

소개

이 문서에서는 클라이언트 인증 EKU를 사용하여 공용 인증 기관에서 발급한 TLS 인증서의 향후 변경 사항으로 인해 ISE 서비스에 미치는 영향에 대해 설명합니다.

배경 정보

디지털 인증서는 신뢰할 수 있는 CA(Certificate Authority)에서 발급하는 전자 자격 증명으로, 인증, 데이터 무결성 및 기밀성을 보장하여 서버와 클라이언트 간의 통신을 보호합니다. 이러한 인증서에는 용도를 정의하는 EKU(Extended Key Usage) 필드가 포함되어 있습니다.

- 서버 인증 EKU(id-kp-serverAuth): 서버가 ID를 확인하기 위해 인증서를 표시할 때 사용됩니다.
- 클라이언트 인증 EKU(id-kp-clientAuth): 양 당사자가 서로 인증하는 mTLS(mutual TLS) 연결에 사용됩니다.

기존에는 단일 인증서에 서버 및 클라이언트 인증 EKU를 모두 포함할 수 있으므로 이중 용도로 사용할 수 있습니다. 이것은 특히 다른 연결 시나리오에서 서버 및 클라이언트 역할을 하는 Cisco ISE와 같은 제품에 중요합니다.

문제 정의

Chrome 루트 프로그램 정책 변경

2026년 5월부터 많은 공용 CA(Certificate Authority)가 클라이언트 인증 EKU(Extended Key Usage)가 포함된 TLS(Transport Layer Security) 인증서 발급을 중단합니다. 새로 발급된 인증서에는 일반적으로 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.
- 인증서는 서버 인증 EKU만 포함해야 합니다.
- 이러한 인증서에 클라이언트 인증 EKU를 포함하는 것은 금지됩니다
- 클라이언트 인증 EKU를 사용하여 계속해서 인증서를 발급하는 루트 CA는 결국 Chrome 루트 저장소에서 제거됩니다
- 공용 서버 TLS 인증서에 대해 더 이상 혼합 사용 루트 CA 없음
- 시행 일정: 2027년 3월.

공용 CA 응답 일정

- 2025년 10월: 많은 공용 CA(DigiCert, Sectigo, SSL)가 기본적으로 서버 전용 인증서를 발급하기 시작했습니다.
- 2026년 5월: 많은 공용 CA 서버가 클라이언트 인증 EKU 인증 발급을 중지합니다.
- 2027년 3월: Chrome Root Program Policy가 완전히 유효해짐

참고: 이 정책은 공용 CA에서 발급한 인증서에만 적용됩니다. 개인 PKI 및 자체 서명 인증서는 이 정책의 영향을 받지 않습니다.

Cisco ISE에 미치는 영향

영향을 받는 제품

모든 Cisco ISE 릴리스가 영향을 받습니다.

- ISE 3.1
- ISE 3.2
- ISE 3.3
- ISE 3.4
- ISE 3.5

참고: Cisco ISE 2.x 버전도 영향을 받습니다. 그러나 이 릴리스가 EOL(end of life)에 도달했으므로 수정이 계획되지 않았습니다.

Cisco ISE의 이중 역할

ISE는 다양한 연결 시나리오에서 서버 및 클라이언트 역할을 수행하며, 서버 및 클라이언트 인증 EKU를 모두 포함하는 인증서가 필요합니다.

서버로 Cisco ISE(서버 인증 EKU 필요):

- PxGrid
- ISE 메시징 서비스

클라이언트로 Cisco ISE(클라이언트 인증 EKU 필요):

- TC-NAC
- 보안 Syslog
- LDAPS
- Radius DTLS

영향을 받는 특정 활용 사례

아래 표에는 각 서비스에 대한 예상 영향과 함께 다가오는 클라이언트 인증 EKU 변경의 영향을 받을 수 있는 Cisco ISE 서비스가 요약되어 있습니다.

서비스	영향

pxGrid	pxGrid 인증서는 ISE 노드와 외부 pxGrid 통합 간의 통신에 사용됩니다. 외부 pxGrid 통합에는 서버 인증 EKU만 필요하지만, Cisco ISE는 UI 제한으로 인해 현재 가져온 pxGrid 인증서에 서버 인증 EKU 및 클라이언트 인증 EKU를 모두 포함해야 합니다. 따라서 공용 CA에서 발급한 pxGrid 인증서는 두 EKU에 모두 구축됩니다.
ISE 메시징 서비스(IMS)	IMS는 내부 ISE 서비스 간의 백엔드 통신에 사용됩니다. Cisco ISE는 현재 서버 인증 EKU와 클라이언트 인증 EKU를 모두 포함하는 IMS 인증서가 필요합니다. 서버 인증 EKU가 있는 공용 CA에서 갱신된 인증서는 내부 ISE 통신에 장애가 발생할 수 있는 IMS에만 사용할 수 있습니다.
TC-NAC	관리자 인증서에 서버 인증 EKU만 포함된 경우 FIPS 모드가 활성화되었거나 mTLS로 Tenable이 구성된 경우(ISE 버전 3.4P3 및 3.5에 도입됨) TC-NAC에 대한 인증서 기반 인증이 영향을 받을 수 있습니다.
보안 Syslog	
LDAP	
RADIUS DTLS	

⚠ 주의: 고객은 외부 pxGrid 클라이언트에서 사용하는 인증서 유형을 확인해야 합니다. 갱신 시 공용 CA 서명 인증서에는 더 이상 클라이언트 인증 EKU가 포함되지 않을 수 있습니다. 외부 pxGrid 클라이언트 통합은 ISE와 통신할 때 클라이언트 인증 EKU를 포함해야 합니다. 그렇지 않으면 연결이 거부됩니다.

문제 증상

Cisco ISE에서 서버 인증 EKU 전용 인증서를 구축한 후 고객은 선택한 서비스에 대한 현재 EKU(Extended Key Usage) 요구 사항을 충족하지 않는 pxGrid 또는 ISE IMS(Messaging Service) 인증서 업로드를 시도할 때 Cisco ISE GUI에서 인증서 가져오기 실패를 관찰합니다.

다음은 GUI에 표시되는 오류 메시지의 예입니다.

권장 사항

현재 인증서 감사(필수 첫 단계)

- 클라이언트 인증 EKU를 포함하는 인증서를 식별하기 위해 모든 공용 TLS 인증서의 인벤

토리를 준비합니다.
- 문서 인증서 사용: 위 표에 따라 Public-CA로 서명된 인증서가 사용되는지 식별합니다.
- CA 및 루트 정보를 확인합니다. 각 인증서를 발급한 CA 및 루트 문서
- 만료 날짜 확인: 정책 시행 전에 전략적으로 갱신 계획

클라이언트 EKU가 필요한 서비스에 대한 제안

아래 표에는 클라이언트 인증 EKU를 포함하는 인증서를 사용하는 Cisco ISE 서비스 및 통합에 대한 권장 작업이 나와 있습니다.

서비스	권장 작업
TC-NAC	• Tenable을 사용하면 Tenable 측에서 엄격한 EKU 검증을 비활성화하여 연결을 유지할 수 있습니다.
보안 Syslog	
LDAP	
RADIUS DTLS	
PxGrid 클라이언트 (CatC, FMC...등)	
EAP-TLS	

단기 해결 방법(2026년 6월 이전)

관리자는 다음 해결 옵션 중 하나를 선택할 수 있습니다.

옵션 1: 결합된 EKU 인증서를 제공하는 공용 루트 CA로 전환

일부 공용 루트 CA(예: DigiCert 및 IdenTrust)는 대체 루트의 EKU가 결합된 인증서를 발급하며, 이는 Chrome 브라우저 신뢰 저장소에 포함될 수 없습니다.

공용 루트 CA 및 EKU 유형의 예:

CA 벤더	EKU 유형	루트 CA	발급/하위 CA
아이덴트러스	클라이언트 인증 + 서버	IdenTrust 공공 부문 루트	IdenTrust 공공 부문 서버

트	인증	CA 1	CA 1
디지인증서	클라이언트 인증 + 서버 인증	DigiCert Assured ID Root G2	DigiCert Assured ID CA G2

이 접근 방식의 전제 조건:

- CA 공급자와 협력하여 이러한 인증서의 가용성을 확인합니다.
- 인증서를 배포하기 전에 인증서를 제공하는 서버와 인증서를 사용하는 모든 클라이언트가 해당 루트 CA를 신뢰하는지 확인합니다.
- 통신 피어와 루트 인증서 정보를 교환합니다.
- 따라서 소프트웨어 업그레이드가 즉각적으로 필요하지 않습니다.

인증서 관리 참조:

- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.3
- ISE에서 인증서 갱신 구성

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.

갱신 전략

일반적인 권장 사항은 다음과 같습니다.

- 정책 설정 해제 전에 통합된 EKU 인증서 갱신
- 최대 인증서 유효성을 위해 2026년 3월 15일 이전에 인증서를 갱신할 계획입니다.
- 이 날짜 이후에는 공용 CA 발급 인증서가 200일 동안만 유효합니다.
- Cisco에서는 이 옵션을 계속 사용하려면 이 날짜 전에 인증서를 갱신할 것을 적극 권장합니다.
- 퍼블릭 CA 정책 및 구현 날짜는 달라질 수 있습니다.
- 일부 공용 CA가 통합된 EKU 인증서 발급을 중지했으며 기본적으로 이를 제공할 수 없습니다.
- 결합된 EKU로 인증서를 생성하려면 CA 기관과 함께 공용 CA에서 제공하는 특수 프로파일을 사용합니다.

옵션 3: 평가 및 대체 CA 공급자로 마이그레이션

사설 PKI 접근 방식

- 사설 PKI로의 전환 가능성 평가
- 결합된 EKU(필요한 EKU가 있는 서버 및 클라이언트 인증서)를 사용하여 단일 인증서를 발급하도록 사설 CA 설정
- 프라이빗 CA 서명 인증서를 발급할 때 피어와 루트 인증서 정보를 공유해야 합니다.

- 인증서를 발급하거나 배포하기 전에 인증서를 제공하는 서버와 인증서를 사용하는 모든 클라이언트가 해당 루트 CA를 신뢰하는지 확인하십시오.
- 프라이빗 CA는 Chrome 루트 프로그램 정책의 적용을 받지 않습니다.
- 인증서 정책에 대한 장기 제어 기능 제공

장기 솔루션(소프트웨어 업그레이드 필요)

고객은 새로운 CA 정책에 따라 발급된 인증서를 지원하기 위해 업데이트된 인증서 처리를 도입하는 패치 릴리스로 Cisco ISE를 업그레이드해야 합니다.

다음 패치 릴리스는 2026년 4월에 계획된 이 문제를 해결합니다.

Cisco ISE 버전	패치 버전
ISE 3.1	패치 11
ISE 3.2	패치 10
ISE 3.3	패치 11
ISE 3.4	패치 6
ISE 3.5	패치 3

패치 설치 후 동작

PxGrid 인증서

패치 릴리스를 설치한 후:

- pxGrid 인증서용 서버 인증 EKU 및 클라이언트 인증 EKU를 모두 적용하는 현재 UI 요구 사항이 제거됩니다.
- Cisco ISE는 서버 인증 EKU만 포함 된 pxGrid 인증서, 서버 및 클라이언트 인증 EKU 모두 또는 EKU 확장을 포함 하지 않는 가져오기를 허용 합니다.
- 클라이언트 인증 EKU만 포함하는 인증서는 허용되지 않습니다.

ISE IMS(Messaging Service) 인증서

ISE 3.1, 3.2 및 3.3의 경우

패치를 설치한 후 동작에 변화가 없습니다. ISE 메시징 서비스에는 클라이언트 및 서버 EKU가 모두 포함된 인증서가 계속 필요합니다. 고객은 현재 인증서가 만료되면 ISE 내부 CA 인증서를 사용할

계획이어야 합니다.

ISE 3.4 및 3.5의 경우

이제 IMS는 서버 인증 EKU를 포함하는 공용 CA 인증서만 지원합니다. 그러나 IMS는 내부 Cisco ISE 통신에만 사용되므로 Cisco에서는 인증서를 갱신할 때 ISE 내부 CA 인증서를 사용하는 것을 권장합니다.

의사 결정 트리

시작하기: Cisco ISE에서 공용 CA 인증서를 사용합니까?

|

├─ 번호: 개인 PKI 또는 자체 서명

| └─ 작업 필요 없음 - 정책의 영향을 받지 않음

|

└─: 사용 중인 공용 CA 인증서

  |

  ├─ "특정 영향 받는 사용 사례" 섹션에 언급된 서비스에 사용되고 있습니까?

  | |

  |이 TLS 클라이언트로 작동할 때 ├─ 서비스 사용

  | | └─ "클라이언트 EKU가 필요한 서비스에 대한 제안" 섹션을 검토합니다.

  | |

  |이 TLS 서버(PxGrid 또는 IMS)로 작동할 때 └─ 서비스

  | |

  |의 └─을 선택할 수 있습니다.

  | |

  | ├─ 옵션 A: 대체 루트 CA로 전환

  | | ├─ 대체 루트의 결합된 EKU에 대해 CA 공급자에게 문의

  | | ├─ 모든 피어가 새 루트를 신뢰하는지 확인

  | | └─ 즉각적인 소프트웨어 업그레이드 불필요

  | |

│ ├─ 옵션 B: 기한 전에 인증서 갱신

│ │ ├─ Cisco ISE 패치의 긴급성을 해제하는 데 도움이 됩니다.

│ │ │

│ │ ├─ 최대 유효 기간: 2026년 3월 15일 이전에 갱신

│ │ └─ 인증서 만료까지 소요 시간

│ │

│ ├─ 옵션 C: 프라이빗 PKI로 마이그레이션

│ │ ├─ 프라이빗 CA 인프라 설정

│ │ ├─ 통합 EKU 인증서 발급

│ │ ├─ ISE Trusted Store에 새 CA 설치

│ │ └─ 장기 제어

│ │

│ └─ D: 소프트웨어 업그레이드 계획

│ ├─ 필수 ISE 패치 릴리스 적용(2026년 4월부터 사용 가능)

FAQ(자주 묻는 질문)

일반 질문

Q: 프라이빗 PKI를 사용할 경우 이에 대한 고민이 필요합니까?

A : 아니요. 이 정책은 공용 루트 CA에서 발급한 인증서에만 적용됩니다. 프라이빗 PKI 및 자체 서명 인증서는 영향을 받지 않습니다.

Q: 기존 인증서를 계속 사용할 수 있습니까?

A : 예. 통합된 EKU를 사용하는 기존 인증서는 만료될 때까지 유효합니다. 이 문제는 갱신해야 할 때 발생합니다. 만료될 때까지 TLS 및 mTLS 연결 모두에서 작동합니다.

Q: mTLS 또는 표준 TLS를 사용하는지 어떻게 알 수 있습니까?

A : 영향을 받는 특정 활용 사례 섹션을 검토합니다.

업그레이드 질문

인증서 관리

일정 질문

Q: 2026년 6월 15일에 무슨 일이 일어나나요?

A : Chrome은 서버 및 클라이언트 인증 EKU를 모두 포함하는 공용 TLS 인증서의 신뢰를 중지합니다. 이러한 인증서를 사용하는 서비스는 실패할 수 있습니다.

Q: 2026년 3월 15일 이전에 갱신해야 하는 이유는 무엇입니까?

A : 2026년 3월 15일 이후에는 인증서 유효기간이 398일에서 200일로 줄어듭니다. 이 날짜 전에 갱신하면 최대 인증서 수명이 제공됩니다.

Q: 조치 기한은 어떻게 됩니까?

A : 마감일은 여러 가지입니다.

- 2026년 3월 15일: 인증서 유효 기간이 200일로 단축됨
- 2026년 5월: 대부분의 퍼블릭 CA는 통합된 EKU 발급을 완전히 중단합니다.
- 2027년 3월: Chrome 정책이 완전히 적용됨

추가 리소스

- Cisco 버그 ID: CSCws83036 - ISE에서 ClientAuth EKU 시행의 영향 평가

외부 참조

- Chrome 루트 프로그램 정책

인증 기관 리소스

- IdenTrust 포털

결론

공용 CA 인증서에서 클라이언트 인증 EKU의 선셋은 mTLS 연결을 사용하는 Cisco ISE 구축에 영향을 미치는 중요한 보안 정책 전환을 나타냅니다. 이는 업계 전반의 변화이지만 영향 등급은 매우 중요하며 서비스 중단을 방지하기 위해 즉각적인 조치가 필요합니다.

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.