공용 CA 인증서에서 Expressway for Client Auth EKU 일몰 준비

목차

소개

이 문서에서는 Cisco Expressway의 Chrome 루트 프로그램 정책 변경 사항 및 6/26 이후 공용 CA 인증서의 클라이언트 인증 EKU 일몰에 대해 설명합니다.

백그룹 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. 이 점은 Cisco Expressway와 같이 서로 다른 연결 시나리오에서 서버와 클라이언트 역할을 모두 수행하는 제품에 특히 중요합니다.

문제 정의

Chrome 루트 프로그램 정책 변경

2026년 6월부터 Chrome 루트 프로그램 정책은 Chrome 루트 저장소에 포함된 루트 CA(Certificate Authority) 인증서를 제한하여 다목적 루트를 단계적으로 축소하여 모든 PKI(public-key infrastructure) 계층을 정렬하여 TLS 서버 인증 사용 사례만 제공합니다.

주요 정책 요구 사항

- 공용 루트 CA는 서버 인증(id-kp-serverAuth)에 대해서만 EKU(Extended Key Usage)를 어설션해야 합니다.
- 인증서는 Google Chrome 브라우저에서 신뢰를 유지하기 위해 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: 2026년 6월

공용 CA 응답 일정

- 2025년 10월: 많은 공용 CA(DigiCert, Sectigo, SSL)가 기본적으로 서버 전용 인증서를 발급하기 시작했습니다

- 2026년 2월 11일: Let's Encrypt는 기존 ACME 프로필을 사용하여 클라이언트 인증 EKU를 통한 인증서 발급을 중지합니다
- 2026년 5월: 공용 CA 서버가 클라이언트 인증 EKU 인증 발급을 중지합니다.
- 2026년 6월: 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.

관련 Cisco 문서

- Cisco 버그 ID: CSCwr73373- Expressway용 별도의 서버 및 클라이언트 인증서 지원
- 필드 알림: FN 74362
- Chrome Root Program Policy: Chrome Root Program Policy 설명서

Expressway 솔루션에 미치는 영향

영향을 받는 제품

Field Notice FN74362에 따라 모든 Cisco Expressway 버전이 영향을 받습니다.

제품	영향을 받는 릴리스	영향
Expressway 코어 및 에지	X14(모든 버전)	X14.0.0~X14.3.7 - 모든 릴리스가 영향을 받음
Expressway 코어 및 에지	X15(X15.4 이전 버전)	X15.0.0~X15.3.2 - 모든 릴리스가 영향을 받음

Expressway의 이중 역할

Cisco Expressway 제품(Expressway-C 및 Expressway-E)은 다양한 연결 시나리오에서 서버 및 클라이언트 역할을 수행하며, 서버 및 클라이언트 인증 EKU를 모두 포함하는 인증서가 필요합니다.

Expressway E as Server(서버 인증 EKU 필요):

- HTTPS 브라우저 액세스
- SIP UC 접근 연결
- Webex Edge 오디오/MRA 연결

Expressway E as Client(클라이언트 인증 EKU 필요):

- B2B 통신
- MRA(모바일 및 원격 액세스) 연결
- XMPP 페더레이션

- SIP 네이버 영역/CMS 연결
- 외부 엔티티와의 상호 작용
- Cisco Cloud에 연결(MRA 온보딩)

영향을 받는 특정 활용 사례

Cisco Expressway에서 현재 mTLS 연결에 사용되는 클라이언트 인증 EKU가 있는 공용 CA 서명 인증서는 Expressway 서버 인증서입니다. 이 인증서는 다음 mTLS 연결에 사용됩니다.

1. mTLS를 통한 SIP B2B 호출 - Expressway E는 세션 시작 사이트에 따라 mTLS 연결에서 클라이언트 또는 서버가 됨
2. SIP IMP Federation over mTLS - Expressway E는 세션 시작 사이트에 따라 mTLS 연결에서 클라이언트 또는 서버가 됨
3. UC Traversal Zone - Expressway C에서 클라이언트 인증 EKU 표시
4. Traversal Zone with mTLS configuration(mTLS 컨피그레이션이 포함된 접근 영역) - Expressway C에서 클라이언트 인증 EKU 표시
5. mTLS 컨피그레이션이 포함된 SIP Neighbor Zone - Expressway는 세션 시작 사이트에 따라 mTLS 연결에서 클라이언트 또는 서버가 됩니다(다음과의 연결 포함).

- Cisco Unified Communications Manager(Unified CM)
- Cisco Unity
- CUBE(Cisco Unified Border Element)
- CMS(Cisco Meeting Server)
- Cisco Cloud 연결 - MRA 온보딩(Expressway가 Cisco Cloud 연결을 시작하고 클라이언트 인증 EKU 제시)

권장 사항

현재 인증서 감사(필수 첫 단계)

해결 방법 및 솔루션 옵션을 고려하기 전에 Field Notice FN74362에 따라 다음을 수행합니다.

- 클라이언트 인증 EKU를 포함하는 인증서를 식별하기 위해 모든 공용 TLS 인증서의 인벤토리를 준비합니다.
- Cisco Expressway 인스턴스를 백업하거나 서명된 인증서 및 개인 키를 수동으로 복사합니다
- 문서 인증서 사용: mTLS 연결에 사용되는 인증서 식별
- CA 및 루트 정보를 확인합니다. 각 인증서를 발급한 CA 및 루트 문서
- 만료 날짜 확인: 정책 시행 전에 전략적으로 갱신 계획

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.

퍼블릭 루트 CA 및 EKU 유형의 예(FN당74362:

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
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 Expressway 인증서 생성 및 사용 배포 가이드(X14.0)
- Cisco Expressway 인증서 생성 및 사용 배포 가이드(X15.0)

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.

Let's Encrypt Certificates에 대한 특별 고려 사항

FN74362에 따라 Let's Encrypt 인증서를 사용하는 경우:

- 현재 Expressway는 하드 코드되어 사용자가 수정할 수 없는 클래식 ACME 프로필을 사용합니다
- 이 클래식 ACME 프로파일은 현재 서버 및 클라이언트 인증 EKU를 모두 포함하는 인증서를 요청하는 데 사용됩니다
- 2026년 2월 11일부터 이 프로필을 사용하는 인증서 요청에는 Let's Encrypt에서 생성한 인증서에 더 이상 클라이언트 인증 EKU가 포함되지 않습니다
- 자세한 내용은 2026년 TLS 클라이언트 인증 인증서 지원 종료 - 암호화합니다

사용자 암호화에 대한 작업 항목

- 2026년 2월 11일 이전에 인증서를 갱신하십시오. 90일 유효 기간을 최대화하려면 이 날짜에 최대한 가까운 것이 좋습니다.
- 2026년 2월 11일 이후 인증서가 자동으로 갱신되지 않도록 하려면 ACME 자동 스케줄러를 비활성화합니다.
- 이 작업을 수행하면 서버 인증 EKU만 포함된 버전으로 실수로 인증서를 덮어쓰지 않도록 할 수 있습니다.
- 2026년 2월 11일 이전에 갱신하지 않을 경우 Cisco TAC에 지원을 요청하십시오.

옵션 3: 평가 및 대체 CA 공급자로 마이그레이션

이 옵션은 Expressway C에만 적용되며 Expressway E에는 적용되지 않습니다.

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

⚠ 주의: 이 옵션은 외부 연결 서비스 및 브라우저 신뢰에 공용 CA 인증서가 필요한 Expressway-E에서는 사용할 수 없습니다.

장기 솔루션(소프트웨어 업그레이드 필요)

Field Notice FN74362에 따라 Cisco는 이 문제를 종합적으로 해결하기 위해 고정 릴리스에서 제품 개선 사항을 구현하고 있습니다.

고정 릴리스 일정:

제품	영향 받는 릴리스	고정 릴리스	수정의 목적	사용 가능성
Cisco Expressway	X14.x(모든 릴리스) X15.x(X15.4 이전)	X15.4	간헐적 해결: Expressway E에서 ServerAuth EKU 전용 서명 인증서를 추가로 업로드하고 Expressway E와 Expressway C 간의 MRA SIP 신호에 대한 인증서 확인 조정을 허용합니다.	2026년 2월
Cisco Expressway	X14.x(모든 릴리스) X15.x(X15.5 이전)	X15.5	포괄적인 솔루션: 클라이언트 및 서버 인증서 분리를 위한 UI 개선 사항을 제공하고 관리자에게 EKU 검사를 비활성화하는 옵션을 제공합니다.	2026년 5월

참고: Cisco Expressway E와 Expressway C를 모두 동일한 버전으로 업그레이드해야 합니다.

Cisco Expressway X15.4 솔루션 세부사항(2026년 2월)

목적: ServerAuth EKU를 사용하는 인증서만 수용하고 MRA 등록을 활성화하는 간헐적 솔루션

주요 개선 사항은 다음과 같습니다.

- 인증서 업로드에 대한 제한을 제거합니다.
- 관리자가 Expressway E에서 웹 GUI를 통해 서버 인증 EKU만 사용하여 인증서를 업로드할 수 있습니다.
- 이전에는 Expressway가 서버 전용 인증서를 거부했습니다.
- MRA에 대한 인증서 확인을 조정합니다.
- MRA 솔루션에서 Expressway-E와 Expressway-C 간의 SIP 시그널링에 대한 인증서 확인을 수정합니다.
- 서드파티 애플리케이션에서 서버 전용 인증서를 수락할 수 있습니다.

X15.4로 업그레이드할 수 있는 사용자:

- 서버 전용 서명 인증서를 사용하여 MRA용 Expressway-E를 새로 배포하거나 재배포하는

경우.
- 2026년 2월 11일 이후에 ACME(Let's Encrypt) 인증서를 사용하는 경우.
- 서버 인증 EKU만 포함된 서명된 인증서를 업그레이드해야 하는 기존 구축입니다.
- mTLS 연결에서 인증서 관련 인증 문제가 발생하는 경우

X15.4의 중요 요구 사항:

- Expressway-E와 Expressway-C를 모두 X15.4로 업그레이드해야 합니다.
- 서비스 중단을 최소화하기 위해 유지 보수 기간 동안 업그레이드 계획

X15.4의 제한 사항은 다음과 같습니다.

- 이는 즉각적인 호환성 문제를 해결하는 간헐적인 솔루션입니다
- 완전한 이중 인증서 지원을 제공하지 않음
- EKU 확인을 비활성화하는 서비스 매개 변수를 포함하지 않음
- mTLS 연결은 세션 시작 사이트에 따라 실패할 수 있습니다.

Cisco Expressway X15.5 솔루션 세부사항(2026년 5월)

목적: 글로벌 Google Chrome Root Program 요구 사항을 충족하는 포괄적인 솔루션

주요 제품 개선 사항:

- 클라이언트 및 서버 인증서 분리
- 동일한 인터페이스에서 두 개의 개별 인증서에 대한 지원을 활성화합니다
- 고유 서버 인증 EKU 및 클라이언트 인증 EKU가 있는 Expressway 인증서
- 분리된 인증서 역할로 적절한 mTLS 연결 지원
- UI 및 백엔드 개선 사항
- 두 인증서의 개별 관리를 위한 새로운 인증서 관리 인터페이스
- 실수로 MTLS 연결이 끊어지는 것을 방지하기 위해 인증서 업로드 중에 클라이언트 인증 EKU 검증
- 관리자는 서버 및 클라이언트 인증서를 개별적으로 업로드 및 관리할 수 있습니다
- 클라이언트 인증 EKU 확인을 비활성화 하는 옵션
- 관리자가 개별 기업 요구 사항에 따라 클라이언트 인증 EKU 확인을 비활성화할 수 있는 서비스 매개변수
- Cisco Expressway가 서버 인증 EKU 인증서만 사용하여 연결을 요청하는 원격 피어(클라이언트)의 EKU를 무시하도록 허용합니다.
- 클라이언트 인증 EKU 인증서가 없을 경우 Expressway에서 서버 인증 EKU 전용 인증서를 클라이언트 인증서로 (다시) 사용할 수 있습니다

참고: 이 경우 원격 피어는 유사한 클라이언트 인증 무시 EKU 모델도 지원해야 합니다

의사 결정 트리

시작하기: Expressway에서 공용 CA 인증서를 사용합니까?

|

├─ 번호: 개인 PKI 또는 자체 서명

| └─ 작업 필요 없음 - 정책의 영향을 받지 않음

|

└: 사용 중인 공용 CA 인증서

  |

  ├─ mTLS 연결에 사용됩니까?(특정 영향 받는 사용 사례 섹션에서 사용 사례 확인)

  | |

  | ├─ 번호: 서버 인증만

  | | └─ 영향 최소화 - 향후 변경 사항 모니터링

  | |

  | └─ 예: 클라이언트 인증 EKU를 사용하는 mTLS 연결

  | |

  |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

  | | ├─은 경우 2026년 2월 11일 이전에 갱신

  | | | └─ 갱신 후 ACME 스케줄러 비활성화

  | | ├─ 최대 유효 기간: 2026년 3월 15일 이전에 갱신

  | | └─ 인증서 만료까지 소요 시간

  | |

│ ├─ 옵션 C: 프라이빗 PKI로 마이그레이션(Expressway-C만 해당)

│ │ ├─ 프라이빗 CA 인프라 설정

│ │ ├─ 통합 EKU 인증서 발급

│ │ ├─ 모든 피어에 루트 배포

│ │ └─ Expressway-E가 아닌 장기 제어

│ │

│ └─ D: 소프트웨어 업그레이드 계획

│이 ├─? → X15.4로 업그레이드(2026년 2월)

│ └─ Comprehensive Solution → X15.5로 업그레이드(2026년 5월)

│ └─ 별도의 서버/클라이언트 인증서를 가져옵니다.

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: mTLS 연결을 사용하지 않는 경우 어떻게 합니까?

A: 표준 TLS(서버 인증)만 사용하는 경우 이 정책의 영향을 받지 않습니다. 서버 전용 인증서는 계속 작동합니다. 그러나 일부 활용 사례는 기본적으로 mTLS를 사용하므로 Specific Affected Use Cases(특정 영향 받는 활용 사례) 섹션의 목록에서 사용 사례를 확인하십시오.

Q: Expressway에 대한 표준 HTTPS 웹 연결이 작동하지 않습니까?

A: 아니요. 표준 TLS 연결은 영향을 받지 않습니다. Expressway에 대한 웹 브라우저 액세스는 서버 전용 EKU 인증서를 사용해도 계속 정상적으로 작동합니다.

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 : 검토특정 영향 받는 사용 사례 섹션.

Q. 열차 티켓을 예매하려면 어떻게 해야 하나요?

A: Cisco에서는 다음과 같은 즉각적인 조치를 적극 권장합니다.

- 인증서 감사

  mTLS에 사용되는 공용 TLS 인증서 식별

- 인증서 조기 갱신

  2026년 3월 15일 전까지 갱신하여 유효성 극대화

- ACME 자동화 제어

  인증서를 예기치 않게 교체할 수 있는 자동 갱신 비활성화

- CA와 협력

  일부 CA는 임시 또는 대체 인증서 프로필을 제공합니다

Q: CUCM SU3(a)가 X15.4 및 X15.5와 호환됩니까?

A : 예

Q: Cisco Expressway E(X15.5 릴리스 포함)에서 클라이언트 EKU 검사를 비활성화할 때 보안 취약성이 있습니까?

A: 인증서는 연결 소스가 유효한지 확인하기 위해 CN/SAN을 계속 확인하며, Google이 보안 문제를 제기할 때까지 기본적으로 포함된 EKU 검증(클라이언트 역할 목적의 인증서)만 우회하므로 이전과 비교하여 보안 문제가 없어야 합니다.

특정 암호화

Q: Expressway에서 Let's Encrypt with ACME를 사용합니다. 내가 뭘 할 수 있을까?

A :

1. 2026년 2월 11일 이전에 인증서를 갱신하십시오(가능한 한 해당 날짜에 근접함).
2. 갱신 직후 ACME 자동 스케줄러 비활성화
3. 장기 솔루션을 위해 X15.5로 업그레이드할 계획임

Q: 결합된 EKU 인증서를 계속 가져오도록 ACME 프로필을 수정할 수 있습니까?

A : 아니요. 현재 Expressway는 사용자가 수정할 수 없는 하드코딩된 "클래식" ACME 프로필을 사용합니다. ACME 인증서 프로필 지원은 Cisco TAC에 문의하십시오.

업그레이드 질문

Q: Expressway-E와 Expressway-C를 모두 업그레이드해야 합니까?

A : 네, 물론입니다. 올바른 작동을 위해서는 두 버전을 모두 동일한 버전(X15.4 또는 X15.5)으로 업

그레이드해야 합니다.

Q: X15.4로 업그레이드하거나 X15.5를 기다릴 수 있습니까?

A :

- 긴급한 문제가 있거나 서버 전용 인증서를 지금 수락해야 하는 경우 X15.4로 업그레이드하십시오.
- 가능하면 X15.5(2026년 5월)에서 듀얼 인증서 지원을 통한 포괄적인 솔루션을 기다립니다.

Q: 인증서 갱신 후 클러스터 복제가 중단되었습니다. 무슨 일인데?

A: 새 인증서에 서버 인증 EKU만 있는 경우가 많지만:

- X15.4 이전 버전에서 TLS Verify = Enforcement를 적용하는 경우: 클러스터 피어가 클라이언트 인증 EKU 없이 mTLS 연결을 설정할 수 없음
- 솔루션 옵션(하나):

  TLS 확인 모드를 "허용"(보안 수준이 낮음)으로 설정

  대체 CA 루트에서 결합된 EKU로 인증서 얻기

  ClusterDB에 대한 클라이언트 인증 EKU 확인을 우회하는 X15.4 이상으로 업그레이드

Q: X15.4로 업그레이드한 후 클러스터에 있는 서버 전용 인증서와 함께 Enforcement 모드를 사용할 수 있습니까?

A: 예. X15.4부터 Expressway는 mTLS ClusterDB 연결에 대한 클라이언트 인증 EKU 확인을 우회합니다. 따라서 하나 이상의 클러스터 노드에 서버 인증 EKU만 있는 경우에도 TLS 확인을 "적용"으로 설정할 수 있습니다.

Q: Expressway 웹 GUI를 통해 인증서를 업로드할 수 없는 이유는 무엇입니까?

A: X15.4 이전에 웹 GUI는 클라이언트 인증 EKU를 갖는 인증서가 필요한 하드코딩된 검증을 적용합니다. 인증서에 서버 인증 EKU만 있는 경우 두 가지 옵션이 있습니다.

- SCP(Secure Copy Protocol)를 사용하여 인증서를 서버(/persistent/Certs 폴더)에 직접 업로드합니다.
- X15.4 이상(Expressway-E에만 해당)으로 업그레이드하면 이 제한 사항이 제거됩니다.

Q: X15.4로 업그레이드한 후에도 서버 전용 인증서를 Expressway-E에 업로드할 수 없습니다

A: 업그레이드한 후 이 명령이 활성화되었는지 확인합니다

  xConfiguration XCP TLS 인증서 CVS EnableServerEkuUpload: On

Q: X15.4로 업그레이드했습니다. 이제 Expressway-E와 Expressway-C 모두에 서버 전용 인증서를 업로드할 수 있습니까?

A: 안돼. X15.4는 Expressway-E에 대한 업로드 제한만 제거합니다. Expressway-C는 웹 GUI를 통

한 업로드를 위해 결합된 EKU 인증서가 필요합니다. 이는 Expressway-C가 UC 접근 영역에서 TLS 클라이언트 역할을 자주 수행하며 클라이언트 인증 EKU가 필요하기 때문입니다. Expressway-E에서 이 명령을 실행해야 합니다. 이 명령은 Expressway-C에서 실행되지 않습니다

xConfiguration XCP TLS 인증서 CVS EnableServerEkuUpload: On

Q: 인증서 갱신 후에는 Smart License를 등록할 수 없습니다. 왜 그럴까요?

A : 인증서 갱신 후 Smart Licensing 실패는 일반적으로 EKU와 관련이 없습니다.

- Expressway에서 tools.cisco.com(CSSM)에 연결할 수 있는지 확인
- 방화벽 규칙에서 HTTPS 아웃바운드 허용(포트 443) 확인
- 프록시 컨피그레이션이 올바른지 확인(HTTP 프록시를 사용하는 경우)
- CSSM 서버 인증서가 Expressway 트러스트 저장소에서 트러스트되는지 확인
- Smart Licensing에는 clientAuth가 필요하지 않으므로 이 정책 변경은 영향을 주지 않습니다

MRA(모바일 및 원격 액세스) 관련

Q: MRA에는 Expressway-E에서 클라이언트 인증 EKU가 필요합니까?

A: Expressway 버전에 따라 다릅니다.

- X15.4 이전: 예, 간접적으로 필요합니다.

  MRA SIP 신호 처리 중에 Expressway-E는 SIP 서비스 메시지에서 서명된 인증서를 Expressway-C에 보냅니다

  Expressway-C가 인증서를 검증하므로 클라이언트 인증 및 서버 인증 EKU가 모두 필요합니다.

  결합된 EKU를 사용하지 않으면 MRA SIP 등록 실패

- X15.4 이상: 아니요

  Expressway-C가 더 이상 SIP 서비스 메시지에서 클라이언트 인증 EKU를 검증하지 않습니다.

  Expressway-E에는 MRA용 서버 인증 EKU만 필요

  UC 접근 영역이 단방향으로 작동함(Expressway-C는 Expressway-E 서버 인증서만 검증)

Q: 를 업로드한 후 내 네이버 영역이 실패하는 이유Expresswayx15.4의 서버 인증 EKU

A : TLS 확인 모드를 "on"으로 설정하면 클라이언트 인증 EKU가 필요합니다. 따라서 네이버 영역 구성에서 TLS 확인을 사용하지 않도록 설정할 수 있습니다

Q: MRA가 제대로 작동하려면 어떤 인증서가 필요합니까?

A : 일반적인 MRA 구축의 경우

구성 요소	인증서 요구 사항	EKU 필요	참고
Expressway-E(X15.4 이전)	serverAuth + clientAuth	둘 다	Exp-C에 의한 SIP 서비스 검증
Expressway-E(X15.4+)	serverAuth 전용	서버만	클라이언트 EKU 검사를 우회했습니다.
고속도로 C	클라이언트 인증 + 서버 인증	둘 다	UC Traversal에서 항상 클라이언트 역할 수행
UC 접근 영역	단방향 유효성 검사	Exp-E: serverAuth Exp-C: clientAuth	Exp-C에서 Exp-E 서버 인증서 검증

Q: MRA는 정상적으로 작동했지만 서버 전용 EKU로 Expressway-E 인증서를 갱신한 후 SIP 등록이 실패했습니다. 무엇이 문제입니까?

A: X15.4 이전 버전을 실행 중인 경우, MRA SIP 신호에는 SIP 서비스 메시지에 서버 및 클라이언트 인증 EKU를 모두 표시하는 Expressway-E가 필요합니다. 옵션:

- 결합된 EKU로 인증서 얻기
- 결합된 EKU를 발급하는 대체 CA 루트로 전환
- Expressway-E 및 Expressway-C를 모두 X15.4 이상으로 업그레이드(권장)

인증서 관리

Q: DigiCert 또는 IdenTrust에서 통합된 EKU로 인증서를 받으려면 어떻게 해야 합니까?

A : CA 공급자에게 문의하여 통합 EKU를 계속 발급하는 대체 루트에서 인증서를 요청합니다.

Q: 내 CA가 서버 전용 인증서만 제공할 수 있다고 합니다. 내가 뭘 할 수 있을까?

A : 몇 가지 옵션이 있습니다.

- 대체 루트 확인: CA에게 통합 EKU를 발급하는 대체 루트(예: DigiCert Assured ID 또는 IdenTrust Public Sector)가 있는지 문의하십시오.
- 스위치 CA 공급자: Chrome을 신뢰하지 않는 루트에서 통합된 EKU를 제공하는 CA 찾기
- 개인 PKI 사용: 결합된 EKU 인증서를 위한 내부 CA 설정(Expressway-C 구축에만 해당)
- X15.4로 업그레이드: ServerAuth EKU를 사용하는 인증서만 수용하고 MRA 등록을 활성화하는 간헐적 솔루션
- X15.5로 업그레이드 가능 후: 서버 전용 인증서를 수용할 수 있는 듀얼 인증서 아키텍처를 계획하고 글로벌 Google Chrome Root Program 요구 사항을 충족하는 포괄적인 솔루션

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.

- February 11, 2026: Let's Encrypt stop combined EKU via classic ACME
- 2026년 3월 15일: 인증서 유효 기간이 200일로 단축됨
- 2026년 5월: 대부분의 퍼블릭 CA는 통합된 EKU 발급을 완전히 중단합니다.
- 2026년 6월: Chrome 정책이 완전히 적용됨

추가 리소스

Cisco 설명서

- 필드 알림 FN74362: Cisco Expressway가 TLS 인증서의 향후 변경 사항으로 인해 보안 통신에 미치는 영향
- Cisco 버그 ID CSCwr73373: Expressway용 별도의 서버 및 클라이언트 인증서 지원

외부 참조

- Chrome 루트 프로그램 정책
- 암호화할 내용: 2026년에 TLS 클라이언트 인증 인증서 지원 종료
- CA/브라우저 포럼 베이스라인 요구 사항

인증 기관 리소스

- DigiCert 지원 포털
- IdenTrust 인증서 서비스
- 커뮤니티 포럼 암호화
- 섹티고 기술 자료

결론

공용 CA 인증서에서 클라이언트 인증 EKU의 일몰은 mTLS 연결을 사용하는 Cisco Expressway 구축에 영향을 주는 중요한 보안 정책 전환을 나타냅니다. 이는 업계 전반의 변화이지만, 영향 등급은 Field Notice FN74362에 따라 매우 중요하며, 서비스 중단을 방지하기 위해 즉각적인 조치가 필요합니다.

핵심 요점

- 이는 모든 Expressway 버전(X15.4 이전 X14 및 X15)에 영향을 미칩니다.
- 지금 인증서 감사 - 필수 첫 번째 단계입니다
- 다양한 해결 방법 사용 가능 - 환경에 가장 적합한 방법을 선택하십시오.
- 장기 솔루션을 위해 소프트웨어 업그레이드 필요 - X15.5 계획
- Expressway-E와 Expressway-C를 함께 업그레이드해야 합니다.
- Let's Encrypt users have the earliest deadline - 2026년 2월 11일

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.