Expressway 인증서 갱신

목차

소개

이 문서에서는 Expressway/VCS(Video Communication Server) 인증서 갱신 프로세스에 대해 설명합니다.

이 문서의 정보는 Expressway 및 VCS에 모두 적용됩니다. 이 문서는 Expressway를 참조하지만 VCS와 상호 교환할 수 있습니다.

> **참고:** 이 문서는 인증서 갱신 프로세스에 도움이 되도록 설계되었지만, 사용 중인 버전에 대한 Cisco Expressway 인증서 생성 및 사용 구축 가이드도 확인하는 것이 좋습니다.

배경 정보

인증서를 갱신할 때마다, 새 인증서가 설치된 후에도 시스템이 계속 제대로 작동하도록 하려면 두 가지 주요 사항을 고려해야 합니다.

1. 새 인증서의 특성은 이전 인증서의 특성과 일치해야 합니다(주로 주체 대체 이름 및 확장 키 사용)

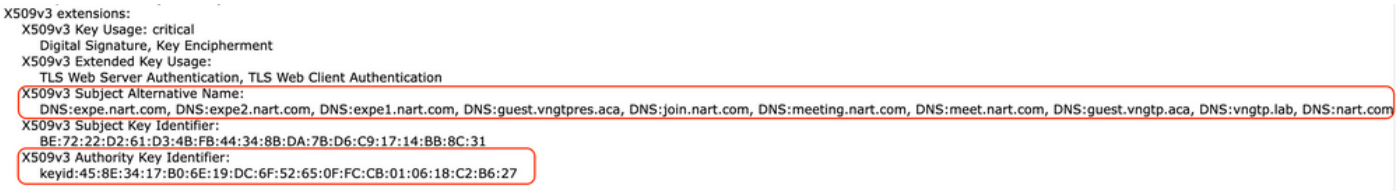
2. 새 인증서를 서명하는 데 사용할 CA(Certification Authority)가 Expressway(예: CUCM, Expressway-C, Expressway-E 등)와 직접 통신하는 다른 서버에서 신뢰받을 수 있어야 합니다.

프로세스

A) 현재 인증서에서 정보 가져오기

1. Expressway 웹 페이지 **유지 관리 > 보안 > 서버 인증서 > 해독된 표시 를 엽니다.**

2. 열리는 새 창에서 "주체 대체 이름" 및 "권한 키 식별자" X509v3 확장을 메모장 문서에 복사합니다.

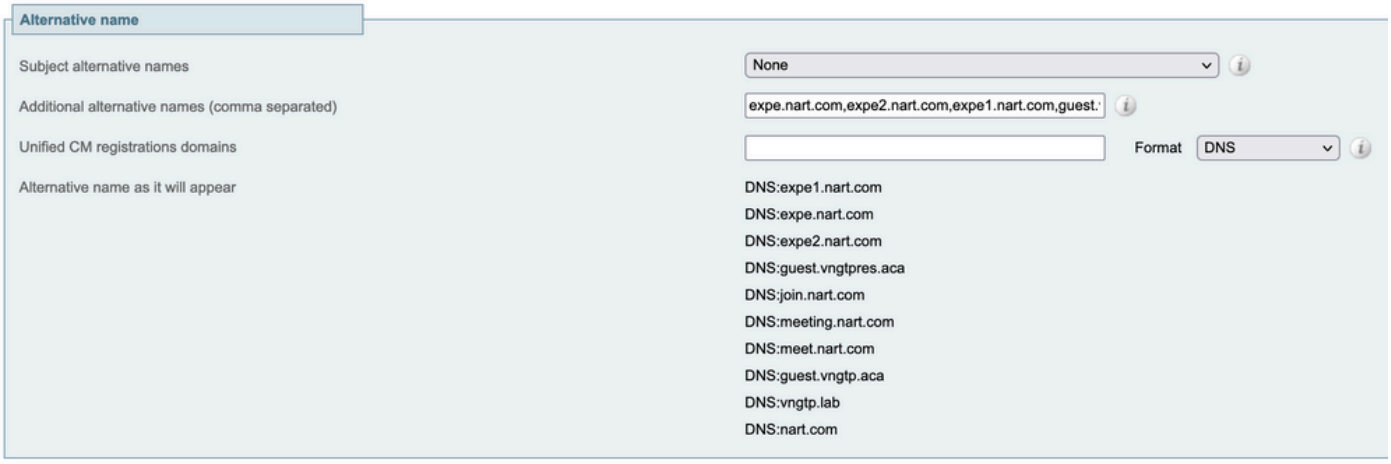


"Show decoded" 인증서 창

B) CSR(Certificate Signing Request)을 생성하고 서명을 위해 CA(Certificate Authority)에 전송합니다.

1. Expressway 웹 페이지 유지 관리 **> 보안 > 서버 인증서 > CSR 생성.**

2. Generate CSR(CSR 생성) 창의 **Additional alternative names (comma separated) 필드**에서 섹션 A에 저장한 "Subject Alternative Names"의 모든 값을 입력하고 "DNS:"를 제거한 후 목록을 쉼표로 구분하려면 이미지를 참조하십시오("표시될 대체 이름" 옆에 있는 인증서에 사용할 모든 SAN 목록을 볼 수 있습니다).



CSR SAN 항목 생성

3. 국가, 회사, 국가 등의 **추가 정보** 섹션에 있는 나머지 정보를 입력하고 CSR 생성을 **클릭합니다.**

4. CSR을 생성한 후에는 **Maintenance(유지 관리) > Security(보안) > Server Certificate(서버 인증서) 페이지**에 CSR을 **폐기하고 다운로드할 수** 있는 옵션이 표시됩니다. Download(다운로드)**를** 선택하고 서명을 위해 CA에 CSR을 보내야 합니다.

> **참고:** 새 인증서를 설치하기 전에 CSR을 **폐기하지** 마십시오. Discard CSR(CSR **폐기**)을 완료한 후 폐기된 CSR로 서명된 인증서를 설치하려고 하면 인증서 설치가 실패합니다.

C) 새 인증서에서 SAN 목록 및 확장/확장 키 사용 특성을 확인합니다

Windows 인증서 관리자에서 새로 서명된 인증서를 열고 다음을 확인합니다.

1. SAN 목록은 CSR을 생성한 후 사용한 섹션 A에 저장한 SAN 목록과 일치합니다.

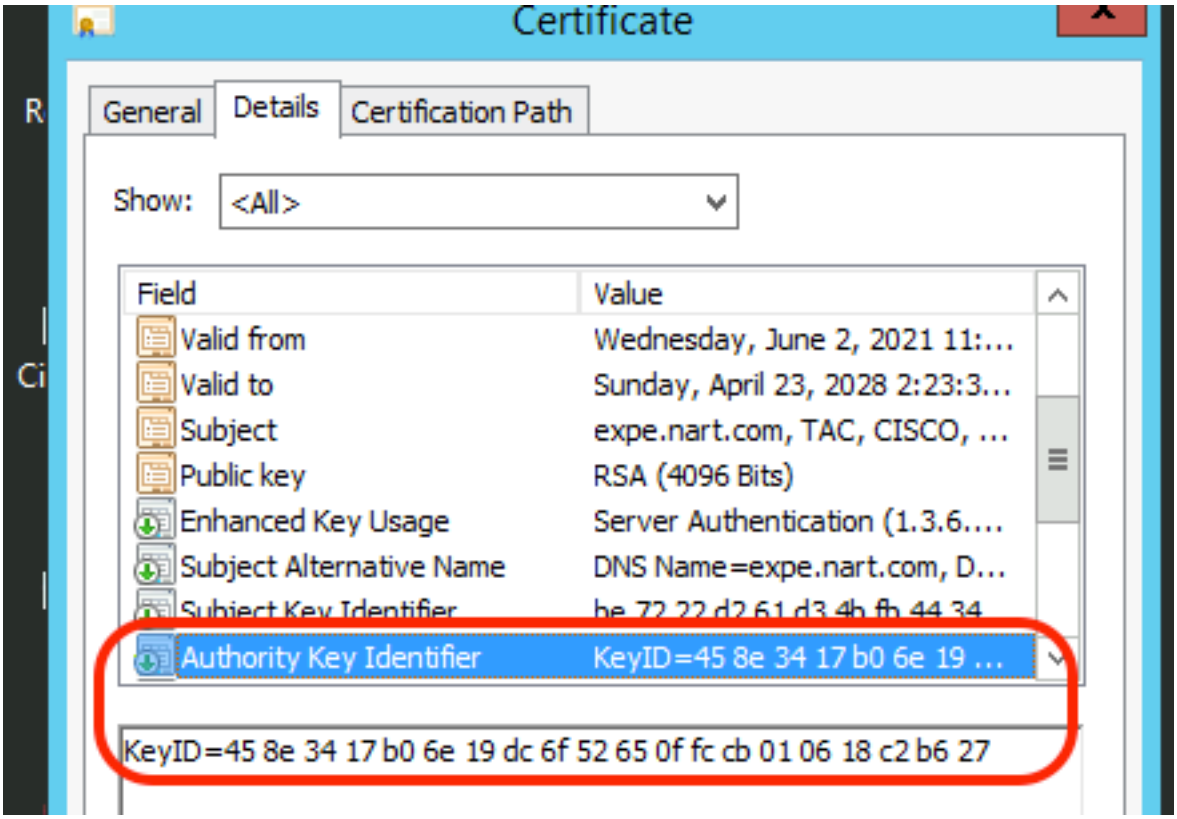
2. "확장/확장 키 사용" 특성에는 "클라이언트 인증" 및 "서버 인증"이 모두 포함되어야 합니다.

> **참고:** 인증서의 확장명이 .pem인 경우 Windows Certificate Manager에서 열 수 있도록 이름을 .cer 또는 .crt로 변경합니다. Windows Certificate Manager에서 인증서를 연 후에는 **Details(세**

부 사항) 탭 > Copy to File(파일**에 복사)**로 이동하여 Base64 인코딩 파일로 내보낼 수 있습니다. 일반적으로 Base64 인코딩 파일은 텍스트 편집기에서 열 때 위쪽에 "-----BEGIN CERTIFICATE-----"가 있고 아래쪽에 "-----END CERTIFICATE-----"가 있습니다

D) 새 인증서를 서명한 CA가 이전 인증서를 서명한 CA와 동일한지 확인

Windows 인증서 관리자에서 새로 서명된 인증서를 열고 "Authority Key Identifier(권한 키 식별자)" 값을 복사하여 섹션 A에 저장한 "Authority Key Identifier(권한 키 식별자)" 값과 비교합니다.



Windows 인증서 관리자로 열린 새 인증서

두 값이 동일한 경우, 이는 이전 인증서를 서명하는 데 사용된 것과 동일한 CA가 새 인증서를 서명하는 데 사용되었음을 의미하며, E 섹션으로 이동하여 새 인증서를 업로드할 수 있습니다.

값이 다르면 새 인증서를 서명하는 데 사용된 CA가 기존 인증서를 서명하는 데 사용된 CA와 다르며, E 섹션으로 진행하기 전에 따라야 할 단계는 다음과 같습니다.

1. 모든 중간 CA 인증서(있는 경우) 및 루트 CA 인증서를 가져옵니다.

2. **Maintenance(유지 관리) > Security(보안) > Trusted CA certificate(신뢰할 수 있는 CA 인증서)**로 이동하여 Browse(찾아보기)를 클릭한 다음 컴퓨터에서 중간 CA 인증서를 검색하여 업로드합니다. 다른 중간 CA 인증서 및 루트 CA 인증서에 대해서도 동일한 작업을 수행합니다.

3. 이 서버에 연결된 Expressway-E(갱신할 인증서가 Expressway-C 인증서인 경우) 또는 이 서버에 연결된 Expressway-C(갱신할 인증서가 Expressway-E 인증서인 경우)에서 동일하게 수행합니다.

4. 갱신할 인증서가 Expressway-C 인증서이고 MRA가 있거나 CUCM에 대한 보안 영역이 있는 경우 CUCM이 새 루트 및 중간 CA를 신뢰하고 루트 및 중간 CA 인증서를 CUCM tomcat-trust 및 callmanager-trust 저장소에 업로드한 다음 CUCM에서 관련 서비스를 다시 시작해야 합니다.

E) 새 인증서 설치

이전의 모든 포인트를 확인한 후에는 **Maintenance(유지 관리) > Security(보안) > Server Certificate(서버 인증서)**에서 Expressway에 새 인증서를 설치할 수 있습니다. Browse(찾아보기)를 클릭하고 컴퓨터에서 새 인증서 파일을 선택하여 업로드할 수 있습니다.

새 인증서를 설치한 후 Expressway를 다시 시작해야 합니다.

> **참고: Maintenance(유지 관리) > Security(보안) > Server Certificate(서버 인증서)**에서 Expressway로 업로드하는 인증서에는 Expressway 서버 인증서만 포함되어 있고 전체 인증서 체인이 포함되어 있지 않은지, Base64 인증서가 포함되어 있는지 확인합니다

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.