Expressway 인증서 문제 해결

목차

소개

이 문서에서는 인증서가 작동하는 방법과 Expressway 서버의 가장 일반적인 인증서 문제 및 팁에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Expressway 및 VCS(Video Communications Server) 서버
- SSL(Secure Sockets Layer)
- 인증서
- 텔레프레즌스 장치
- 모바일 및 원격 액세스
- 협업 구축

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Expressway x14

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.

배경 정보

SSL과 인증서는 표준이며 다른 디바이스와 브랜드에서 동일하게 작동합니다. 이 문서에서는 Expressway의 인증서 사용에 대해 중점적으로 설명합니다.

정의

인증서는 두 디바이스 간의 보안 연결을 생성하는 데 사용됩니다. 서버 또는 디바이스 ID를 인증하는 디지털 서명입니다. HTTPS(Hypertext Transfer Protocol Secure) 또는 SIP(Session Initiation Protocol) TLS(Transport Layer Security)와 같은 일부 프로토콜의 경우 작동하려면 인증서를 사용해야 합니다.

인증서에 대해 이야기할 때 사용되는 다른 용어:

- CSR(Certificate Signing Request): 나중에 서명하고 클라이언트 또는 서버 인증서로 변환하기 위해 디바이스를 식별하는 이름으로 생성된 템플릿입니다
- 인증서: 서명된 CSR입니다. 이러한 ID는 ID 유형이며 SSL 협상에 사용하기 위해 디바이스에 설치됩니다. 자체 또는 인증 기관에서 서명할 수 있습니다.
- 인증서 서명: 해당 인증서가 합법적인지 확인하는 ID입니다. 이는 다른 인증서의 형태로 표시됩니다.
- 자체 서명 인증서: 자체적으로 서명한 클라이언트 또는 서버 인증서
- CA(Certificate Authority): 인증서에 서명하는 엔터티
    - Intermediate Certificate(중간 인증서): 자체 서명되지 않고 다른 CA 인증서에 의해 서명되는 CA 인증서입니다. 일반적으로 루트 인증서에 의해 서명되지만 다른 중간 인증서에 의해 서명될 수도 있습니다.
    - 루트 인증서: 자체 서명된 CA 인증서

기본 원리

클라이언트가 서버와 대화하고 SSL 대화를 시작하면 인증서를 교환하며, 이는 나중에 디바이스 간 트래픽을 암호화하는 데 사용됩니다. 교환의 일환으로 디바이스는 인증서를 신뢰할 수 있는지도 확인합니다. 인증서를 신뢰할 수 있는지 여부를 확인하려면 여러 조건을 충족해야 합니다.

- 서버에 접속하기 위해 초기에 사용된 FQDN(Fully Qualified Domain Name)은 서버가 제공한 인증서 내부의 이름과 일치합니다.
    - 예를 들어 브라우저에서 웹 페이지를 열 때 cisco.com은 인증서를 제공하는 서버의 IP를 확인합니다. 신뢰할 수 있으려면 cisco.com을 이름으로 포함해야 합니다.

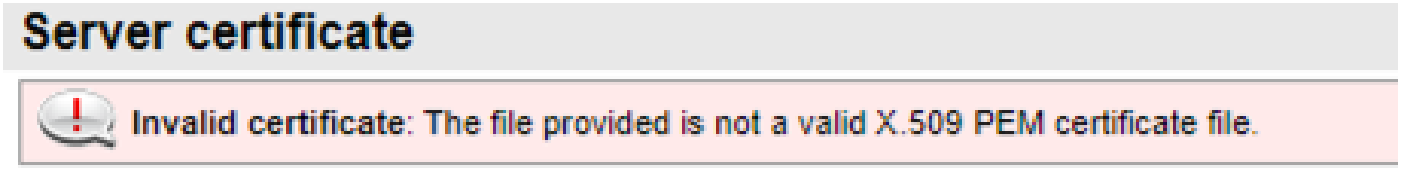
- 서버에서 제공한 서버 인증서(또는 자체 서명 시 동일한 서버 인증서)에 서명한 CA 인증서가 디바이스의 CA Trusted Certificate 목록에 있습니다.
    - 디바이스에는 신뢰할 수 있는 CA 인증서 목록이 있으며, 컴퓨터는 잘 알려진 공용 인증 기관이 있는 사전 구축 목록을 포함하는 경우가 많습니다.

- 현재 날짜와 시간은 인증서의 유효 기간 이내입니다.
  - 인증 기관은 설정된 시간 동안 CSR에 서명만 합니다. 이는 CA에 의해 결정됩니다.
- 인증서가 해지되지 않았습니다.
  - 공용 인증 기관은 인증서 내에 인증서 취소 목록 URL을 포함하는 경우가 많습니다. 이는 인증서를 받은 당사자가 CA에서 인증서를 취소하지 않았음을 확인할 수 있도록 하기 위한 것입니다.

일반적인 문제

Expressway 인증서 업로드 실패

이런 원인이 될 수 있는 몇 가지 조건이 있다. 다른 설명 오류가 발생합니다.



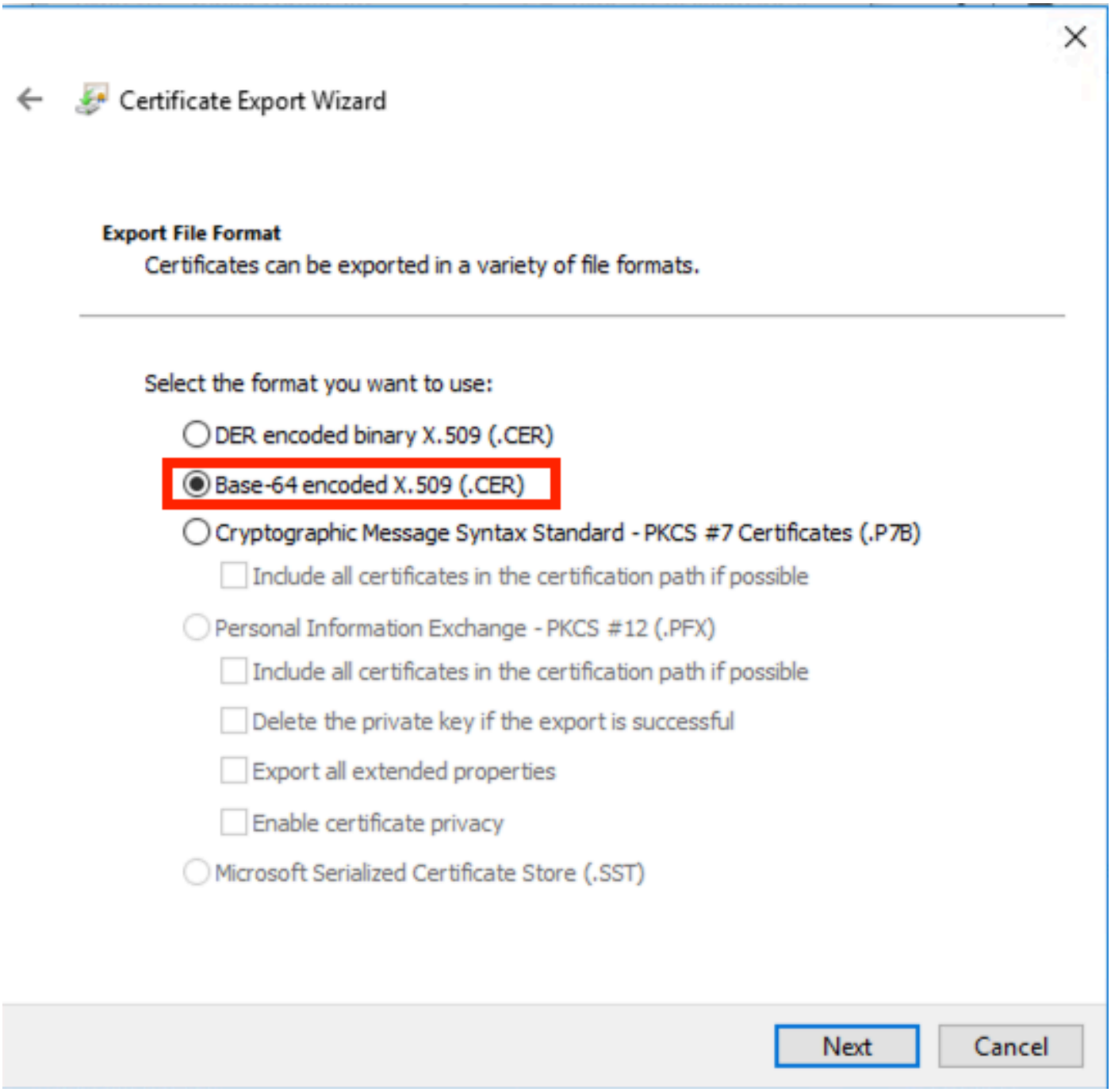
인증서 형식이 잘못되었습니다.

이 첫 번째 오류는 인증서가 유효한 형식이 아닐 때 발생합니다. 파일 확장명은 중요하지 않습니다.

인증서가 열리지 않으면 CA에서 올바른 형식으로 새 인증서를 요청할 수 있습니다

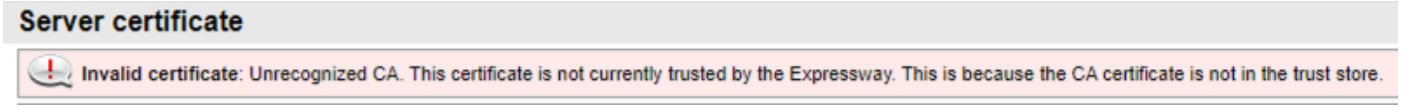
인증서가 열려 있으면 다음 단계를 수행하십시오.

1단계. 인증서를 열고 Details(세부사항) 탭으로 이동합니다.
2단계. 파일에 복사를 선택합니다.
3단계. 마법사를 따라 Base-64 인코딩이 선택되었는지 확인합니다.



인증서 형식 선택

4단계. 저장했으면 Expressway에 새 파일을 업로드합니다.



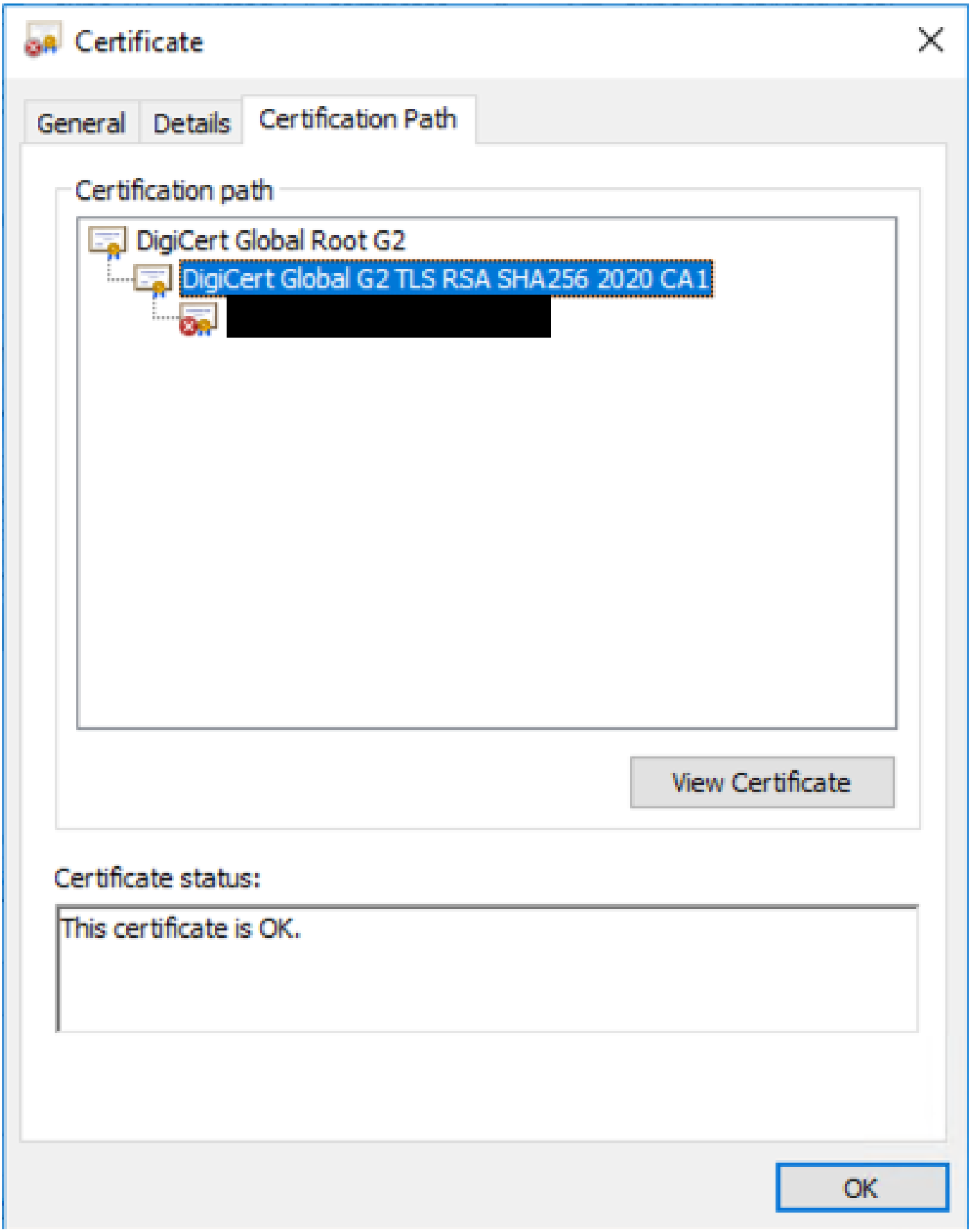
신뢰할 수 없는 CA 인증서 체인

이 오류는 서버 인증서를 서명한 CA 인증서를 신뢰할 수 없을 때 발생합니다. 서버 인증서를 업로드하기 전에 서버는 체인의 모든 CA 인증서를 신뢰해야 합니다.

일반적으로 CA는 서명된 서버 인증서와 함께 CA 인증서를 제공합니다. 이러한 옵션이 제공되는 경우 아래의 6단계로 건너뜁니다.

CA 인증서를 사용할 수 없는 경우 서버 인증서에서 인증서를 가져올 수 있습니다. 다음 단계를 수행합니다.

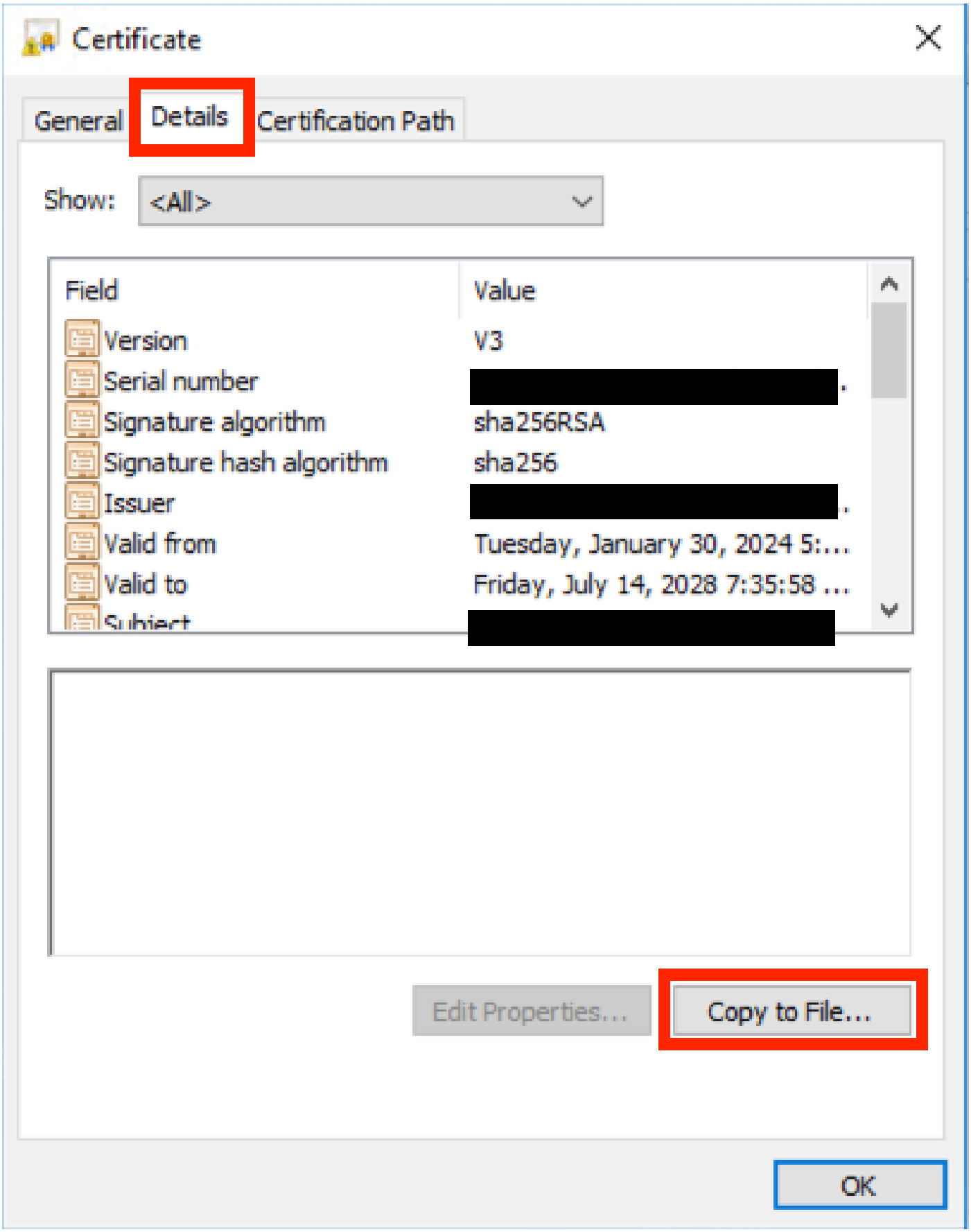
1단계. 서버 인증서를 엽니다.
2단계. Certification Path(인증 경로) 탭으로 이동합니다. 상위 인증서는 루트 CA 인증서로 간주됩니다. 아래쪽 인증서는 서버 인증서이며 그 사이의 모든 인증서는 중간 CA 인증서로 간주됩니다.
3단계. CA 인증서를 선택하고 View Certificate(인증서 보기)를 선택합니다.



인증 경로

4단계. Details(세부사항) 탭으로 이동한 다음 이전 단계를 따라 인증서를 별도의 파일에 저장합니

다.
5단계. 존재하는 모든 CA 인증서에 대해 이 단계를 반복합니다.



Certificate Details 탭

모든 CA 인증서를 사용할 수 있게 되면 Expressway Trusted CA Certificate(Expressway 신뢰할 수 있는 CA 인증서) 목록에 업로드합니다.

6단계. Expressway 서버에서 Maintenance(유지 관리) > Security(보안) > Trusted CA Certificate(신뢰할 수 있는 CA 인증서)로 이동합니다.
7단계. Choose File and upload를 선택합니다.
8단계. 각 CA 인증서에 대해 7단계를 반복합니다.
9단계. 모든 CA 인증서가 신뢰 목록에 업로드되면 서버에 서버 인증서를 업로드합니다.

Traversal Zone down with error TLS Negotiation Error(TLS 협상 오류 오류로 이동 영역 중단)

이 오류는 Expressway-C와 Expressway-E 간의 SSL 교환이 성공적으로 완료되지 않았을 때 발생합니다. 이를 유발할 수 있는 몇 가지 예는 다음과 같습니다.

- 호스트 이름이 제공된 인증서의 이름과 일치하지 않습니다.
  - Expressway-C 접근 영역에 구성된 피어 주소가 Expressway-E 서버 인증서의 이름 중 하나 이상과 일치하는지 확인합니다
- TLS Verify(TLS 확인) 이름이 제공된 인증서의 이름과 일치하지 않습니다.
  - Expressway-E 접근 영역에 구성된 TLS Verify 이름이 Expressway-C 서버 인증서의 이름 중 하나와 일치하는지 확인합니다. 클러스터 컨피그레이션인 경우 Expressway-C 클러스터 FQDN을 TLS로 구성하는 것이 좋습니다. 이 이름이 클러스터의 모든 노드에 있어야 하므로 이름을 확인합니다.
- CA 인증서는 서버에서 신뢰하지 않습니다
  - 서버 인증서를 업로드하기 전에 각 서버가 자체 CA 인증서를 신뢰해야 하는 것처럼, 다른 서버도 서버 인증서를 신뢰하려면 해당 CA 인증서를 신뢰해야 합니다. 이를 위해 두 Expressway 서버의 인증 경로에 있는 모든 CA 인증서가 관련된 모든 서버의 신뢰할 수 있는 CA 목록에 있는지 확인합니다. CA 인증서는 이 문서의 앞부분에서 설명한 단계를 통해 추출할 수 있습니다.

Traversal Zone up(통과 영역)을 사용하지만 인증서 갱신 후 SSH 터널 다운(Tunnels Down)

SSH 터널 실패

이 오류는 중간 CA 인증서 중 하나 이상을 신뢰할 수 없는 경우 인증서 갱신 이후에 일반적으로 발생하며, 루트 CA 인증서 신뢰는 접근 영역 연결을 활성화하지만, SSH 터널은 더 자세한 연결이며 전체 체인을 신뢰할 수 없는 경우 실패할 수 있습니다. 중간 CA 인증서는 종종 인증 기관에 의해 변경되므로 인증서 갱신으로 인해 이 문제가 발생할 수 있습니다. 모든 중간 CA 인증서가 모든 Expressway 신뢰 목록에 업로드되었는지 확인합니다.

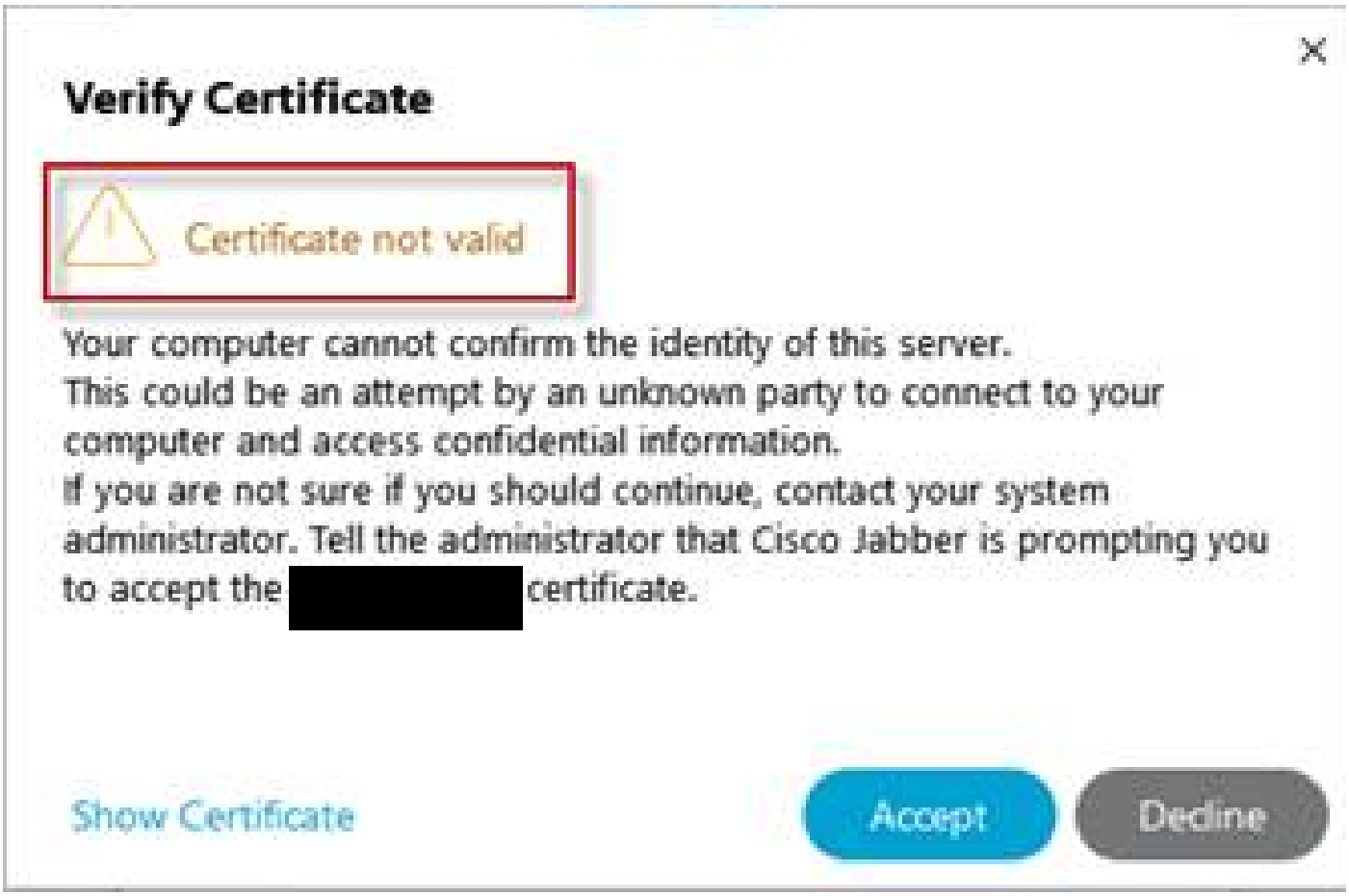
업그레이드 또는 인증서 갱신 후 모바일 및 원격 액세스 로그인이 실패함

여러 가지 방법으로 인증서 때문에 로그인이 실패할 수 있지만, 최신 버전의 Expressway 소프트웨어에서는 보안상의 이유로 이전에 하지 않은 위치에서 인증서 확인을 강제하는 일부 소프트웨어 변경이 구현되었습니다.

여기서 더 잘 설명됨: 트래픽 서버가 인증서 확인을 시행함

해결 방법으로 Expressway-C CA 인증서가 Cisco Unified Communications Manager에 tomcat-trust 및 callmanager-trust로 업로드되었는지 확인하고 필요한 서비스를 재시작합니다.

모바일 및 원격 액세스 로그인 시 Jabber의 인증서 알람



Jabber 신뢰할 수 없는 인증서 경고

이 동작은 응용 프로그램에 사용된 도메인이 Expressway-E 서버 인증서의 주체 대체 이름과 일치하지 않을 때 발생합니다.
example.com 또는 alternative collab-edge.example.com이 인증서에 있는 주체 대체 이름 중 하나인지 확인합니다.

관련 정보

Cisco 기술 지원 및 다운로드

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.