

2021-03-31의 Cisco Webex 루트 CA 인증서 업데이트

목차

[소개](#)

[사용되는 구성 요소](#)

[문제](#)

[솔루션](#)

소개

이 문서에서는 Cisco Webex가 새로운 인증 기관인 IdenTrust Commercial Root CA 1로 전환하는 방법에 대해 설명합니다. Expressway를 사용하여 Webex 회의에 전화를 걸거나 Expressway를 활용하는 커넥터 중 하나를 사용하는 고객은 2021-03-31년 이전에 Expressway 디바이스에 새 인증서를 업로드해야 합니다.

사용되는 구성 요소

이 문서의 정보는 VCS(Video Communication Server)-Expressway 또는 Expressway를 기반으로 합니다.

문제

루트 CA 인증서가 Expressway 신뢰 저장소에 업로드되지 않은 경우 Webex와의 TLS 협상이 다음 구축에서 실패할 수 있습니다.

- 엔드포인트를 사용하여 VCS-Expressway 또는 Expressway Edge를 통해 Cisco Webex Video Platform에 연결합니다. VCS 또는 Expressway의 신뢰할 수 있는 루트 저장소에 새 인증서를 추가해야 합니다.
- VCS-Control 또는 Expressway Core에서 커넥터 또는 하이브리드 서비스를 사용하며 클라우드 인증서 관리로 선택하지 않았습니다. VCS의 신뢰할 수 있는 루트 저장소에 새 인증서를 추가해야 합니다.
- VCS-Expressway 또는 Expressway Edge를 통해 Cisco Webex Edge 오디오를 사용합니다. VCS 또는 Expressway의 신뢰할 수 있는 루트 저장소에 인증서를 추가해야 합니다.
- 2021-03-23 업데이트: 클라우드 인증서 관리를 활용하는 고객은 현재 인증서 목록에 새 IdenTrust 인증서가 표시되지 않습니다. 기존 Quovadis(O=QuoVadis Limited, CN=QuoVadis Root CA 2) 인증서는 여전히 유효합니다. IdenTrust 인증서는 향후 TBD 시점에 클라우드 인증서 관리에 사용할 수 있습니다. Cloud Certificate Management를 사용하는 고객은 이번 발표를 통해 어떠한 서비스 중단도 겪지 않으며, 현재로서는 어떠한 조치도 취할 필요가 없습니다.

- Certificate Revocation List(인증서 해지 목록)를 검사하기 위해 URL에 대한 액세스를 제한했습니다. Webex 클라이언트가 <http://validation.identrust.com/crl/hydrantidcao1.crl>에서 호스팅되는 인증서 해지 목록에 도달할 수 있도록 허용해야 합니다. Cisco는 또한 인증서 확인을 위해 허용해야 하는 URL 목록에 *.identrust.com을 추가했습니다.
- 운영 체제에는 기본 인증서 신뢰 저장소를 사용하지 않습니다. 신뢰할 수 있는 루트 저장소에 인증서를 추가해야 합니다. 이 인증서는 기본적으로 모든 주요 운영 체제의 기본 신뢰 저장소에 포함되어 있습니다.

솔루션

이러한 단계는 [2021년 3월 Expressway 비디오용 Cisco Webex Root CA 인증서 업데이트에서도 설명됩니다.](#)

VCS-Control, VCS-Expressway, Expressway-Core 및 Expressway Edge에 새 인증서를 업로드하려면 다음 단계를 완료하십시오.

1단계: IdenTrust [Commercial Root CA 1](#)을 다운로드하고 identrust_RootCA1.pem 또는 identrust_RootCA1.cer로 저장합니다.

a. IdenTrust [Commercial Root CA 1](#)에 액세스합니다.

b. 상자 안에 텍스트를 복사합니다.

c. 메모장에 텍스트를 저장하고 파일을 저장합니다. 파일 이름을 identtrust_RootCA1.pem 또는 identtrust_RootCA1.cer로 지정합니다.

Home - IdenTrust Commercial Root CA 1

Copy and Paste the following DST Root certificate into a text file on your computer.

```
MIIFYDCCA0igAwIBAgIQcGFCgAAAAUjyES1AAAAAjANBgkqhkiG9w0BAQsFADBK
MQswCQYDVQQGEwJVUzESMBAGA1UEChMJSWRlbiRydXN0MScwJQYDVQQDEEx5J
ZGVu
VHJ1c3QgQ29tbWV5Y2lhbCBSb290IENBIDEwHhcNMTQwMTE2MTgxMjZWhcNMzQ
w
MTE2MTgxMjZWhcNjBKMzswCQYDVQQGEwJVUzESMBAGA1UEChMJSWRlbiRydXN0M
Scw
JQYDVQQDEEx5JZGVuVHJ1c3QgQ29tbWV5Y2lhbCBSb290IENBIDEwggliMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQCnUBneP5k91DNG8W9RYYKyqU+PZ4ldhNIT
3Qwo2dfw/66VQ3KZ+bVdfIRBuExUHTRgQ18zZshq0PirK1ehm7zCYofWjK9ouuU
+ehcCuz/mNKvcb00U590h++SvL3sTzIwiEsXXIfEU8L2ApeN2WlrvyQfYo3fw7gp
S0l4PJNgiCL8mdo2yMKi1CxUAGc1bnO/AljwpN3lsKlmesrgNqUZFvX9t++uP0D1
bVoE/c40yiTcdCMbXTMTEl3EASX2MN0CXZ/g1Ue9t0sbobtJSdifWwLziuQkkORi
T0/Br4sOdBeo0XKlanoBScy0RnnGF7Hamb4HWfp1IYVl3ZBWzvurpWCdxJ35UrCL
```

모든 Expressway 디바이스에서 Maintenance(유지 관리) > Security(보안) > Trusted CA Certificate(신뢰할 수 있는 CA 인증서)를 선택합니다.

2단계: Expressway Trust Store에 파일을 업로드합니다.



Navigation: Status > System > Configuration > Applications > Users > **Maintenance**

Overview

- System mode: Generic - Do you want to [Run service setup](#)
- System information:
 - System name
 - Up time: 4 hours 14 minutes 44 seconds
 - Software version: X12.7
 - IPv4 address: LAN 1: [redacted]
 - Options: 0 Rich Media Sessions, 5 Room Systems,
- Resource usage (last updated: 12:26:41 IST)

	Current video	Total
Registered calls		0

Maintenance Menu:

- Upgrade
- Logging
- Smart licensing
- Email Notifications
- Option keys
- Tools >
- Security** (highlighted in red)
- Backup and restore
- Diagnostics >
- Maintenance mode

Security Sub-menu:

- Trusted CA certificate** (highlighted in blue)
- Server certificate
- CRL management
- Client certificate testing

a. Expressway Trust Store에서 CA 인증서를 업로드하려면 Append CA certificate(CA 인증서 추가)를 클릭합니다.

b. 찾아보기를 클릭합니다. identtrust_RootCA1.pem 또는 identtrust_RootCA1.cer 파일을 업로드합

니다. CA 인증서를 추가합니다.

The screenshot shows the Cisco Expressway-E interface for managing trusted CA certificates. The main area displays a table of certificates with the following data:

Type	Issuer
<input type="checkbox"/> Certificate	O=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12, OU=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12
<input type="checkbox"/> Certificate	CN=federation-AD-CA-1
<input type="checkbox"/> Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2

Below the table are buttons: Show all (decoded), Show all (PEM file), Delete, Select all, Unselect all. An Upload section contains a 'Browse...' button. At the bottom, there are buttons for 'Append CA certificate' and 'Reset to default CA certificate'. A File Upload dialog is open, showing the file 'identrust_RootCA1.cer' selected in the 'CA webex cert' folder.

3단계: 인증서가 성공적으로 업로드되었으며 VCS/Expressway Trust Store에 있는지 확인합니다.

The screenshot shows the Cisco Expressway-E interface after a successful certificate upload. A message at the top indicates: 'File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0.' The table below shows the updated list of certificates:

Type	Issuer	Subject	Expiration date	Validity	View
<input type="checkbox"/> Certificate	O=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12, OU=Temporary CA f80fac88-644e-48e8-b15c-38a14839ed12	Matches Issuer	Feb 11 2023	Valid	View (decoded)
<input type="checkbox"/> Certificate	CN=federation-AD-CA-1	Matches Issuer	Apr 01 2022	Valid	View (decoded)
<input type="checkbox"/> Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer	Nov 24 2031	Valid	View (decoded)
<input type="checkbox"/> Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer	Jan 16 2034	Valid	View (decoded)

Buttons at the bottom: Show all (decoded), Show all (PEM file), Delete, Select all, Unselect all.

변경 사항을 적용하려면 이 작업 후에 재부팅하거나 다시 시작할 필요가 없습니다.

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.