Expressway-Core의 루트/중간 인증서를 CUCM에 업로드

목차

[소개](#)

[배경 정보](#)

[설정](#)

- [1단계. Expressway-C 서버 인증서를 서명한 루트 및 중간 인증서 가져오기](#)
- [2단계. CUCM에 루트 및 중간 인증서 업로드(해당되는 경우)](#)
- [3단계. CUCM에서 필요한 서비스 다시 시작](#)

[관련 정보](#)

소개

이 문서에서는 Expressway-C 인증서를 서명한 CA의 루트 및 중간 인증서를 CUCM 게시자에게 업로드하는 방법에 대해 설명합니다.

배경 정보

X14.0.2의 Expressway에서 트래픽 서버 서비스가 개선되었기 때문에 Expressway-C는 CUCM이 비보안 모드에 있는 경우에도 서버(CUCM)가 8443이 아닌 포트(예: 6971,6972)에서 실행되는 서비스에 대해 요청할 때마다 클라이언트 인증서를 보냅니다. 이 변경 사항으로 인해 Expressway-C CA(Certificate Signing Certificate Authority)가 tomcat-trust 및 callmanager-trust로 CUCM에 추가되어야 합니다.

CUCM에서 Expressway-C 서명 CA를 업로드하지 않으면 Expressway를 X14.0.2 이상으로 업그레이드한 후 MRA 로그인이 실패합니다.

CUCM이 Expressway-C가 보내는 인증서를 신뢰하려면 tomcat-trust 및 callmanager-trust에 루트 CA 및 Expressway-C 인증서 서명에 관여하는 중간 CA가 포함되어야 합니다.

설정

1단계. Expressway-C 서버 인증서를 서명한 루트 및 중간 인증서 가져오기

서버 인증서를 서명한 CA로부터 서버 인증서를 처음 받은 경우 해당 서버 인증서에 대한 루트 및 중간 인증서도 보유하여 안전한 위치에 저장합니다. 이러한 파일이 아직 있거나 CA에서 다시 다운로드할 수 있는 경우 2단계로 이동하여 CUCM에 파일을 업로드하는 방법에 대한 지침을 확인할 수 있습니다.

이러한 파일이 더 이상 없으면 Expressway-C 웹 인터페이스에서 다운로드할 수 있습니다. 이는 약간 복잡하므로 가능한 경우 CA에 문의하여 신뢰 저장소를 다운로드하는 것이 좋습니다.

Expressway-C에서 Maintenance(유지 관리) > Security(보안) > Server certificate(서버 인증서)로 이동하고 Server certificate(서버 인증서) 옆에 있는 Show(디코딩됨) 버튼을 클릭합니다. 이렇게 하면 Expressway-C 서버 인증서의 내용이 포함된 새 창/탭이 열립니다. Issuer(발급자) 필드를 찾습니다.

<#root>

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            55:00:00:02:21:bb:2d:41:60:55:d7:b2:27:00:01:00:00:02:21
    Signature Algorithm: sha256WithRSAEncryption


 Issuer: O=DigiCert Inc, CN=DigiCert Global CA-1

        Validity
            Not Before: Dec  8 10:36:57 2021 GMT
            Not After : Dec  8 10:36:57 2023 GMT
        Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=vcs-c1.vngtp.lab
        Subject Public Key Info:
...
```

이 예에서 Expressway-C 서버 인증서는 DigiCert Global CA-1(DigiCert Global CA-1)이라는 이름을 가진 Organization, DigiCert Inc.에서 발급합니다.

이제 Maintenance(유지 관리) > Security(보안) > Trusted CA certificate(신뢰할 수 있는 CA 인증서)로 이동하고 목록에서 Subject(제목) 필드에 정확히 동일한 값을 갖는 인증서가 있는지 확인합니다. 이 예에서는 Subject(제목) 필드에서 O=DigiCert Inc, CN=DigiCert Global CA-1입니다. 일치하는 항목이 있는 경우 이는 중간 CA임을 의미합니다. 이 파일이 필요하며, 루트 CA를 찾을 때까지 계속 확인해야 합니다.

일치하는 항목을 찾을 수 없는 경우 Subject of Matches Issuer(일치하는 주체 발급자)의 Issuer(발급자) 필드에서 이 값을 갖는 인증서를 검색합니다. 일치하는 항목이 있는 경우 이는 루트 CA 파일이며 이 파일만 필요한 것임을 의미합니다.

	Type	Issuer	Subject
☐	Certificate	CN=vngtp-ACTIVE-DIR-CA	Matches Issuer
☐	Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer
☐	Certificate	O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root	Matches Issuer
☐	Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	Matches Issuer
☐	Certificate	O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority	Matches Issuer
☐	Certificate	O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2	Matches Issuer
☐	Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer
☐	Certificate	O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA	Matches Issuer
☐	Certificate	O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5	Matches Issuer
☐	Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	O=DigiCert Inc, CN=DigiCert Global CA-1

Show all (decoded) | Show all (PEM file) | Delete | Select all | Unselect all

Expressway 트러스트 저장소

이 예에서는 인증서를 찾은 후 Subject(주체) 필드가 Issuer(발급자) 필드와 일치하지 않습니다. 이는 중간 CA 인증서임을 의미합니다. 루트 인증서 외에 이 인증서가 필요합니다. Subject(주체)가 Matches Issuer(발급자 일치)라고 하면 루트 인증 기관이며 신뢰할 수 있는 유일한 인증서임을 알 수 있습니다.

중간 인증서가 있는 경우 루트 인증서를 찾을 때까지 계속해야 합니다. 이렇게 하려면 중간 인증서의 Issuer(발급자) 필드를 확인합니다. 그런 다음 Subject(제목) 필드에서 동일한 값을 갖는 인증서를 찾습니다. 이 경우 O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA입니다. Subject(주체) 필드에서 이 값을 갖는 인증서를 찾습니다. 일치하는 인증서를 찾을 수 없는 경우 Subject of Matches Issuer(일치하는 발급자)의 Issuer(발급자) 필드에서 이 값을 찾습니다.

이 예에서는 Expressway-C 서버 인증서가 중간 CA O=DigiCert Inc, CN=DigiCert Global CA-1에 의해 서명되었으며 루트 CA O=DigiCert Inc. OU=www.digicert.com, CN=DigiCert Global Root CA에 의해 서명되었음을 볼 수 있습니다. 루트 CA를 찾았으므로 완료되었습니다. 그러나 다른 중간 CA를 찾은 경우 모든 중간 CA와 루트 CA를 식별할 때까지 이 프로세스를 계속해야 합니다.

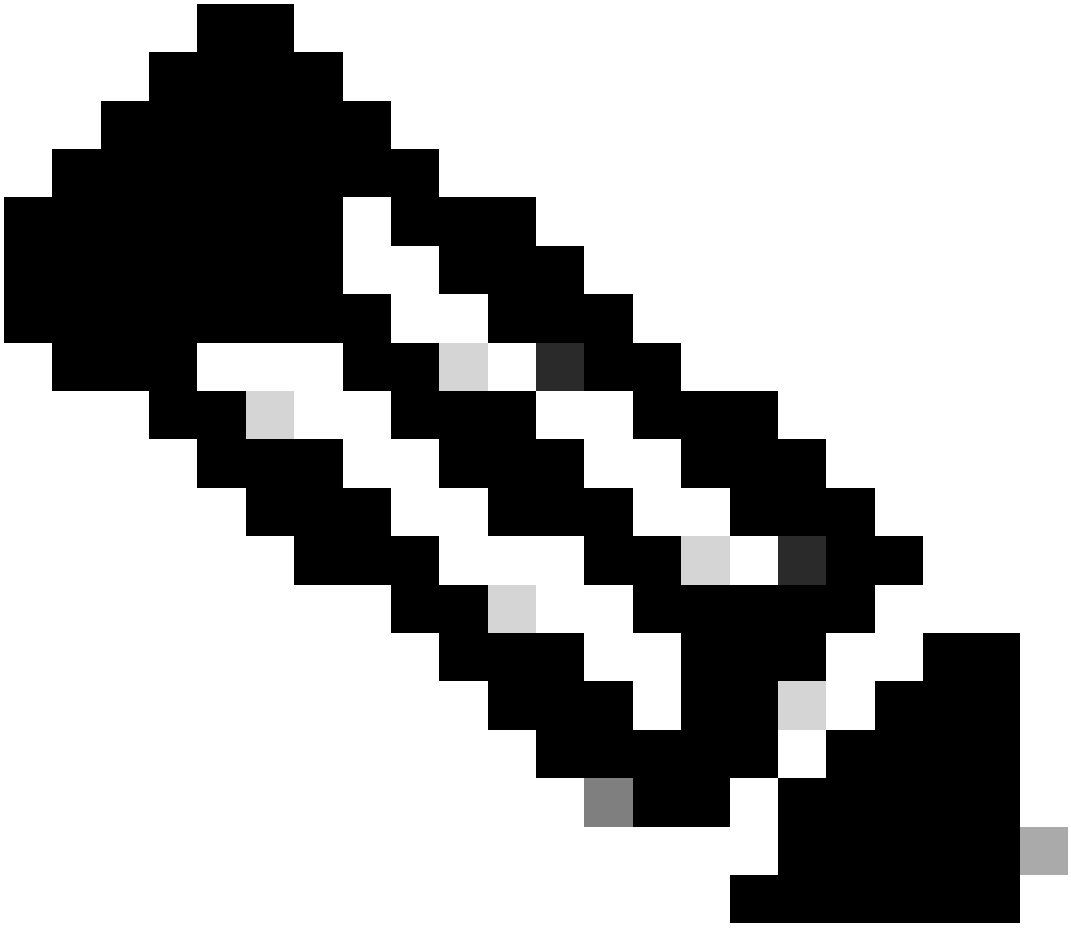
루트 및 중간 인증서 파일을 다운로드하려면 목록 아래의 Show all (PEM file) 버튼을 클릭합니다. 그러면 모든 루트 및 중간 인증서가 PEM 형식으로 표시됩니다. 중간 인증서 또는 루트 인증서 중 하나와 일치하는 인증서를 찾을 때까지 아래로 스크롤합니다. 이 예에서 가장 먼저 찾을 수 있는 것은 O=DigiCert Inc, CN=DigiCert Global Root CA입니다. 이 인증서를 파일에 복사하고 로컬에 저장합니다.

```
...
Epn3oOWC4zxe9Z2etiefC7IpJ5OCBRLbf1wbWsaY71k5h+3zvDyny67G7fyUIhz
ksLi4xaNmjICq44Y3ekQEe5+NauQrz4wlHrQMz2nZQ/1/I6eYs9HRCwBXbsdtTLS
R9I4LtD+gdwyah617jzV/OeBHRnDJELqYzmp
-----END CERTIFICATE-----

O=DigiCert Inc, CN=DigiCert Global Root CA
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
```

```
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr
hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls
YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----

O=The Go Daddy Group, Inc.
-----BEGIN CERTIFICATE-----
MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh
MB8GA1UEChMYVGhlIEdvIERhZGR5IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBE
...
```

루트 및 최종 중간 인증서 각각에 대해 (포함됨) -----BEGIN CERTIFICATE-----으로 시작하고 (포함됨) -----END CERTIFICATE-----으로 끝나는 모든 인증서를 복사합니다. 각 텍스트 파일을 별도의 텍스트 파일에 넣고 맨 아래에 1개의 빈 줄을 추가합니다(-----END CERTIFICATE----- 줄 뒤). .pem 확장명: root.pem, intermediate1.pem, intermediate2.pem, ...로 파일을 저장합니다. 각 루트/중간 인증서마다 별도의 파일이 필요합니다. 앞의 예에서 root.pem 파일에는 다음이 포함됩니다.

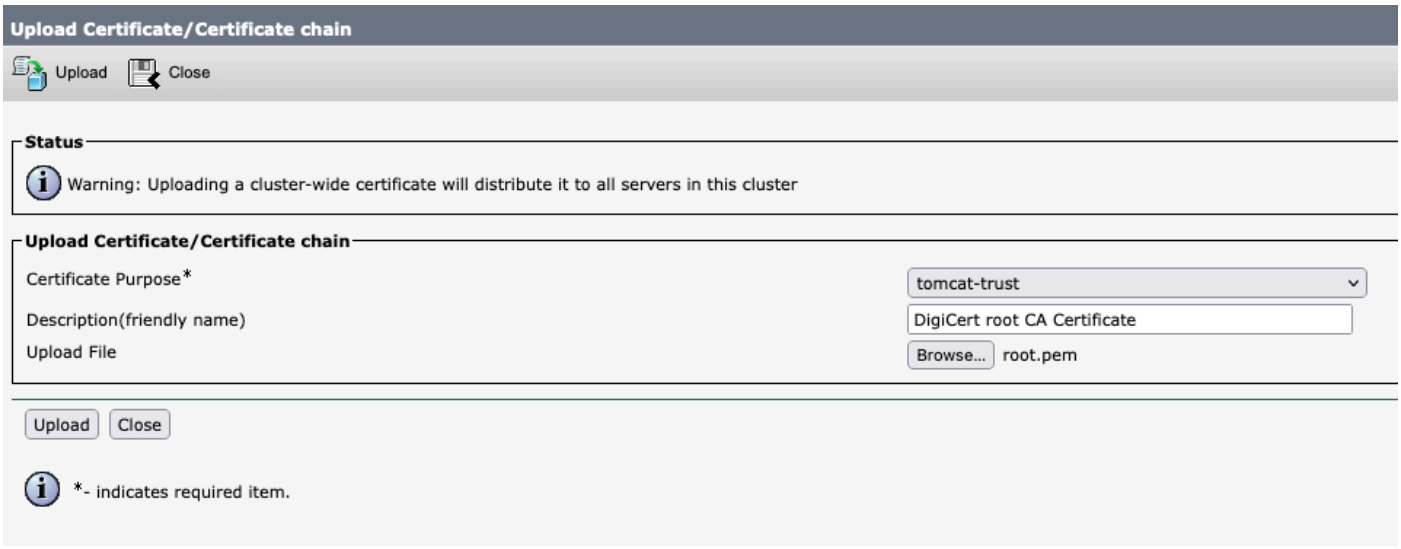
```
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr
hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls
YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----
```



참고: 맨 아래에 빈 줄이 하나만 있어야 합니다.

2단계. CUCM에 루트 및 중간 인증서 업로드(해당되는 경우)

- CUCM 게시자의 Cisco Unified OS Administration(Cisco Unified OS 관리) 페이지에 로그인합니다.
- Security(보안) > Certificate Management(인증서 관리)로 이동합니다.
- Upload Certificate/Certificate chain(인증서/인증서 체인 업로드) 버튼을 클릭합니다.
- 새 창에서 1단계의 루트 인증서 업로드를 시작합니다. tomcat-trust에 업로드합니다.



- Upload(업로드) 버튼을 클릭하고 Success: Certificate Uploaded(성공: 인증서 업로드됨)를 확인해야 합니다. Tomcat을 재시작하라는 메시지는 무시하십시오.
- 이제 CallManager-trust를 사용하여 인증서 용도로 동일한 루트 파일을 업로드합니다.
- Expressway-C에서 사용 중인 모든 중간 인증서에 대해 이전 단계(tomcat-trust 및 CallManager-trust로 업로드)를 반복합니다.

3단계. CUCM에서 필요한 서비스 다시 시작

CUCM 클러스터의 각 CUCM 노드에서 다음 서비스를 다시 시작해야 합니다.

- Cisco CallManager
- Cisco TFTP
- Cisco Tomcat

Cisco CallManager 및 Cisco TFTP는 CUCM의 Cisco Unified Serviceability 페이지에서 다시 시작할 수 있습니다.

- CUCM 게시자의 Cisco Unified serviceability(Cisco Unified 서비스 가용성) 페이지에 로그인합니다.
- Tools(툴) > Control Center - Feature Services(제어 센터 - 기능 서비스)로 이동합니다.
- 게시자를 서버로 선택합니다.
- Cisco CallManager 서비스를 선택하고 Restart(재시작) 버튼을 클릭합니다.
- Cisco CallManager 서비스를 다시 시작한 후 Cisco TFTP 서비스를 선택하고 Restart(재시작) 버튼을 클릭합니다.

Cisco Tomcat은 CLI에서만 재시작할 수 있습니다.

- CUCM 게시자에 대한 명령줄 연결을 엽니다.
- utils service restart Cisco Tomcat 명령을 사용합니다.

관련 정보

[기술 지원 및 문서 - Cisco Systems]

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.