

MRA(Collaboration Edge) 인증서 구성 및 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[공용 및 사설 CA\(Certificate Authority\) 비교](#)

[인증서 체인의 작동 방식](#)

[SSL 핸드셰이크 요약](#)

[구성](#)

[Expressway-C 및 Expressway-E Traversal Zone/Trust](#)

[CSR 생성 및 서명](#)

[Expressway-C와 Expressway-E가 서로 신뢰하도록 구성](#)

[Cisco Unified Communications Manager\(CUCM\)와 Expressway-C 간 보안 통신](#)

[개요](#)

[CUCM과 Expressway-C 간 트러스트 구성](#)

[자체 서명 인증서가 있는 CUCM 서버](#)

[Expressway-C 및 Expressway-E 클러스터 고려 사항](#)

[클러스터 인증서](#)

[신뢰할 수 있는 CA 목록](#)

[다음을 확인합니다.](#)

[현재 인증서 정보 확인](#)

[Wireshark에서 인증서 읽기/내보내기](#)

[문제 해결](#)

[Expressway에서 인증서를 신뢰할 수 있는지 테스트](#)

[Synergy Light Endpoints\(7800/8800 Series 폰\)](#)

[비디오 리소스](#)

[MRA 또는 클러스터형 Expressway에 대한 CSR 생성](#)

[Expressway에 InstallServer 인증서 설치](#)

[Expressway 간에 인증서 신뢰를 구성하는 방법](#)

소개

이 문서에서는 MRA(Mobile Remote Access) 구축과 관련된 인증서를 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

퍼블릭 및 프라이빗 CA(Certificate Authority)

Expressway-C 및 E 서버에는 인증서를 서명하는 여러 옵션이 있습니다. GoDaddy, Verisign 등의 공용 CA에서 CSR(Certificate Signing Request)을 서명하도록 선택하거나 자체 인증 기관을 사용하는 경우 내부에서 서명할 수 있습니다(OpenSSL로 자체 서명하거나 Microsoft Windows 서버와 같은 내부 엔터프라이즈 CA로 자체 서명할 수 있음). 이러한 방법에서 사용하는 CSR을 만들고 서명하는 방법에 대한 자세한 내용은 VCS([Video Communication Server](#)) [Certificate Creation Guide](#)를 [참조하십시오](#).

공용 CA에서 서명해야 하는 유일한 서버는 Expressway-E입니다. 이 서버는 클라이언트가 MRA를 통해 로그인할 때 인증서를 볼 수 있는 유일한 서버이므로 공용 CA를 사용하여 사용자가 인증서를 수동으로 승인할 필요가 없도록 합니다. Expressway-E는 내부 CA 서명 인증서를 사용하여 작업할 수 있지만 처음 사용자에게 신뢰할 수 없는 인증서를 수락하라는 메시지가 표시됩니다. 7800 및 8800 시리즈 전화기의 MRA 등록은 인증서 신뢰 목록을 수정할 수 없으므로 내부 인증서와 함께 작동하지 않습니다. 간소화를 위해 Expressway-C 및 Expressway-E 인증서 모두 동일한 CA에서 서명하는 것이 좋습니다. 그러나 두 서버에서 신뢰할 수 있는 CA 목록을 제대로 구성한 경우에는 이 작업이 필요하지 않습니다.

인증서 체인의 작동 방식

인증서는 서버의 인증서에 서명한 소스를 확인하는 데 사용되는 둘 이상의 체인으로 함께 연결됩니다. 체인에 클라이언트/서버 인증서, 중간 인증서(경우에 따라) 및 루트 인증서(인증서를 서명한 최고 레벨의 기관이므로 루트 CA라고도 함)의 세 가지 인증서 유형이 있습니다.

인증서에는 체인을 구성하는 두 개의 기본 필드(주체 및 발급자)가 포함되어 있습니다.

제목은 이 인증서가 나타내는 서버 또는 기관의 이름입니다. Expressway-C 또는 Expressway-E(또는 기타 UC(Unified Communications) 디바이스)의 경우 FQDN(Fully Qualified Domain Name)에서 생성됩니다.

발급자는 특정 인증서를 검증한 기관입니다. 누구나 인증서를 만든 서버(자체 서명 인증서라고도 함)를 비롯하여 인증서에 서명할 수 있으므로 서버와 클라이언트에는 인증된 것으로 신뢰하는 발급자 또는 CA 목록이 있습니다.

인증서 체인은 항상 자체 서명된 최상위 또는 루트 인증서로 끝납니다. 인증서 계층 구조를 이동하

는 동안 각 인증서는 주제와 관련하여 다른 발급자를 갖습니다. 결국 주체와 발급자가 일치하는 루트 CA를 만나게 됩니다. 이는 최상위 인증서이므로 클라이언트 또는 서버의 신뢰할 수 있는 CA 목록에서 신뢰해야 함을 나타냅니다.

SSL 핸드셰이크 요약

접근 영역의 경우 Expressway-C는 항상 클라이언트 역할을 하고 Expressway-E는 항상 서버입니다. 간소화된 교환은 다음과 같이 작동합니다.

Expressway-C Expressway-E

```
-----클라이언트 Hello----->
<-----서버 Hello-----
<----서버 인증서-----
<----인증서 요청--
-----클라이언트 인증서----->
```

Expressway-C는 항상 연결을 시작하므로 여기서 키는 교환에 있으며, 따라서 항상 클라이언트입니다. Expressway-E가 인증서를 보내는 첫 번째 방법입니다. Expressway-C에서 이 인증서의 유효성을 검사할 수 없는 경우 핸드셰이크를 해제하며 Expressway-E로 자신의 인증서를 보낼 수 없습니다.

또 하나 주의해야 할 점은 인증서의 TLS(Transport Layer Security) 웹 클라이언트 인증 및 TLS 웹 서버 인증 특성입니다. 이러한 특성은 CSR에 서명한 CA에서 결정되며(Windows CA를 사용하는 경우 선택한 템플릿에 의해 결정됨) 인증서가 클라이언트 또는 서버(또는 둘 다)의 역할에서 유효한지 나타냅니다. VCS 또는 Expressway의 경우 상황을 기반으로 할 수 있으며(접근 영역에서는 항상 동일함) 인증서에 클라이언트 및 서버 인증 특성이 모두 있어야 합니다.

Expressway-C 및 Expressway-E는 새 서버 인증서에 업로드할 때 둘 다 적용되지 않은 경우 오류를 표시합니다.

인증서에 이러한 특성이 있는지 확실하지 않은 경우 브라우저 또는 OS에서 인증서 세부 정보를 열고 Extended Key Usage(확장 키 사용) 섹션을 확인할 수 있습니다(이미지 참조). 형식은 다양할 수 있으며 인증서를 보는 방법에 따라 달라집니다.

예:

Certificate Hierarchy

ACTIVE DIRECTORY-CA

Certificate Fields

- Extended Key Usage
- Certificate Subject Alt Name
- Certificate Subject Key ID
- Certificate Authority Key Identifier
- CRL Distribution Points
- Authority Information Access
- Object Identifier (1 3 6 1 4 1 311 21 7)
- Object Identifier (1 3 6 1 4 1 311 21 10)

Field Value

Not Critical
TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)


Export...


구성

Expressway-C 및 Expressway-E Traversal Zone/Trust

CSR 생성 및 서명

앞에서 설명한 것처럼 Expressway-C 및 Expressway-E 인증서는 내부 또는 외부 CA에 의해 또는 OpenSSL에 의해 자체 서명되어야 합니다.

 참고: Expressway 서버에서 제공되는 임시 인증서는 지원되지 않으므로 사용할 수 없습니다. CA 서명 인증서가 있고 제목 줄이 구체적으로 정의되지 않은 경우 와일드카드 인증서를 사용

 하는 경우 지원되지 않습니다.


첫 번째 단계는 CSR을 생성하고 기본 설정 CA 유형으로 서명하도록 하는 것입니다. 이에 대한 프로세스는 [Certificate Creation Guide](#)에서 구체적으로 [설명합니다](#). CSR을 생성하는 동안 인증서에 포함해야 할 필수 SAN(주체 대체 이름)을 엄두에 두어야 합니다. 이는 인증서 가이드 및 모바일 원격 액세스 구축 가이드에도 나와 있습니다. 새로운 기능이 제공될 때 추가할 수 있는 가이드의 최신 버전을 확인합니다. 사용된 기능에 따라 포함해야 할 공통 SAN 목록:

고속도로 C

- 도메인 목록에 추가된 모든 도메인(내부 또는 외부)
- XMPP 페더레이션을 사용하는 경우 모든 persistent chat 노드 별칭
- 보안 디바이스 프로파일을 사용하는 경우 CUCM에서 디바이스 프로파일 이름을 보호합니다.

고속도로 E

- Expressway-C에 구성된 모든 도메인
- XMPP 페더레이션을 사용하는 경우 모든 persistent chat 노드 별칭
- XMPP 페더레이션에 대해 광고된 모든 도메인.

 참고: 외부 서비스 레코드(SRV) 조회에 사용되는 기본 도메인이 Expressway-E 인증서 (xxx.com 또는 collab-edge.xxx.com)에 SAN으로 포함되어 있지 않은 경우, Jabber 클라이언트는 여전히 최종 사용자가 첫 번째 연결에서 인증서를 수락해야 하며 TC 엔드포인트는 전혀 연결되지 않습니다.

Expressway-C와 Expressway-E가 서로 신뢰하도록 구성

Unified Communications 접근 영역이 연결을 설정하려면 Expressway-C와 Expressway-E가 서로의 인증서를 신뢰해야 합니다. 이 예에서는 Expressway-E 인증서가 이 계층 구조를 사용하는 공용 CA에 의해 서명되었다고 가정합니다.

인증서 3

발급자: GoDaddy 루트 CA

제목: GoDaddy Root CA

인증서 2

발급자: GoDaddy 루트 CA

제목: GoDaddy Intermediate Authority

인증서 1

발급자: GoDaddy 중간 기관

제목: Expressway-E.lab

Expressway-C는 트러스트 인증서 1을 사용하여 구성해야 합니다. 대부분의 경우 서버에 적용된 신뢰할 수 있는 인증서를 기반으로 가장 낮은 레벨의 서버 인증서만 전송합니다. 즉, Expressway-C에서 인증서 1을 신뢰하려면 인증서 2와 3을 모두 Expressway-C의 신뢰받는 CA 목록 (Maintenance(유지 관리) > Security(보안) > Trusted CA List(신뢰받는 CA 목록)에 업로드해야 합니다. Expressway-C가 Expressway-E 인증서를 받을 때 중간 인증서 2를 생략하면 신뢰할 수 있는 GoDaddy Root CA에 연결할 수 없으므로 거부됩니다.

인증서 3

발급자: GoDaddy 루트 CA

제목: GoDaddy Root CA

인증서 1

발급자: GoDaddy Intermediate Authority - 신뢰할 수 없음!

제목: Expressway-E.lab

또한 루트 없이 중간 인증서만 Expressway-C의 신뢰할 수 있는 CA 목록에 업로드하면 GoDaddy Intermediate Authority가 신뢰할 수 있는 것으로 표시되지만 상위 기관, 이 경우 신뢰할 수 없는 GoDaddy Root CA가 서명되므로 실패합니다.

인증서 2

발급자: GoDaddy 루트 CA - 신뢰할 수 없음!

제목: GoDaddy Intermediate Authority

인증서 1

발급자: GoDaddy 중간 기관

제목: Expressway-E.lab

모든 중간체와 루트가 신뢰할 수 있는 CA 목록에 추가되면 인증서를 검증할 수 있습니다.

인증서 3

발급자: GoDaddy 루트 CA - 자체 서명된 최상위 인증서가 신뢰되며 체인이 완료되었습니다!

제목: GoDaddy Root CA

인증서 2

발급자: GoDaddy 루트 CA

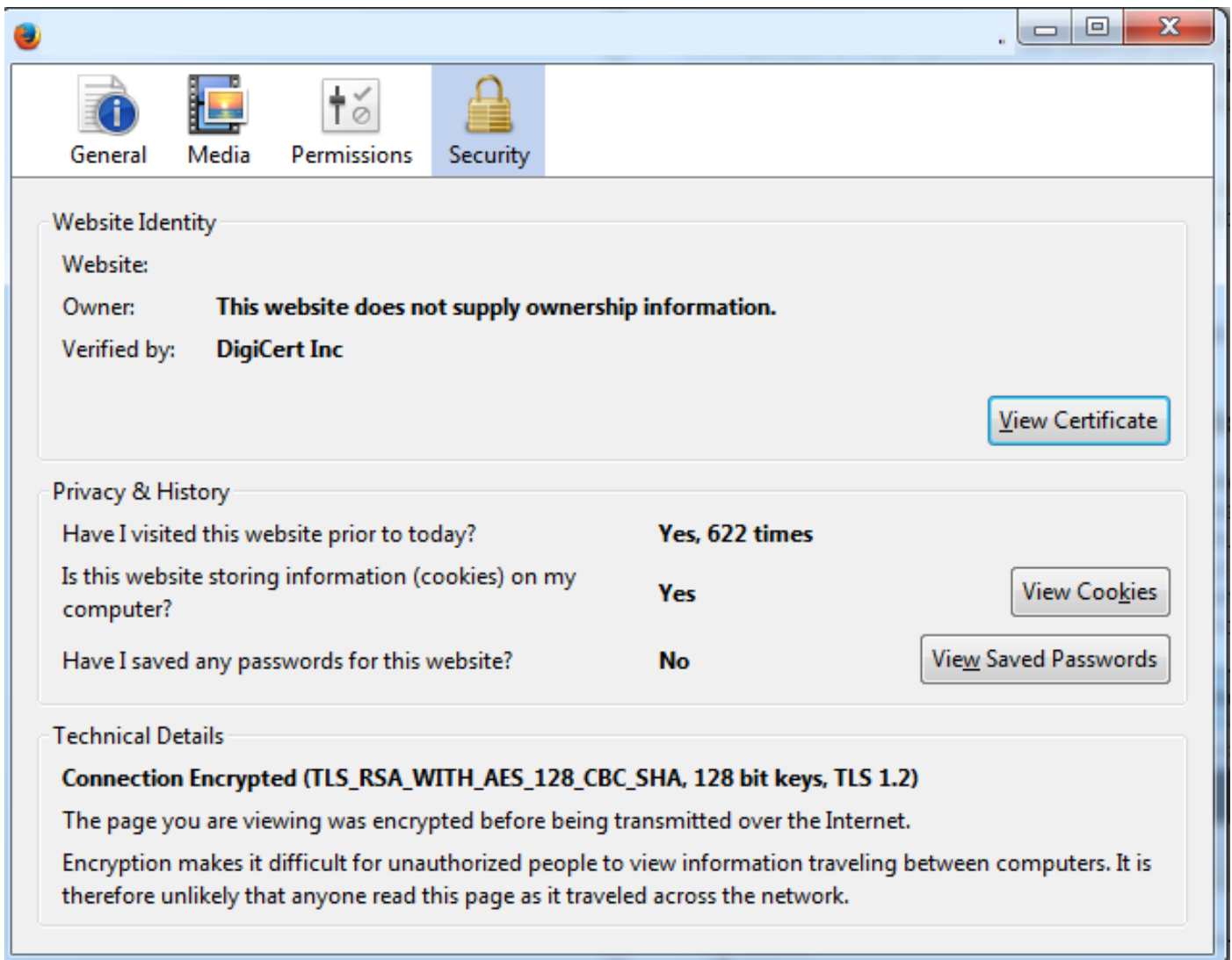
제목: GoDaddy Intermediate Authority

인증서 1.

발급자: GoDaddy 중간 기관

제목: Expressway-E.lab

인증서 체인이 무엇인지 확실하지 않은 경우 특정 Expressway의 웹 인터페이스에 로그인할 때 브라우저를 확인할 수 있습니다. 프로세스는 브라우저에 따라 조금씩 다르지만, Firefox에서는 주소 표시줄 맨 왼쪽에 있는 잠금 아이콘을 클릭할 수 있습니다. 그런 다음 팝업창에서 More Information(추가 정보) > View Certificate(인증서 보기) > Details(세부사항)를 클릭합니다. 브라우저가 전체 체인을 결합할 수 있는 경우 위에서 아래로 체인을 볼 수 있습니다. 최상위 인증서에 일치하는 주체 및 발급자가 없으면 체인이 완료되지 않은 것입니다. 원하는 인증서가 강조 표시된 상태로 내보내기를 클릭하면 체인의 각 인증서를 직접 내보낼 수도 있습니다. 이는 CA 신뢰 목록에 올바른 인증서를 업로드했다고 100% 확신할 수 없는 경우에 유용합니다.



General Details

This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN)

Organization (O)

Organizational Unit (OU)

Serial Number

Issued By

Common Name (CN) DigiCert SHA2 High Assurance Server CA

Organization (O) DigiCert Inc

Organizational Unit (OU)

Period of Validity

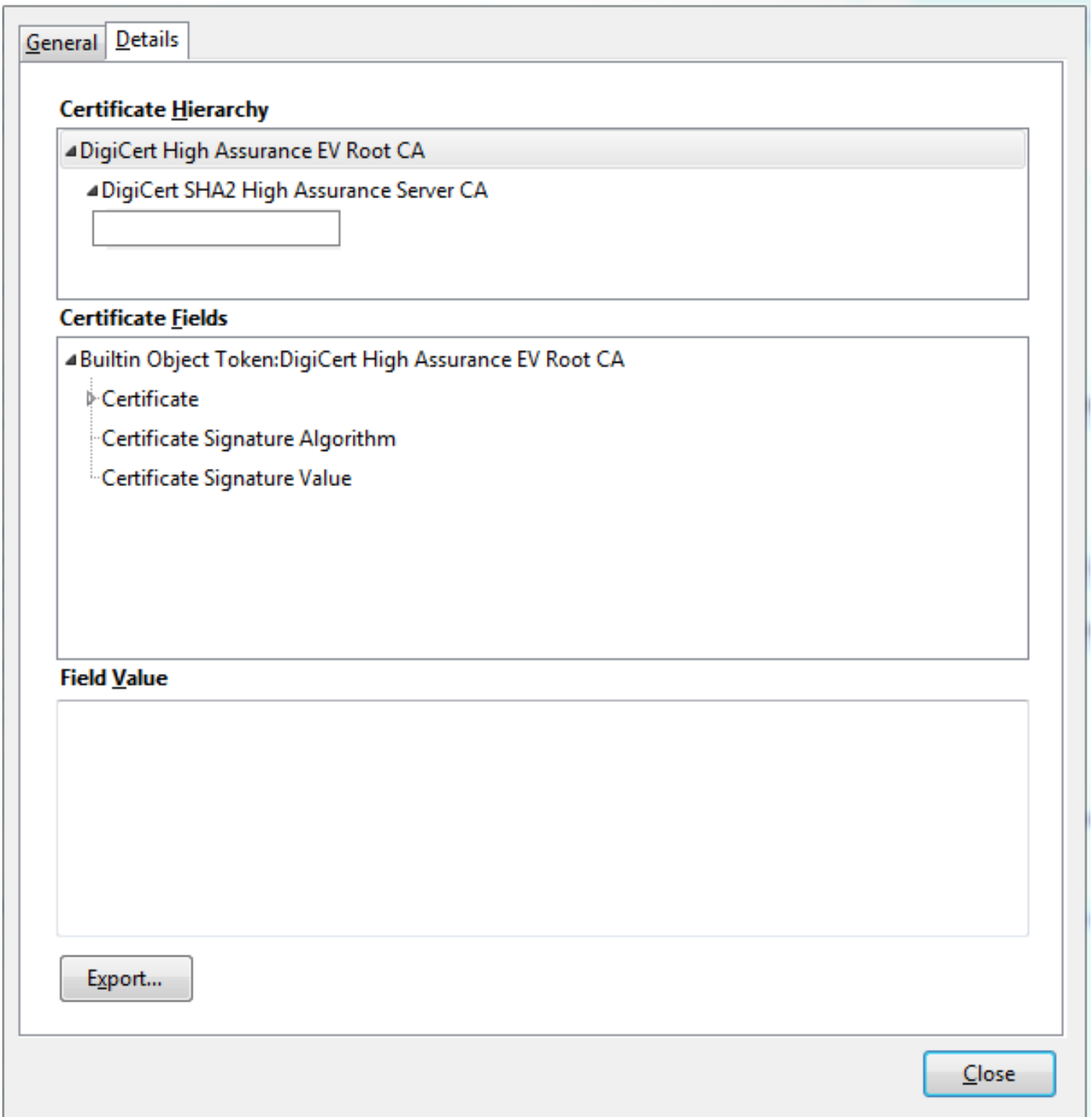
Begins On 3/25/2015

Expires On 4/12/2017

FingerprintsSHA-256 Fingerprint 3B:37:23:04:BE:92:0C:FF:2D:48:0B:52:07:5C:D5:08:
F3:75:F6:0D:43:98:8B:73:22:A4:ED:A8:E6:D7:2A:23

SHA1 Fingerprint CE:7B:79:41:94:9E:07:48:F3:A4:B4:07:03:76:D3:52:12:5D:A9:42

Close



이제 Expressway-C가 Expressway-E의 인증서를 신뢰하므로 반대 방향으로 작동하는지 확인합니다. Expressway-C 인증서가 Expressway-E에 서명한 CA에 의해 서명된 경우 프로세스는 간단합니다. C에 이미 업로드한 것과 동일한 인증서를 Expressway-E의 신뢰할 수 있는 CA 목록에 업로드합니다. C가 다른 CA에 의해 서명된 경우 이미지에 표시된 것과 동일한 프로세스를 사용해야 하지만 대신 서명된 Expressway-C 인증서의 체인을 사용해야 합니다.

CUCM(Cisco Unified Communications Manager)과 Expressway-C 간 보안 통신

개요

Expressway-C와 Expressway-E 간의 접근 영역과는 달리 Expressway-C와 CUCM 간에는 보안 신호 처리가 필요하지 않습니다. 내부 보안 정책에서 허용하지 않는 경우가 아니면 항상 MRA가 CUCM에서 비보안 장치 프로파일과 작동하도록 먼저 구성한 다음 이 단계를 계속하기 전에 나머지 배포가 올바른지 확인해야 합니다.

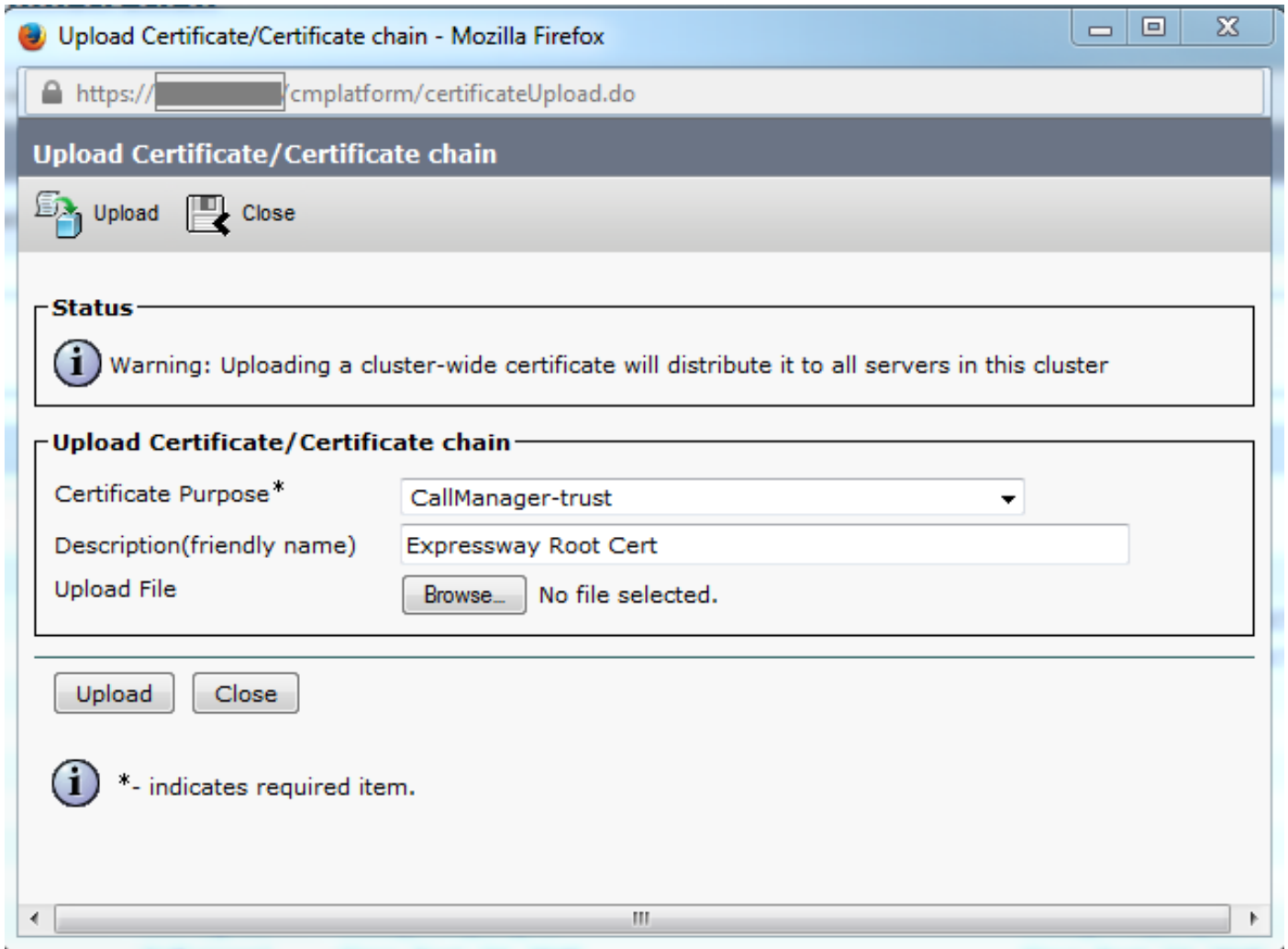
CUCM과 Expressway-C 간에는 TLS Verify(TLS 확인) 및 Secure Device Registrations(보안 디바이스 등록)라는 두 가지 주요 보안 기능이 있습니다. SSL 핸드셰이크의 CUCM 측과 다른 두 인증서를 사용하기 때문에 이 두 가지 사이에는 중요한 차이점이 있습니다.

TLS Verify - tomcat 인증서

보안 SIP 등록 - CallManager 인증서


CUCM과 Expressway-C 간 트러스트 구성

이 경우의 개념은 Expressway-C와 Expressway-E 사이와 정확히 동일합니다. CUCM은 먼저 Expressway-C의 서버 인증서를 신뢰해야 합니다. 즉, CUCM에서 Expressway-C의 중간 및 루트 인증서를 TLS 확인 기능의 tomcat-trust 인증서로 업로드하고 보안 디바이스 등록을 위한 CallManager-trust로 업로드해야 합니다. 이 작업을 수행하려면 CUCM 웹 GUI 오른쪽 상단에서 Cisco Unified OS Administration(Cisco Unified OS 관리)으로 이동한 다음 Security(보안) > Certificate Management(인증서 관리)로 이동합니다. 여기에서 Upload Certificate/Certificate Chain(인증서/인증서 체인 업로드)을 클릭하고 올바른 신뢰 형식을 선택하거나 Find(찾기)를 클릭하여 현재 업로드된 인증서 목록을 확인할 수 있습니다.



Expressway-C가 CUCM 인증서에 서명한 CA를 신뢰하는지 확인해야 합니다. 이를 위해 신뢰할 수 있는 CA 목록에 추가할 수 있습니다. 거의 모든 경우 CUCM 인증서를 CA로 서명한 경우 tomcat 및 CallManager 인증서는 동일한 CA에서 서명해야 합니다. 인증서가 다른 경우 TLS Verify 및 Secure Registration을 사용하는 경우 두 인증서를 모두 신뢰해야 합니다.

보안 SIP 등록을 위해서는 디바이스에 적용된 CUCM의 보안 디바이스 프로파일 이름이 Expressway-C 인증서에 SAN으로 나열되어 있는지 확인해야 합니다. 보안 레지스터 메시지가 포함되지 않은 경우 CUCM에서 403으로 TLS 실패를 나타내는 오류가 발생합니다.

 **참고:** 보안 SIP 등록을 위해 CUCM과 Expressway-C 간에 SSL 핸드셰이크가 발생하면 두 번의 핸드셰이크가 발생합니다. 먼저 Expressway-C가 클라이언트 역할을 하고 CUCM과의 연결을 시작합니다. 연결이 성공적으로 완료되면 CUCM은 응답할 클라이언트로서 다른 핸드셰이크를 시작합니다. 즉, Expressway-C와 마찬가지로 CUCM의 CallManager 인증서에는 TLS 웹 클라이언트 및 TLS 웹 서버 인증 특성이 모두 적용되어야 합니다. 차이점은 CUCM에서는 이러한 인증서를 둘 다 업로드하지 않고 업로드할 수 있으며, CUCM에 서버 인증 특성만 있는 경우 내부 보안 등록이 정상적으로 작동한다는 것입니다. 목록에서 CallManager 인증서를 찾아 선택하면 CUCM에서 이를 확인할 수 있습니다. 여기서 Extension(확장) 섹션 아래에서 사용 OID를 확인할 수 있습니다. 클라이언트 인증에는 1.3.6.1.5.5.7.3.2가 표시되고 서버 인증에는 1.3.6.1.5.5.7.3.1이 표시됩니다. 이 창에서 인증서를 다운로드할 수도 있습니다.

Certificate Details(CA-signed) - Mozilla Firefox

https://[redacted]/cmplatform/certificateEdit.do?cert=/usr/local/cm/.security/CallManager/certs/CallManager.per

Certificate Details for cucm10-lab-pub.tkratzke.local, CallManager

Regenerate
 Generate CSR
 Download .PEM File
 Download .DER File

Status

Status: Ready

Certificate Settings

Locally Uploaded	01/04/15
File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Certificate Signed by tkratzke-ACTIVEDIRECTORY-CA

Certificate File Data

```

Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100c3f0061dafbffa97cd781c9627134664cae9f55d5d92871b60ce17ddf78972963a4
1db705c43c97046df73897748e2a2459c96f7cd3cc849c71055b27ffd30dc6d4ebc727beb7a96e98ab78
01d25eb0e354086e318df242d4039004f2c569308c875697ecdf2b9040d4aa22da5b7a82f667abbd2342
0fe820dd157a648ee4c611ca8612cef49f35dd8e01677b18edca260c6aa3920da979e4adadb7ed4c776e
e1c9a28d9eaf90648cafaf757a7050ec0fc383eccbb227d0947e3265737f640e7db4d280e477689ba395
60a6a39db010fadb4e2da05beea5c8f47357726d90e56c1415c499e8d09ab36357c1223f1bae52baa82
32ba70485bd745407b354bd09d0203010001
Extensions: 9 present
[
  Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
  Critical: false
  Usage oids: 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1,
]
  
```

참고: 클러스터의 게시자에 적용된 트러스트 인증서는 가입자에게 복제해야 합니다. 새 컨피그레이션에서 별도로 로그인하여 확인하는 것이 좋습니다.

참고: Expressway-C에서 CUCM의 인증서를 올바르게 검증하려면 IP 주소가 아니라 FQDN을 사용하여 Expressway-C에 CUCM 서버를 추가해야 합니다. IP 주소가 작동할 수 있는 유일한 방법은 각 CUCM 노드의 IP를 인증서에 SAN으로 추가하는 것입니다. 이는 거의 수행되지 않습니다.

자체 서명 인증서가 있는 CUCM 서버

기본적으로 CUCM 서버에는 자체 서명 인증서가 함께 제공됩니다. 이러한 설정이 있는 경우 TLS Verify(TLS 확인) 및 Secure Device Registrations(디바이스 등록 보안)을 동시에 사용할 수 없습니다. 두 기능 중 하나를 단독으로 사용할 수 있지만 인증서가 자체 서명되어 있으므로 자체 서명된 Tomcat 및 자체 서명된 CallManager 인증서를 모두 Expressway-C의 신뢰할 수 있는 CA 목록에 업로드해야 합니다. Expressway-C는 인증서를 검증하기 위해 신뢰 목록을 검색할 때 일치하는 제목이 있는 인증서를 찾으려 합니다. 따라서 신뢰 목록에서 더 높은 tomcat 또는 CallManager 중 어떤 것이든 해당 기능이 작동합니다. 아랫쪽은 마치 없는 것처럼 실패할 것이다. 이를 위한 해결 방법은 CA(공용 또는 사설)로 CUCM 인증서를 서명하고 해당 CA만 신뢰하는 것입니다.

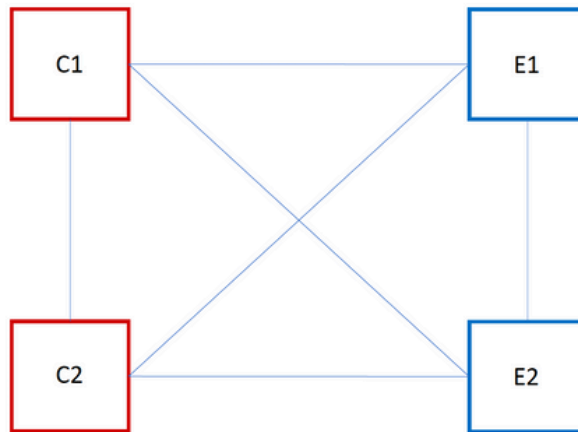
Expressway-C 및 Expressway-E 클러스터 고려 사항

클러스터 인증서

이중화를 위해 Expressway-C 또는 Expressway-E 서버의 클러스터가 있는 경우 각 서버에 대해 별도의 CSR을 생성하고 CA에서 서명하도록 하는 것이 좋습니다. 이전 시나리오에서 각 피어 인증서의 CN(Common Name)은 이미지와 같이 동일한 클러스터 FQDN(Fully Qualified Domain Name)이고 SAN은 클러스터 FQDN 및 각 피어 FQDN입니다.

Expressway Cluster Certificates MRA

CN: FQDN of CLUSTER
SAN: FQDN C1 AND CLUSTER FQDN
SAN: PHONE SECURITY PROFILE
(FQDN FORMAT)(If Configured on CUCM)



CN: FQDN of CLUSTER
SAN: FQDN E1 AND CLUSTER FQDN
SAN: EXTERNAL DOMAIN or
COLLAB-EDGE.EXAMPLE.COM

CN: FQDN of CLUSTER
SAN: FQDN C2 AND CLUSTER FQDN
SAN: PHONE SECURITY PROFILE
(FQDN FORMAT)(If Configured on CUCM)

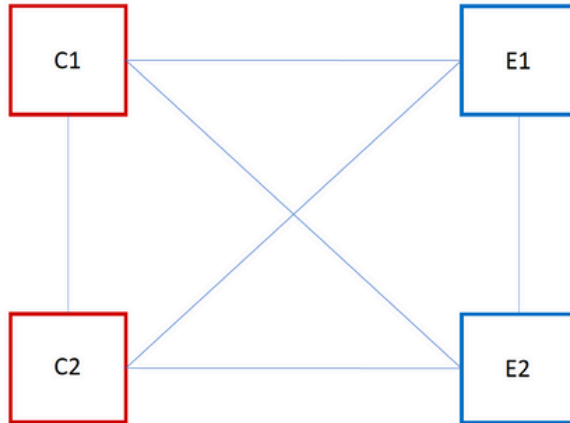
CN: FQDN of CLUSTER
SAN: FQDN E2 AND CLUSTER FQDN
SAN: EXTERNAL DOMAIN or
COLLAB-EDGE.EXAMPLE.COM

클러스터 FQDN을 CN으로 사용하고 SAN의 각 피어 FQDN과 클러스터 FQDN을 사용하여 클러스터의 모든 노드에 동일한 인증서를 사용할 수 있으므로 공용 CA에서 서명한 여러 인증서의 비용을 피할 수 있습니다.

Expressway Cluster Certificates

MRA

CN: FQDN of CLUSTER
SAN: FQDN C1, FQDN C2 AND CLUSTER FQDN
SAN: PHONE SECURITY PROFILE
(FQDN FORMAT)(If Configured on CUCM)



CN: FQDN of CLUSTER
SAN: FQDN E1, FQDN E2 AND CLUSTER FQDN
SAN: EXTERNAL DOMAIN or
COLLAB-EDGE.EXAMPLE.COM

CN: FQDN of CLUSTER
SAN: FQDN C2, FQDN C1 AND CLUSTER FQDN
SAN: PHONE SECURITY PROFILE
(FQDN FORMAT)(If Configured on CUCM)

CN: FQDN of CLUSTER
SAN: FQDN E2, FQDN E1 AND CLUSTER FQDN
SAN: EXTERNAL DOMAIN or
COLLAB-EDGE.EXAMPLE.COM

참고: UCM에서 Secure Phone Security Profiles를 사용하는 경우에만 Cs 인증서의 Phone Security Profile 이름이 필요합니다. 외부 도메인 또는 collab-edge.example.com(여기서 example.com은 사용자 도메인임)은 MRA를 통한 IP Phone 및 TC 엔드포인트 등록에만 필요합니다. MRA를 통한 Jabber 등록의 경우 선택 사항입니다. Jabber가 없을 경우, jabber가 MRA를 통해 로그인할 때 인증서를 수락하라는 프롬프트가 표시됩니다.

절대적으로 필요한 경우 다음 프로세스로 이 작업을 수행하거나 OpenSSL을 사용하여 개인 키와 CSR을 모두 수동으로 생성할 수 있습니다.

1단계. 클러스터의 기본 노드에서 CSR을 생성하고 클러스터 별칭을 CN으로 나열하도록 구성합니다. 클러스터의 모든 피어를 다른 필수 SAN과 함께 대체 이름으로 추가합니다.

2단계. 이 CSR에 서명하고 기본 피어에 업로드합니다.

3단계. 기본 키를 root로 로그인하고 /Tandberg/persistent/certs에 있는 개인 키를 다운로드합니다.

4단계. 서명된 인증서와 일치하는 개인 키를 클러스터의 다른 피어에 업로드합니다.

참고: 다음과 같은 이유로 권장되지 않습니다.

- 모든 피어가 동일한 개인 키를 사용하므로 보안 위험이 있습니다. 어떤 공격이든 감염되면 공격자는 모든 서버에서 트래픽을 해독할 수 있습니다.
- 인증서를 변경해야 하는 경우, 간단한 CSR 생성 및 서명 대신 이 전체 프로세스를 다시 따라야 합니다.

신뢰할 수 있는 CA 목록

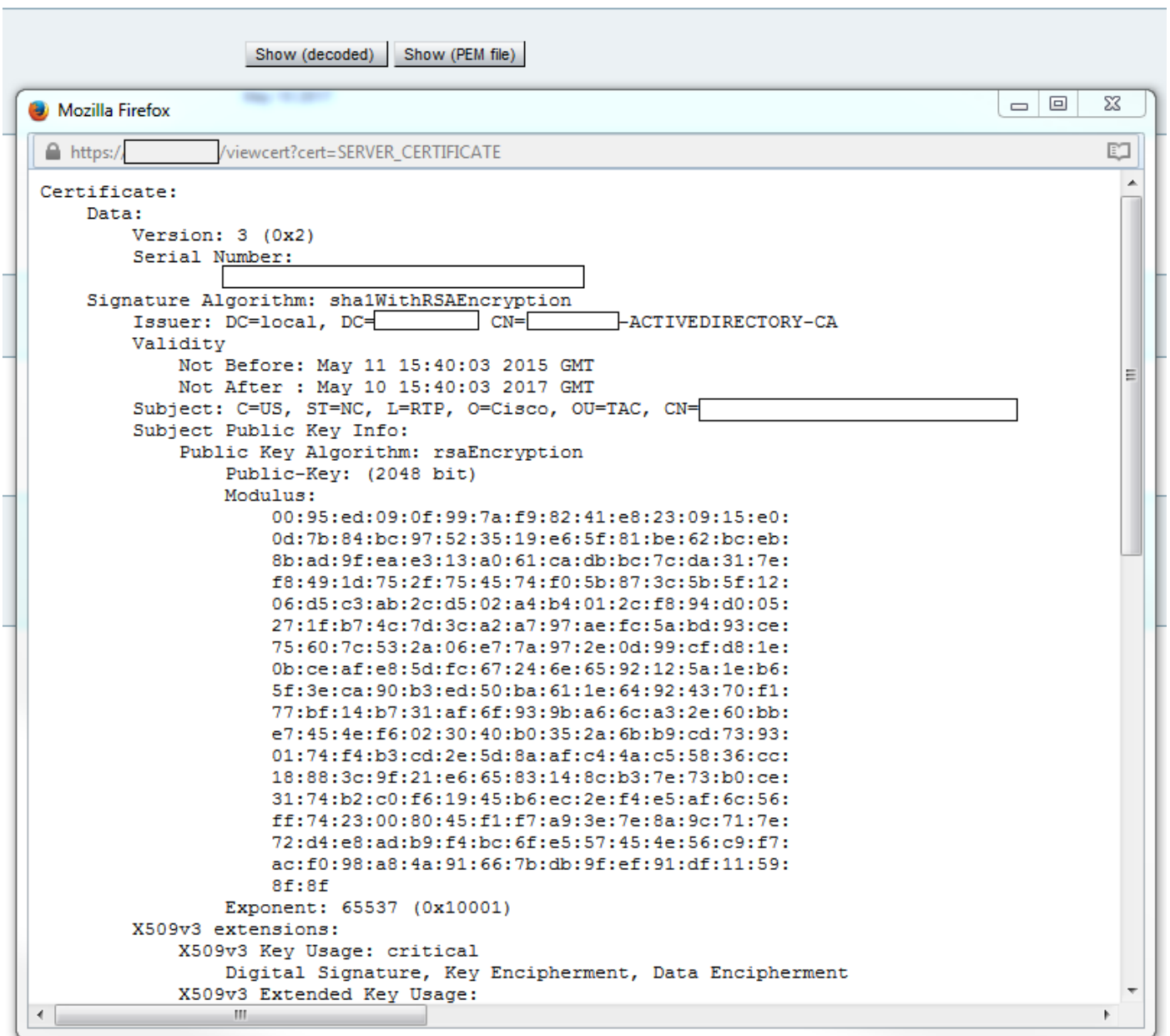
클러스터의 CUCM 가입자와 달리 신뢰할 수 있는 CA 목록은 Expressway 또는 VCS 클러스터의 한 피어에서 다른 피어로 복제되지 않습니다. 즉, 클러스터가 있는 경우 신뢰할 수 있는 인증서를 각 피어의 CA 목록에 수동으로 업로드해야 합니다.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

현재 인증서 정보 확인

기존 인증서에 대한 정보를 확인할 수 있는 방법은 여러 가지가 있습니다. 첫 번째 옵션은 웹 브라우저를 통한 것입니다. 체인의 특정 인증서를 내보내는 데 사용할 수도 있는 이전 섹션에 설명된 방법을 사용합니다. SAN 또는 Expressway 서버 인증서에 추가된 기타 특성을 확인해야 하는 경우 웹 GUI(그래픽 사용자 인터페이스)를 통해 직접 확인하고 Maintenance(유지 관리) > Security Certificates(보안 인증서) > Server Certificate(서버 인증서)로 이동한 다음 Show Decoded(디코딩된 표시)를 클릭합니다.



여기에서 인증서를 다운로드할 필요 없이 인증서의 모든 세부 사항을 볼 수 있습니다. 연결된 서명

된 인증서가 아직 업로드되지 않은 경우 활성 CSR에 대해서도 동일한 작업을 수행할 수 있습니다.

Wireshark에서 인증서 읽기/내보내기

인증서 교환을 포함하는 SSL 핸드셰이크의 Wireshark 캡처가 있는 경우, Wireshark는 실제로 인증서를 디코딩할 수 있으며, 실제로 체인의 모든 인증서를 내보낼 수 있습니다(전체 체인이 교환되는 경우). 인증서 교환의 특정 포트(일반적으로 접근 영역의 경우 7001)에 대한 패킷 캡처를 필터링합니다. 그런 다음 SSL 핸드셰이크와 함께 클라이언트 및 서버 hello 패킷이 표시되지 않으면 TCP 스트림의 패킷 중 하나를 마우스 오른쪽 버튼으로 클릭하고 decode as를 선택합니다. 여기서 SSL을 선택하고 apply를 클릭합니다. 이제 올바른 트래픽을 캡처한 경우 인증서 교환을 확인해야 합니다. 페이로드에 인증서가 포함된 올바른 서버에서 패킷을 찾습니다. 아래 창에서 SSL 섹션을 확장하여 그림과 같이 인증서 목록을 확인합니다.

Filter: tcp.stream eq 19

No.	Time	Source	Destination	Protocol	Length	Info
1803	2015-06-03 18:01:07.522714			TCP	74	25018→7001 [SYN] S
1806	2015-06-03 18:01:07.522835			TCP	74	7001→25018 [SYN, A
1807	2015-06-03 18:01:07.522855			TCP	66	25018→7001 [ACK] S
1808	2015-06-03 18:01:07.523594			TLSv1.2	266	Client Hello
1809	2015-06-03 18:01:07.523846			TCP	66	7001→25018 [ACK] S
1811	2015-06-03 18:01:07.538935			TLSv1.2	1514	Server Hello
1812	2015-06-03 18:01:07.538970			TCP	66	25018→7001 [ACK] S
1813	2015-06-03 18:01:07.539008			TLSv1.2	1514	Certificate

Frame 1813: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

- Ethernet II, Src: Vmware_a1:14:46 (), Dst: Vmware_a1:1e:e1 ()
- Internet Protocol Version 4, Src:
- Transmission Control Protocol, Src Port: 7001 (7001),
- [2 Reassembled TCP segments (2541 bytes): #1811(1390), #1813(1151)]
- Secure Sockets Layer
 - TLSv1.2 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 2536
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 2532
 - Certificates Length: 2529
 - Certificates (2529 bytes)
 - Certificate Length: 1612
 - Certificate (id-at-commonName=, id-at-organizationalUnitName=, id-at-organizationalName=)
 - Certificate Length: 911
 - Certificate (id-at-commonName= -ACTIVEDIRECTORY-CA, dc=, dc=)

여기에서 인증서를 확장하여 모든 세부 정보를 볼 수 있습니다. 인증서를 내보내려면 체인의 원하는 인증서를 마우스 오른쪽 버튼으로 클릭하고(여러 개 있는 경우) Export Selected Packet Bytes(선택한 패킷 바이트 내보내기)를 선택합니다. 인증서의 이름을 입력하고 저장을 클릭합니다. 이제 Windows 인증서 뷰어에서 인증서를 열거나(확장자가 .cer인 경우) 다른 모든 툴에 업로드하여 분석할 수 있어야 합니다.

문제 해결

이 섹션에서는 컨피그레이션 트러블슈팅에 사용할 수 있는 정보를 제공합니다.

Expressway에서 인증서를 신뢰할 수 있는지 테스트

인증서 체인을 수동으로 확인하고 모든 멤버가 Expressway의 신뢰할 수 있는 CA 목록에 포함되어 있는지 확인하는 것이 가장 좋은 방법이지만, Expressway가 웹 GUI의 Maintenance > Security

Certificates(유지 관리> 보안 인증서)에서 클라이언트 인증서 테스트의 도움을 받아 특정 클라이언트의 인증서를 신뢰하는지 빠르게 확인할 수 있습니다. 모든 기본 설정을 동일하게 유지합니다. 드롭다운에서 Upload Test File (pem format)(테스트 파일 업로드(pem 형식))을 선택하고 확인할 클라이언트 인증서를 선택합니다. 인증서를 신뢰할 수 없는 경우 이미지에 표시된 것처럼 거부된 이유를 설명하는 오류가 발생합니다. 표시되는 오류는 참조용으로 업로드된 인증서의 디코딩된 정보입니다.

Client certificate testing

Client certificate

This tests whether a client certificate is valid with the selected authentication pattern.

Certificate source: Uploaded test file (PEM format) ⓘ

Select the file you want to test: Browse... No file selected. ⓘ

Currently uploaded test file: pm-vcsc01.cer

Certificate-based authentication pattern

This section applies only if your certificate contains a username. It allows you to specify combinations of the nominated username format to the nominated authentication pattern.

Regex to match against certificate: `/Subject: *CN=(?<captureCommonName>[^\s,\\])`

Username format: `#captureCommonName#`

Make these settings permanent

Check certificate

Certificate test results

Valid certificate: Invalid: The client certificate is not signed by a CA in the trusted CA list.

Expressway에서 인증서 CRL을 가져올 수 없지만 Expressway에서 CRL 검사를 사용하지 않는다는 오류가 발생하는 경우, 이는 인증서를 신뢰할 수 있으며 다른 모든 확인 검사를 통과했음을 의미합니다.

Client certificate testing

Client certificate

This tests whether a client certificate is valid when checked against the Expressway-E certificate authority.

Certificate source: Uploaded test file (PEM format) ⓘ

Select the file you want to test: Browse... No file selected. ⓘ

Currently uploaded test file: vcs.cer

Certificate-based authentication pattern

This section applies only if your certificate contains authentication credentials. It allows you to specify a regular expression to match against the certificate's subject field and a username format to use for authentication.

Regex to match against certificate:

Username format:

Make these settings permanent


Check certificate


Certificate test results


Valid certificate: Invalid: unable to get certificate CRL, please ensure that you have uploaded a CRL for the CA that signed this client certificate


Synergy Light Endpoints(7800/8800 Series 폰)

이러한 새 디바이스에는 잘 알려진 공용 CA를 많이 포함하는 인증서 신뢰 목록이 미리 채워져 있습니다. 이 신뢰 목록은 수정할 수 없습니다. 즉, Expressway-E 인증서는 이러한 디바이스에서 작동하려면 이러한 일치하는 공용 CA 중 하나에서 서명해야 합니다. 내부 CA 또는 다른 공용 CA에서 서명한 경우 연결이 실패합니다. Jabber 클라이언트에 있는 것처럼 사용자가 인증서를 수동으로 수락하는 옵션은 없습니다.

 참고: 일부 구축에서는 Expressway-E가 내부 CA를 사용하는 경우에도 7800/8800 Series Phone에 포함된 목록의 CA와 함께 Citrix NetScaler와 같은 디바이스를 사용하여 MRA를 통해 등록할 수 있는 것으로 나타났습니다. SSL 인증이 작동하려면 NetScaler 루트 CA를 Expressway-E에 업로드하고 내부 루트 CA를 Netscaler에 업로드해야 합니다. 이는 효과가 있는 것으로 입증되었으며 최선의 지원입니다.

 참고: 신뢰할 수 있는 CA 목록에 모든 올바른 인증서가 있는 것으로 나타나지만 여전히 거부된 경우, 동일한 주체를 가진 목록 위에 올바른 인증서와 충돌할 수 있는 다른 인증서가 없는지 확인하십시오. 다른 모든 기능이 실패하면 항상 브라우저 또는 Wireshark에서 직접 체인을 내보내고 모든 인증서를 반대편 서버 CA 목록에 업로드할 수 있습니다. 이렇게 하면 신뢰할 수 있는 인증서가 됩니다.

 참고: Traversal Zone(접근 영역) 문제를 해결할 때, 간혹 관련 인증서로 나타날 수 있지만 실제로는 소프트웨어쪽에 있는 문제입니다. 통과에 사용되는 계정 사용자 이름 및 비밀번호가 올바른지 확인합니다.

 참고: VCS 또는 Expressway는 인증서의 SAN 필드에서 999자 이상을 지원하지 않습니다. 이 제한을 초과한 모든 SAN(대체 이름이 많이 필요함)은 마치 없는 것처럼 무시됩니다.

비디오 리소스

이 섹션에서는 모든 인증서 컨피그레이션 프로세스를 안내하는 비디오 정보를 제공합니다.

[MRA 또는 클러스터형 Expressway에 대한 CSR 생성](#)

[Expressway에 서버 인증서 설치](#)

[Expressway 간에 인증서 신뢰를 구성하는 방법](#)

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.