

配置协作边缘 (MRA) 证书并进行故障排除

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[公共证书颁发机构与专用证书颁发机构\(CA\)](#)

[证书链的工作原理](#)

[SSL 握手摘要](#)

[配置](#)

[Expressway C 和 Expressway E 遍历区域/信任](#)

[生成并签署CSR](#)

[将Expressway-C和Expressway-E配置为相互信任](#)

[思科统一通信管理器 \(CUCM\) 和 Expressway C 之间的安全通信](#)

[概述](#)

[配置CUCM和Expressway-C之间的信任](#)

[具有自签名证书的CUCM服务器](#)

[Expressway C 和 Expressway E 集群注意事项](#)

[集群证书](#)

[受信任的 CA 列表](#)

[验证](#)

[检查当前证书信息](#)

[在Wireshark中读取/导出证书](#)

[故障排除](#)

[测试以了解Expressway上的证书是否受信任](#)

[Synergy Light 终端 \(7800/8800 系列电话 \)](#)

[视频资源](#)

[为MRA或群集Expressway生成CSR](#)

[Expressway的InstallServer证书](#)

[如何在Expressway之间配置证书信任](#)

简介

本文档介绍有关移动远程访问(MRA)部署的证书。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

公有与私有证书授权 (CA)

在 Expressway C 和 Expressway E 服务器上签署证书时，有多个选项供您选择。您可以选择由公共CA(如GoDaddy、Verisign等)签署证书签名请求(CSR)，或者如果您使用自己的证书颁发机构(可以使用OpenSSL自签名或内部企业CA(如Microsoft Windows服务器)，则可以在内部签署该请求。有关如何创建和签署上述任何方法使用的CSR的详细信息，请参阅[视频通信服务器\(VCS\)证书创建指南](#)。

实际上，只有 Expressway E 服务器才需要由公共 CA 签署。这是客户端通过MRA登录时看到证书的唯一服务器，因此，请使用公共CA以确保用户不必手动接受证书。Expressway-E可以与内部CA签名证书配合使用，但系统会提示首次用户接受不受信任的证书。7800和8800系列电话的MRA注册不适用于内部证书，因为无法修改其证书信任列表。为简单起见，建议您的Expressway-C和Expressway-E证书都由同一CA签名；但是，只要您在两个服务器上正确配置了受信任CA列表，则不需要此要求。

证书链的工作原理

证书在两个或多个证书链中链接在一起，用于验证签署服务器证书的来源。链中有三种类型的证书：客户端/服务器证书、中间证书（某些情况下）和根证书（也称为根CA，因为这是签署证书的最高级别机构）。

证书包含两个构建链的主要字段：主题和颁发者。

主体是证书代表的服务器或机构的名称。对于Expressway-C或Expressway-E(或其他统一通信(UC)设备)，这是从完全限定域名(FQDN)构建的。

颁发机构是验证该特定证书的机构。由于任何人都可以签署证书（包括创建证书的服务器，首先也称为自签名证书），服务器和客户端具有其信任为可信的颁发者或CA的列表。

证书链始终以自签顶级证书或根证书结尾。当您在证书层次结构中移动时，每个证书相对于主题具有不同的颁发者。最终，您会遇到主题和颁发者匹配的根CA。这表示它是顶级证书，因此是需要由客户端或服务器的受信任CA列表信任的证书。

SSL 握手摘要

对于遍历区域，Expressway-C始终充当客户端，而Expressway-E始终充当服务器。简化交换的工作原理如下所示：

Expressway C

Expressway E

-----客户端Hello----->
<-----Server Hello-----
<----服务器证书-----
<----证书请求 ---
-----客户端证书----->

此处的密钥在交换中，因为Expressway-C始终发起连接，因此始终是客户端。Expressway-E是第一个发送其证书的路由器。如果Expressway-C无法验证此证书，它将断开握手，无法将其自己的证书发送到Expressway-E。

另一个需要格外注意的是证书的传输层安全 (TLS) Web 客户端身份验证属性和 TLS Web 服务器身份验证属性。这些属性在签署CSR的CA上确定（如果使用Windows CA，这由选定的模板确定），并指示证书在客户端或服务（或两者）角色中是否有效。因为对于VCS或Expressway，它可基于情况（对于遍历区域始终相同），并且证书必须具有客户端和服务身份验证属性。

Expressway-C和Expressway-E在上传到新服务器证书时出错（如果两者均未应用）。

如果不确定证书是否具有这些属性，则可以在浏览器或操作系统中打开证书详细信息，并选中“扩展密钥使用”部分（请参见图像）。格式可能不同，具体取决于您如何查看证书。

示例：

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...

配置

Expressway C 和 Expressway E 遍历区域/信任

生成并签署 CSR

如前所述，Expressway-C和Expressway-E证书必须由内部或外部CA或OpenSSL签名才能进行自签名。

 注：不能使用Expressway服务器上的临时证书，因为它不受支持。如果您使用通配符证书，但您有CA签名证书，且主题行未具体定义，则不支持通配符证书。


第一步是生成 CSR 并使用首选 CA 类型签署 CSR。证书创建指南中有关于此过程的详细说明。创建CSR时，请务必记住需要包含在证书中的主题备用名称(SAN)。证书指南和《移动远程访问部署指南》中也列出了这些 SAN。请查阅最新版本的指南，因为新功能推出后，可以添加更多指南。根据使用的功能，需要包括的常见SAN列表：

Expressway-C

- 添加到域列表的任何域（内部或外部）。
- 如果使用XMPP联合，则任何持久聊天节点别名。
- 如果使用安全设备配置文件，则在CUCM上使用安全设备配置文件名称。

Expressway-E

- Expressway C 上配置的任何域。
- 如果使用XMPP联合，则任何持久聊天节点别名。
-

 注意：如果用于外部服务记录(SRV)查找的基础域未作为SAN包含在Expressway-E证书 (xxx.com或collab-edge.xxx.com)中，则Jabber客户端仍要求最终用户在首次连接时接受证书，而TC终端将根本无法连接。

将Expressway-C和Expressway-E配置为相互信任

为了让统一通信穿越区域建立连接，Expressway-C和Expressway-E必须信任彼此的证书。在本示例中，假设Expressway E证书由使用此层次结构的公共CA签名。

证书 3

颁发者：GoDaddy根CA

主题：GoDaddy根CA

证书 2

颁发者：GoDaddy根CA

主题：GoDaddy中间机构

证书 1

签发方：GoDaddy中间机构

主题：Expressway-E.lab

Expressway-C需要配置信任证书1。在大多数情况下，根据应用到服务器的受信任证书，它只发送其最低级别的服务器证书。这意味着Expressway-C要信任证书1，必须将证书2和3上传到Expressway-C的受信任CA列表(Maintenance > Security > Trusted CA List)。如果在Expressway-C收到Expressway-E证书时省略中间证书2，则它无法将其绑定到受信任的GoDaddy根CA，因此它将被拒绝。

证书 3

颁发者：GoDaddy根CA

主题：GoDaddy根CA

证书 1

签发方：GoDaddy中间机构 — 不受信任！

主题：Expressway-E.lab

此外，如果仅上传不带根的中间证书到Expressway-C的受信任CA列表，则会发现GoDaddy中间机构受信任，但它由更高权威签署，在这种情况下，GoDaddy根CA不受信任，因此它将失败。

证书 2

颁发者：GoDaddy根CA — 不受信任！

主题：GoDaddy中间机构

证书 1

签发方：GoDaddy中间机构

主题：Expressway-E.lab

将所有中间 CA 和根 CA 添加到受信任的 CA 列表后，便可以验证证书...

证书 3

颁发者：GoDaddy根CA — 自签顶级证书受信任且链完整！

主题：GoDaddy根CA

证书 2

颁发者：GoDaddy根CA

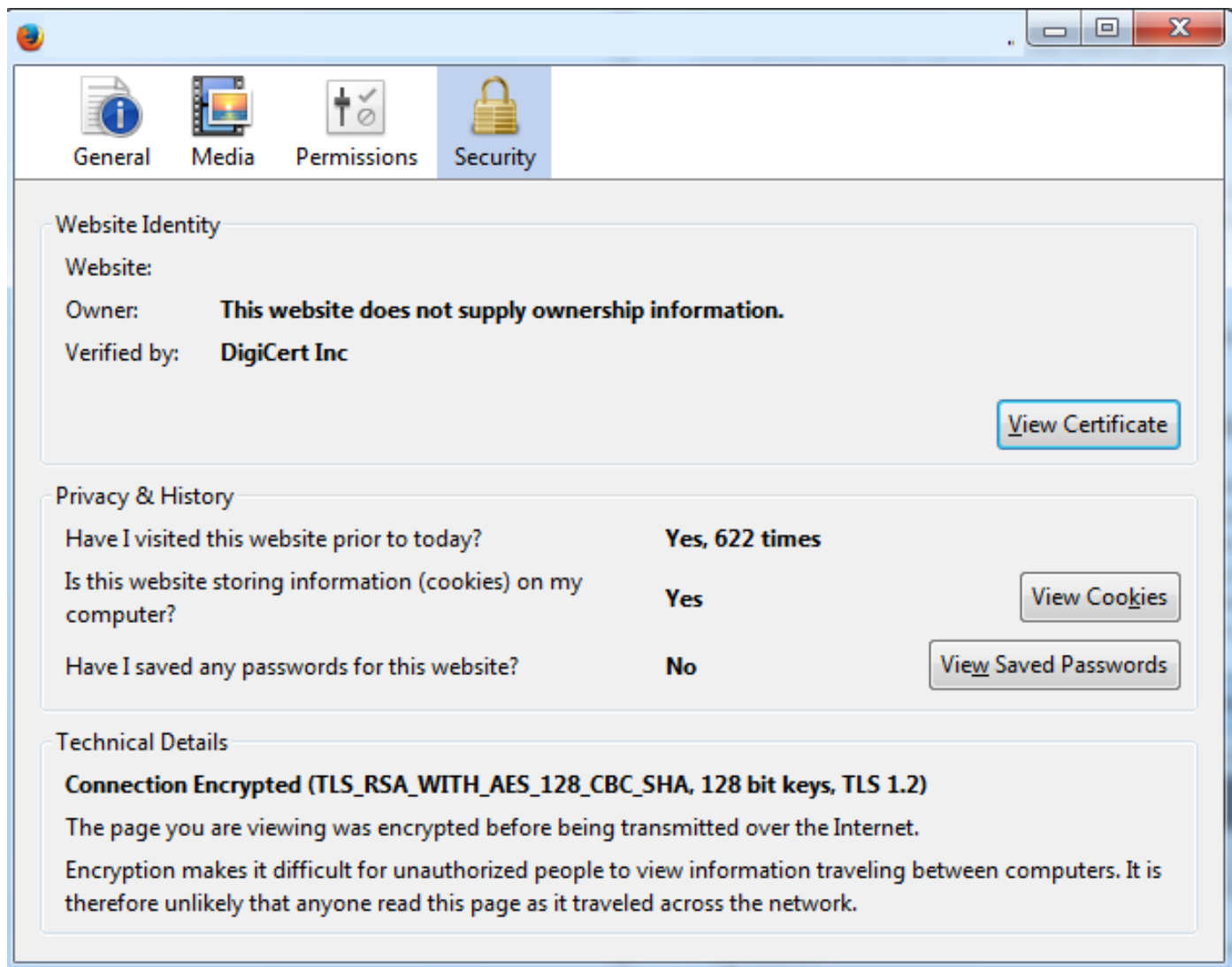
主题：GoDaddy中间机构

证书 1

签发方：GoDaddy中间机构

主题：Expressway-E.lab

如果您不确定证书链是什么，您可以在登录到特定Expressway的Web界面时检查浏览器。该过程因浏览器而异，但在Firefox中，您可以点击地址栏最左侧的锁图标。然后在弹出窗口中，点击更多信息 > 查看证书 > 详细信息。如果浏览器能将整个链拼凑在一起，您就可以从上到下看到链。如果顶级证书没有匹配的主题和颁发者，则意味着链未完成。如果点击export并突出显示所需的证书，则还可以自行导出链中的每个证书。当您不确定是否已向 CA 信任列表上传正确的证书时，这一点非常有用。



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

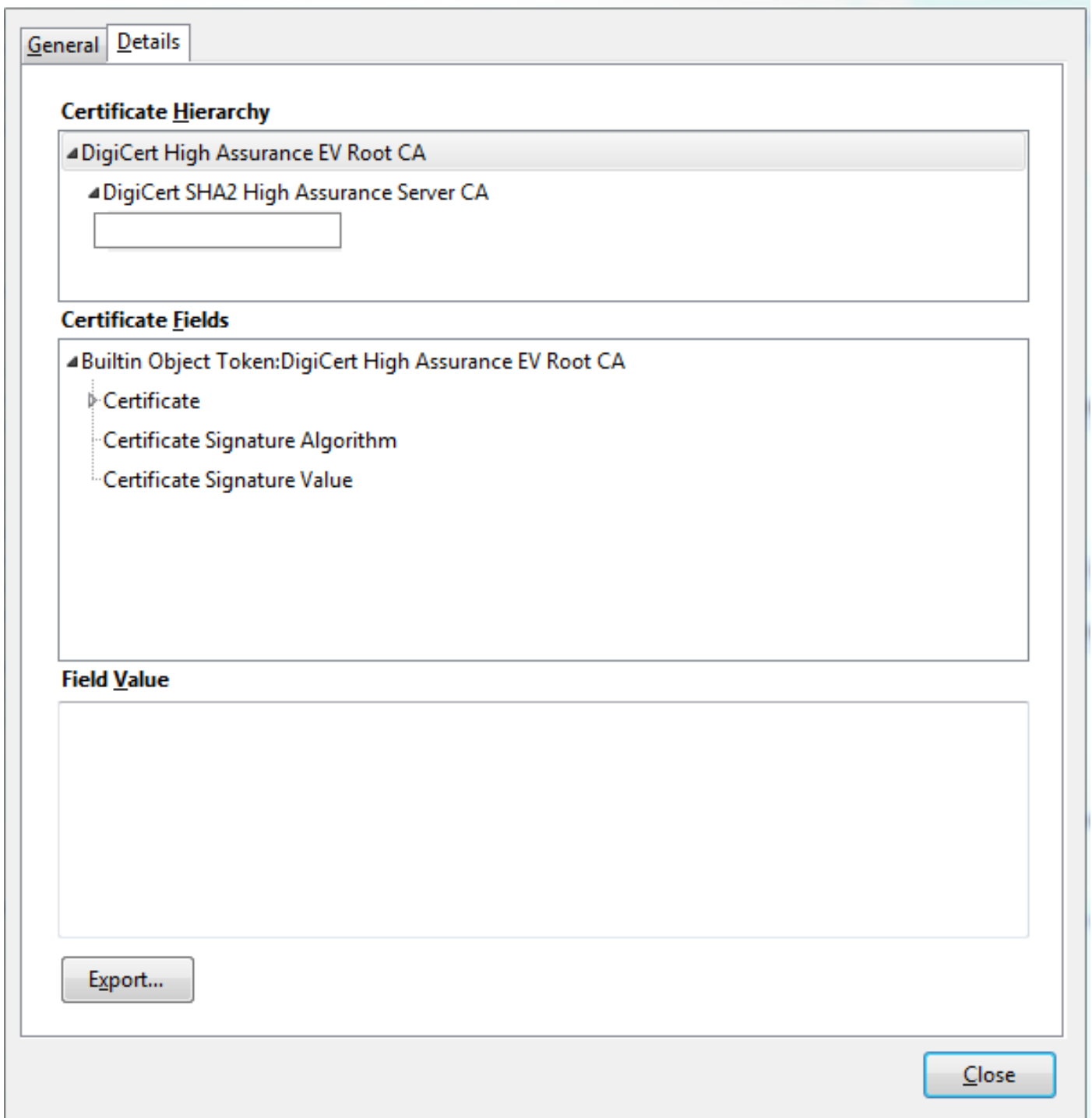
Begins On 3/25/2015

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



现在Expressway-C信任来自Expressway-E的证书，请确保证书在相反方向上运行。如果Expressway-C证书由签署Expressway-E的同一CA签署，则过程非常简单。将已上传到C的相同证书上传到Expressway-E上的受信任CA列表。如果C由不同的CA签名，您需要使用如图所示的相同过程，但改用已签名的Expressway C证书链。

思科统一通信管理器 (CUCM) 和 Expressway C 之间的安全通信

概述

与Expressway-C和Expressway-E之间的遍历区域不同，Expressway-C和CUCM之间不需要安全信

令。除非内部安全策略不允许安全信令，否则必须始终将MRA配置为首先与CUCM上的非安全设备配置文件一起工作，以确认其余部署正确，然后继续此步骤。

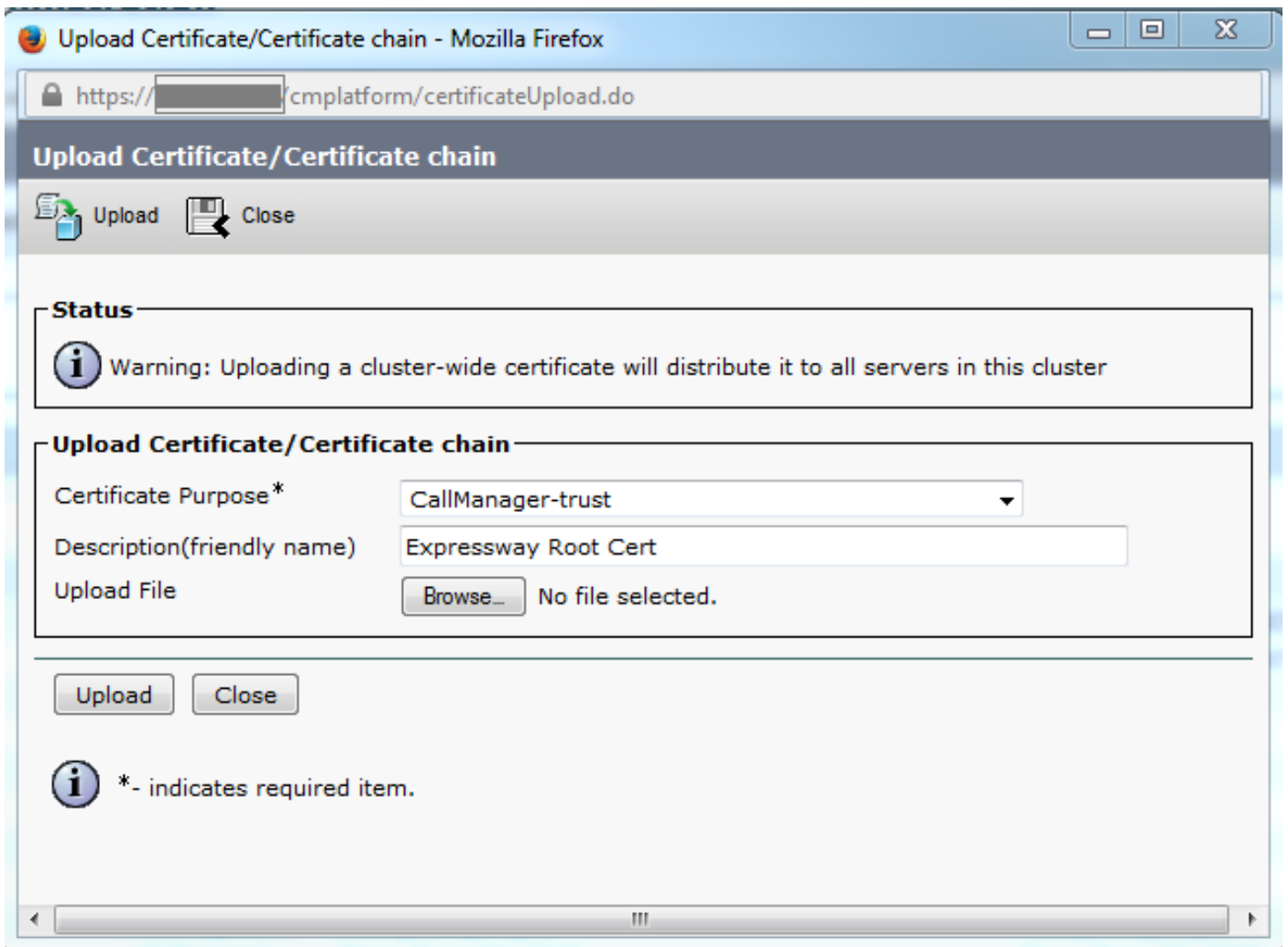
在CUCM和Expressway-C之间可以启用两个主要安全功能：TLS验证和安全设备注册。这两个功能有明显区别，因为在SSL握手过程中，它们在CUCM侧使用两个不同的证书。

TLS 验证 - Tomcat 证书

安全 SIP 注册 - Callmanager 证书


配置CUCM和Expressway-C之间的信任

在本例中，概念与Expressway-C和Expressway-E之间的概念完全相同。CUCM 首先必须信任Expressway C 的服务器证书。这意味着，在CUCM上，需要将Expressway-C的中介和根证书作为tomcat-trust证书上传到TLS验证功能，并作为CallManager-trust上传到安全设备注册。为此，请导航至CUCM Web GUI右上方的Cisco Unified OS Administration，然后导航至Security>Certificate Management。您可在此处点击上传证书/证书链并选择正确的信任格式，或点击查找来查看当前已上传证书列表。



您需要确保Expressway-C信任签署CUCM证书的CA。如果将其添加到受信任CA列表，则可以实现此目的。在几乎所有情况下，如果您使用CA签署CUCM证书，则tomcat和CallManager证书必须由同一CA签署。如果它们不同，则当您使用TLS验证和安全注册时，您需要信任它们。

对于安全SIP注册，您还必须确保应用到设备的CUCM上的安全设备配置文件名称在Expressway-C证书上列为SAN。如果其中不包含安全注册消息，则它将因CUCM中的403而失败，这表示TLS失败。

 **注意：**在CUCM和Expressway-C之间进行SSL握手以进行安全SIP注册时，将发生两次握手。首先，Expressway-C充当客户端并发起与CUCM的连接。成功完成连接后，CUCM会发起另一个握手，作为客户端进行应答。这意味着，与 Expressway C 一样，CUCM 上的 Callmanager 证书必须同时应用 TLS Web 客户端和 TLS Web 服务器身份验证属性。不同之处在于，CUCM允许上传这些证书而不使用这两者，并且如果CUCM仅具有服务器身份验证属性，则内部安全注册可以正常工作。如果您在列表上查找CallManager证书并选择它，则可以在CUCM上确认这一点。在此，您可以查看“分机”部分下的用法oid。您可以看到1.3.6.1.5.5.7.3.2用于客户端身份验证，1.3.6.1.5.5.7.3.1用于服务器身份验证。您还可以在此窗口中下载证书。

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,
]
```

Regenerate Generate CSR Download .PEM File Download .DER File

 **注意：**应用于集群中发布者的信任证书必须复制到订阅服务器。最好在新配置中分别登录这些配置，进行确认。

 **注：**为了使Expressway-C正确验证来自CUCM的证书，必须在Expressway-C中添加具有FQDN而不是IP地址的CUCM服务器。IP地址的唯一工作方式是在证书中将每个CUCM节点的IP添加为SAN，这几乎是永远无法完成的。

具有自签名证书的CUCM服务器

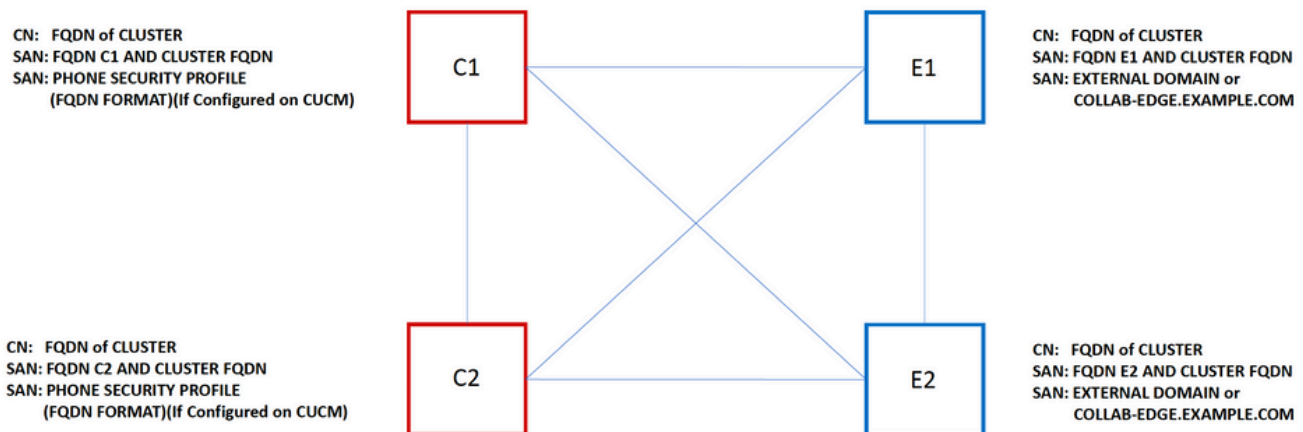
默认情况下，CUCM服务器带有自签名证书。如果已经部署了这些功能，则无法同时使用TLS验证和安全设备注册。任一功能都可以单独使用，但由于证书是自签名的，这意味着自签名Tomcat和自签名CallManager证书都需要上传到Expressway-C上的受信任CA列表。当Expressway-C搜索其信任列表以验证证书时，它会在找到具有匹配的主题的证书后停止。因此，无论信任列表中的哪个较高者（即tomcat或CallManager），此功能都会起作用。下层则会失败，就像它不存在一样。解决此问题的方法是使用CA（公共或私有）签署CUCM证书并单独信任此CA。

Expressway C 和 Expressway E 集群注意事项

集群证书

如果您有用于冗余的 Expressway C 或 Expressway E 服务器集群，则强烈建议您为每个服务器生成单独的 CSR，并使用 CA 签署 CSR。在上一个场景中，每个对等体证书的公用名(CN)将是相同的集群完全限定域名(FQDN)，而SAN将是集群FQDN和相应的对等体FQDN，如图所示：

Expressway Cluster Certificates MRA

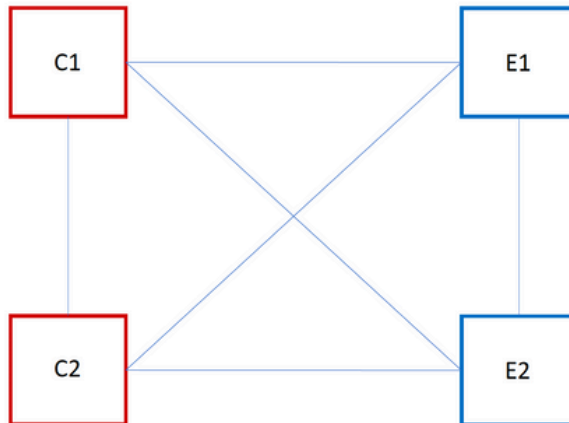


您可以将集群FQDN用作CN，并且在SAN中使用每个对等体FQDN和集群FQDN可为集群中的所有节点使用同一证书，从而避免由公共CA签署多个证书的成本。

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

 注意：只有在UCM上使用安全电话安全配置文件时，才需要Cs证书上的电话安全配置文件名称。外部域或collab-edge.example.com(其中example.com是您的域)仅要求通过MRA注册IP电话和TC终端。这是通过MRA注册Jabber的可选操作。如果不存在，则Jabber在Jabber通过MRA登录时会提示接受证书。

如果绝对必要，可以通过下一个过程完成此操作，也可以使用OpenSSL手动生成私钥和CSR:

步骤1.在集群的主节点上生成CSR，并将其配置为将集群别名列CN。将集群中的所有对等体添加为备用名称，以及所有其他必需的SAN。

步骤2.签署此CSR并将其上传到主要对等体。

步骤3.以root用户身份登录到主目录，并下载位于/Tandberg/persistent/certs中的私钥。

步骤4.将签名证书和匹配的私钥上传到集群中的其他对等设备。

 注：出于以下原因，不建议这样做：

- 1.由于所有对等体使用相同的私钥，因此存在安全风险。如果某个服务器受到某种危害，攻击者可以解密来自任何服务器的流量。
- 2.如果需要对证书进行更改，则必须再次执行整个过程，而不是简单的CSR生成和签名。

受信任的 CA 列表

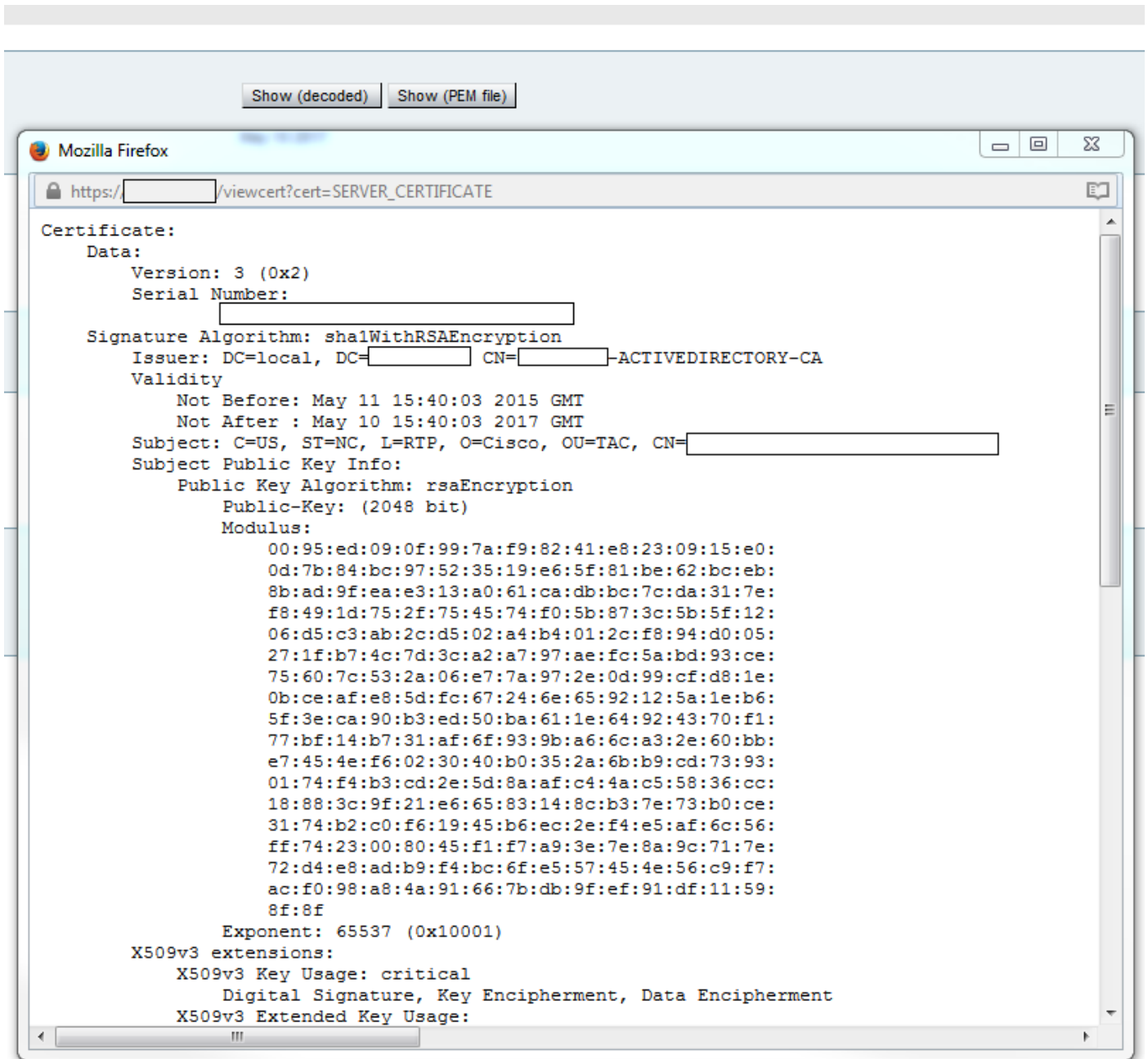
与集群中的 CUCM 订阅方不同，受信任的 CA 列表是不会在 Expressway 或 VCS 集群中的对等体之间复制。这意味着，如果您有一个集群，您需要手动将受信任证书上传到每个对等体上的CA列表。

验证

使用本部分可确认配置能否正常运行。

检查当前证书信息

您可以通过多种方法来查看现有证书的信息。第一个选项是通过Web浏览器。使用上一节中描述的方法，该方法也可用于导出链中的特定证书。如果需要验证SAN或添加到Expressway服务器证书的其他属性，可以直接通过Web图形用户界面(GUI)执行此操作，导航到Maintenance > Security Certificates > Server Certificate，然后单击Show Decoded。

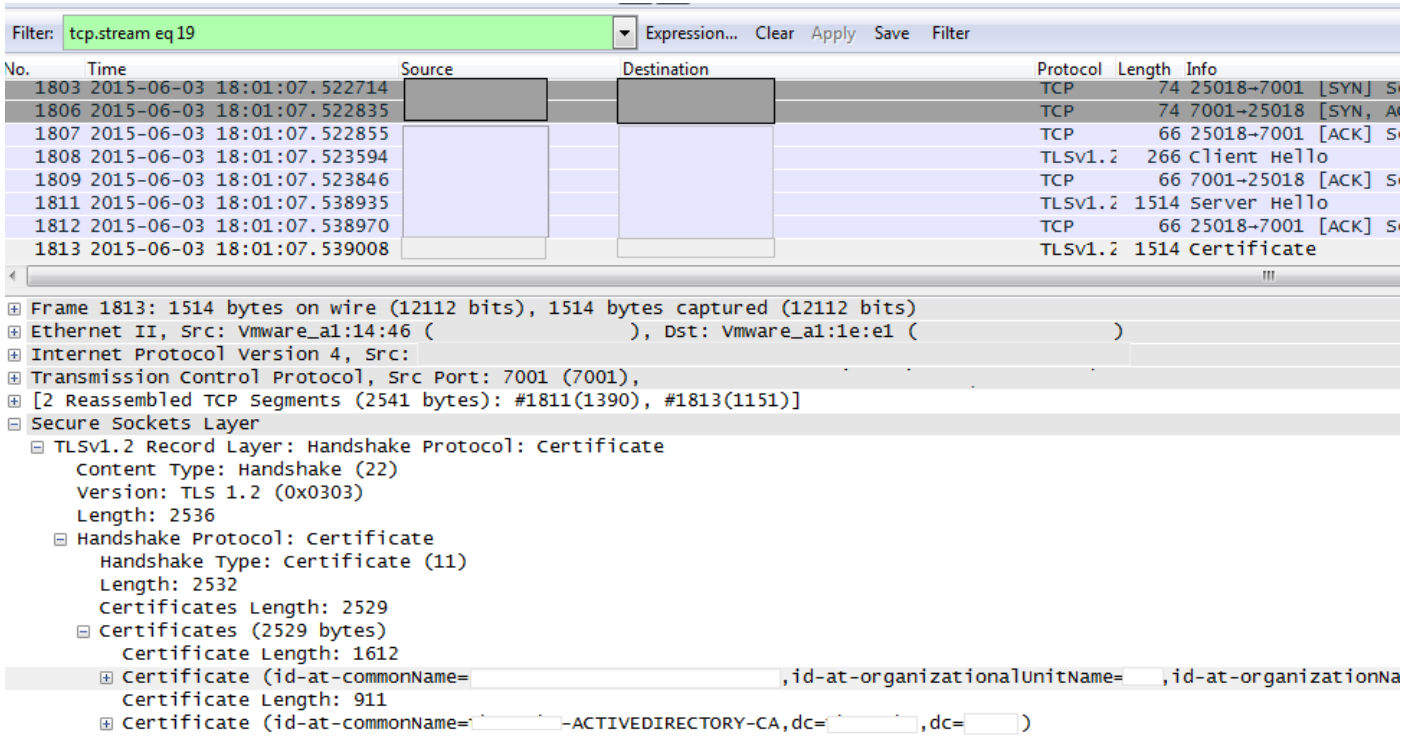


您可以在此处查看证书的所有特定详细信息，而无需下载该证书。如果尚未上传关联的已签名证书，您也可对活动 CSR 执行相同的操作。

在Wireshark中读取/导出证书

如果您拥有包含证书交换的SSL握手的Wireshark捕获，Wireshark实际上可以为您解码证书，并且

您实际上可以从内部导出链中的任何证书（如果交换的是完整链）。为特定的证书交换端口（在遍历区域的情况下，通常为 7001）筛选数据包捕获。接下来，如果您没有看到客户端和服务端 hello 数据包以及 SSL 握手，请右击 TCP 流中的一个数据包，然后选择 decode as。此处，选择 SSL，然后单击 apply。现在，如果您捕获了正确的流量，则必须看到证书交换。查找来自负载中包含证书的正确服务器的数据包。展开下窗格中的 SSL 部分，直到您看到证书列表，如图所示：



您可以在此处展开任何证书以查看所有详细信息。如果要导出证书，请右键单击链中的所需证书（如果有多个证书），然后选择导出选定数据包字节。输入证书名称并点击保存。现在，您必须能够在 Windows 证书查看器中打开证书（如果为其提供 .cer 扩展名），或者将其上传到任何其他工具进行分析。

故障排除

本节提供可用于对配置进行故障排除的信息。

测试以了解 Expressway 上的证书是否受信任

虽然最佳方法是手动检查证书链并确保所有成员都包括在 Expressway 受信任 CA 列表中，但您可以快速进行检查，以确保 Expressway 在 Web GUI 的维护 > “安全证书”(Security Certificates) 下的“客户端证书测试”(Client Certificate Testing) 帮助下信任特定客户端的证书。保持所有默认设置相同。从下拉列表中选择 Upload Test File (pem format)，然后选择要验证的客户端证书。如果证书不受信任，您会收到一个错误（如图所示），说明证书被拒绝的原因。您看到的错误是上载的证书的解码信息以供参考。

Client certificate testing

Client certificate

This tests whether a client certificate is valid when checked against the Expressway CA list.

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 authentication credentials. It allows you to specify username format combinations to the nominated certificate to see if the certificate matches the nominated pattern.

Regex to match against certificate:

Username format:

[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.

如果您收到错误信息，声称Expressway无法获取证书CRL，但Expressway不使用CRL检查，这意味着证书将受信任并已通过所有其他验证检查。

Client certificate testing

Client certificate

This tests whether a client certificate is valid when checked against the Expressway CA list.

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 username format combinations to the nominated certificate to see if the certificate matches the nominated pattern.

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 终端 (7800/8800 系列电话)

这些新设备随附预先填充的证书信任列表，其中包括大量众所周知的公共CA。无法修改此信任列表，这意味着您的Expressway E证书必须由其中一个匹配的公共CA签名才能使用这些设备。如果由内部CA或其他公共CA签名，则连接将失败。与 Jabber 客户端不同，此类型终端不提供手动接受证书的选项。

 注：对于某些部署，使用具有7800/8800系列电话上所包含列表中的CA的Citrix NetScaler等设备可以通过MRA注册，即使Expressway-E使用内部CA也是如此。NetScalers根CA需要上传到Expressway-E，内部根CA需要上传到Netscaler以使SSL身份验证生效。事实证明，这种方法行之有效，是尽最大努力的支持。

 注：如果受信任CA列表似乎包含所有正确的证书，但仍被拒绝，请确保列表中没有另一个主题相同的证书可能与正确的证书冲突。当其他所有证书均发生故障时，您可以始终直接从浏览器或Wireshark导出证书链，并将所有证书上传到对方的服务器CA列表。这将保证它是受信任证书。

 注意：排除遍历区域故障时，有时问题可能看似与证书有关，但实际上问题出在软件端。请确保用于遍历的账户用户名和密码正确。

 注意：VCS或Expressway在证书的SAN字段中不支持超过999个字符。超过此限制（需要许多备用名称）的任何SAN将被忽略，就好像它们不存在一样。

视频资源

本部分提供视频中的信息，可以指导您完成所有证书配置过程。

[为MRA或群集Expressway生成CSR](#)

[将服务器证书安装到Expressway](#)

[如何在Expressway之间配置证书信任](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。