将Expressway-Core的根/中间证书上传到CUCM

目录

简介

背景信息

配置

- 步骤1.获取签署Expressway C服务器证书的根证书和中间证书
- 步骤2.上传CUCM上的根证书和中间证书（如果适用）
- 步骤3.在CUCM上重新启动必要的服务

相关信息

简介

本文档介绍如何将已签名Expressway-C证书的CA的根证书和中间证书上传到CUCM发布服务器。

背景信息

由于X14.0.2中Expressway上的流量服务器服务有所改进，因此，只要服务器(CUCM)请求其提供在8443以外的端口（例如，6971,6972）上运行的服务，Expressway-C就会发送其客户端证书，即使CUCM处于非安全模式。由于此更改，需要将Expressway-C证书签名证书颁发机构(CA)同时作为tomcat-trust和callmanager-trust添加到CUCM中。

在CUCM上上传Expressway-C签名CA失败会导致Expressway升级到X14.0.2或更高版本后MRA登录失败。

为了使CUCM信任Expressway-C发送的证书，tomcat-trust和callmanager-trust必须包括根CA和签署Expressway-C证书所涉及的任何中间CA。

配置

步骤1.获取签署Expressway C服务器证书的根证书和中间证书

当您最初从签署该服务器证书的CA收到服务器证书时，您还拥有该服务器证书的根证书和中间证书，并将其存储在安全位置。如果您仍然拥有这些文件或可以再次从CA下载这些文件，可以进入第

2步，在此可以找到如何将文件上传到CUCM的说明。

如果您不再拥有这些文件，可以从Expressway-C Web界面下载它们。这有点复杂，因此强烈建议您联系您的CA从他们下载信任库（如果可能）。

在Expressway-C上，导航到维护>安全>服务器证书，然后点击服务器证书旁边的显示（解码）按钮。这将打开一个包含Expressway-C服务器证书内容的新窗口/选项卡。您可以在此处查找Issuer字段：

<#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:
...
```

在本示例中，Expressway-C服务器证书由组织DigiCert Inc.颁发，其通用名称为DigiCert Global CA-1。

现在，导航到维护>安全>受信任CA证书，然后在列表中查看您是否有与“主题”字段中的值完全相同的证书。在本例中，即O=DigiCert Inc， CN=DigiCert Global CA-1 in the Subject字段。如果找到匹配项，则表示这是一个中间CA。您需要此文件，并且需要继续查找，直到找到根CA。

如果找不到匹配项，请在Issuer字段中搜索具有此值的证书，其主题为Matches Issuer。如果找到匹配项，则表示这是根CA文件，这是我们需要的唯一文件。



	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信任存储

在本示例中，找到证书后，您注意到Subject字段与Issuer字段不匹配。这意味着这是中间CA证书。除了根证书外，还需要此证书。如果主题said匹配颁发者(Subject said Matches Issuer)，则您会知道这是根证书颁发机构，是您需要信任的唯一证书。

如果您有中间证书，您需要继续操作，直到我们找到根证书。为此，请查看您的中间证书的Issuer字段。然后在Subject字段中查找具有相同值的证书。在本例中，这是O=DigiCert Inc，OU=www.digicert.com,CN=DigiCert Global Root CA — 您将在Subject字段中查找具有此值的证书。如果找不到匹配的证书，则在Issuer字段中查找此值，其主题与Matches Issuer匹配。

在本例中，您可以看到我们的Expressway-C服务器证书由中间CA O=DigiCert Inc.签署，CN=DigiCert Global CA-1由根CA O=DigiCert Inc.签署。OU=www.digicert.com,CN=DigiCert Global Root CA。找到根CA后，您的工作就完成了。如果您找到了另一个中间CA，则需要继续此过程，直到您确定了每个中间CA和根CA。

要下载根证书和中间证书文件，请单击列表下的Show all(PEM file)按钮。这将以PEM格式显示所有根证书和中间证书。向下滚动，直至找到与中间证书或根证书之一匹配的证书。在本例中，您找到的第一个证书是O=DigiCert Inc， CN=DigiCert Global Root CA — 您打算将此证书复制到一个文件并在本地保存。

```
...
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
...
```

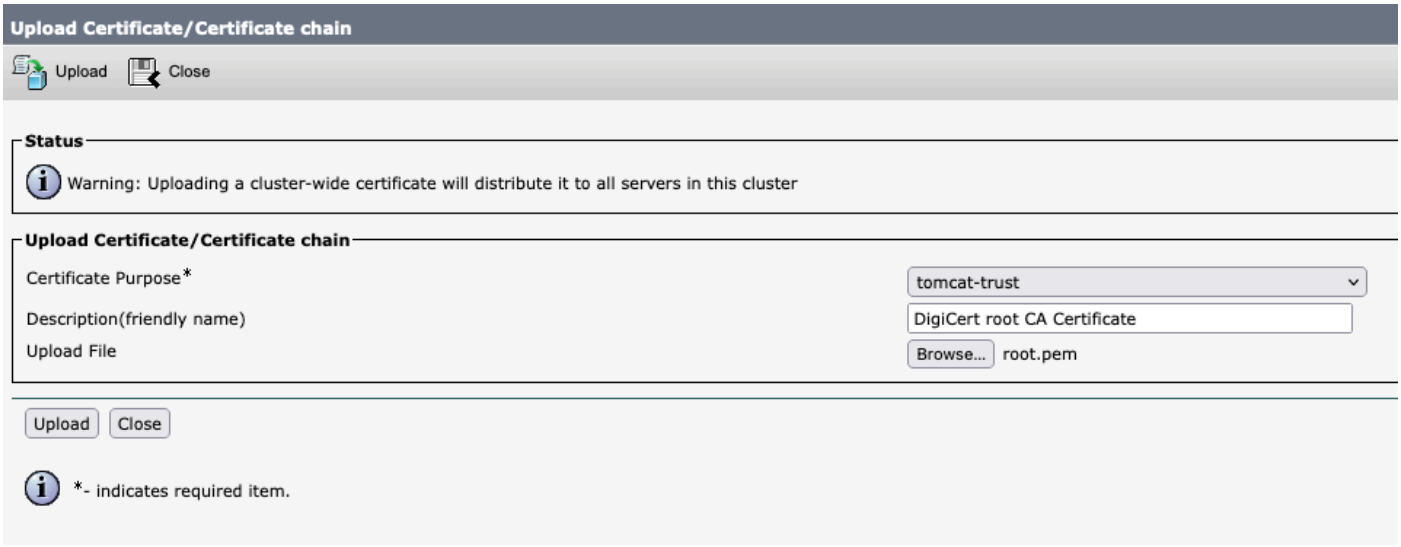
对于每个根证书和最终中间证书，复制以（包括）-----BEGIN CERTIFICATE-----开始、以（包括）-----END CERTIFICATE-----结束的所有内容。将每个文件放在单独的文本文件中，并在底部添加1个额外的空行（在-----END CERTIFICATE-----行之后）。 使用.pem扩展名保存这些文件：root.pem、intermediate1.pem、intermediate2.pem、...每个根/中间证书都需要一个单独的文件。在上一个示例中，我们的root.pem文件将包含：

```
-----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-----
```

注意：底部必须有一个空行。

步骤2.上传CUCM上的根证书和中间证书（如果适用）

- 登录到CUCM发布服务器的Cisco Unified OS Administration页面。
- 导航到安全>证书管理。
- 单击Upload Certificate/Certificate chain按钮。
- 在新窗口中，开始从步骤1上传根证书。将其上传到tomcat-trust。



- 单击Upload按钮，接下来必须看到Success:已上传证书。忽略要求您立即重新启动Tomcat的消息。
- 现在使用CallManager-trust上传相同的根文件以实现证书目的。
- 对Expressway-C上使用的所有中间证书重复前面的步骤（上传到tomcat-trust和CallManager-trust）。

步骤3.在CUCM上重新启动必要的服务

需要在CUCM集群中的每个CUCM节点上重新启动这些服务：

- Cisco CallManager
- Cisco TFTP
- Cisco Tomcat
- Cisco HAProxy

Cisco CallManager和Cisco TFTP可以从CUCM的Cisco Unified Serviceability页面重新启动：

- 登录到CUCM发布服务器的Cisco Unified serviceability页面。
- 导航到工具>控制中心 — 功能服务。
- 选择Publisher作为服务器。
- 选择Cisco CallManager服务，然后单击Restart按钮。
- 重新启动Cisco CallManager服务后，选择Cisco TFTP service，然后单击Restart按钮。

Cisco Tomcat和HAProxy只能从CLI重新启动：

- 打开与CUCM发布服务器的命令行连接。
- 使用命令utils service restart Cisco Tomcat。
- 使用命令utils service restart Cisco HAProxy

相关信息

技术支持和文档- 思科系统

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）。