

Carregue os certificados raiz e intermediários do Expressway-Core no CUCM

Contents

[Introduction](#)

[Prerequisites](#)

[Informações de Apoio](#)

[Configuração](#)

[Passo 1: Obter a raiz e certificados intermediários que assinaram o certificado do servidor Expressway-C](#)

[Passo 2: Carregar a raiz e os certificados intermediários \(se houver\) no CUCM](#)

[Passo 3: Reinicie os serviços necessários no CUCM](#)

Introduction

Este documento descreve como carregar os certificados raiz e intermediários que assinaram o certificado Expressway-C para o editor do CUCM como "tomcat-trust" e como "callmanager-trust".

Devido a melhorias no serviço de servidor de tráfego no Expressway em X14.0.2, o Expressway-C envia seu certificado de cliente sempre que um servidor (CUCM) o solicita, para serviços que são executados em portas diferentes de 8443 (por exemplo, 6971.6972), mesmo que o CUCM esteja no modo não seguro. Devido a essa alteração, é necessário que a Autoridade de Certificação (CA) de assinatura de certificado Expressway-C seja adicionada ao CUCM como "tomcat-trust" e "callmanager-trust".

A falha ao carregar a CA de assinatura do Expressway-C no CUCM faz com que o login do MRA falhe após uma atualização do Expressways para X14.0.2 ou superior. Na captura de pacotes entre o Expressway-C e o CUCM, você verá o CUCM enviar um erro TLS 'CA desconhecida' ao Expressway-C.

Prerequisites

Informações de Apoio

Para que o CUCM confie no certificado enviado pelo Expressway-C, ele precisa ser capaz de estabelecer um link desse certificado para uma Autoridade de Certificação (CA) de nível superior (raiz) na qual ele confia. Esse link, uma hierarquia de certificados que vincula um certificado de entidades a um certificado de CA raiz, é chamado de cadeia de confiança. Para poder verificar essa cadeia de confiança, cada certificado contém dois campos: Emitente (ou 'Emitido por') e Assunto (ou 'Emitido para').

Os certificados do servidor, como o que o Expressway-C envia para o CUCM, têm no campo 'Assunto' normalmente seu FQDN no CN (Nome comum) :

Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=vcs-c1.vngtp.lab

Exemplo de um certificado de servidor para Expressway vcs-c1.vngtp.lab. Ele tem o FQDN no atributo CN do campo Assunto junto com outros atributos como País (C), Estado (ST), Local (L), ... Também podemos ver que o certificado do servidor é distribuído (emitido) por uma CA chamada vngtp-ACTIVE-DIR-CA (vngtp-ACTIVE-DIR-CA.vngtp.lab).

As CAs de nível superior (CAs raiz) também podem emitir um certificado para se identificarem. Nesse certificado CA raiz, vemos que Emissor e Assunto têm o mesmo valor :

Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA

Neste certificado, os campos Emissor e Assunto têm o mesmo valor. É um certificado passado por uma CA raiz para se identificar.

Em uma situação típica, as CAs raiz não emitem diretamente certificados de servidor. Em vez disso, emitem certificados para outras autoridades de certificação. Essas outras CAs são chamadas de CAs intermediárias. Por sua vez, as autoridades de certificação intermediárias podem emitir diretamente certificados de servidor ou certificados para outras autoridades de certificação intermediárias. Podemos ter uma situação em que um certificado de servidor é emitido pela CA 1 intermediária, que por sua vez recebe um certificado da CA 2 intermediária e assim por diante. Até que a CA intermediária obtenha seu certificado diretamente da CA raiz:

Server certificate :

Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-1 Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=vcs-c1.vngtp.lab

Intermediate CA 1 certificate :

Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-2
Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-1

Intermediate CA 2 certificate :

Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-3
Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-2

...

Intermediate CA n certificate :

Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-n

Root CA certificate :

Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-C

Agora, para que o CUCM confie no certificado de servidor enviado pelo Expressway-C, ele precisa ser capaz de criar a cadeia de confiança desse certificado de servidor até um certificado de CA raiz. Para que isso aconteça, precisamos carregar o certificado de CA raiz e também todos os certificados de CA intermediários (se houver, o que não é o caso se a CA raiz teria emitido diretamente o certificado do servidor do Expressway-C) na lista confiável do CUCM.

Note: Embora os campos Emissor e Assunto sejam fáceis de criar a cadeia de Confiança de forma legível por humanos, o Expressway-C e o CUCM não usam esses campos no certificado. Em vez disso, eles usam os campos 'X509v3 Authority Key Identifier' e 'X509v3 Subject Key Identifier' para criar a cadeia de confiança. Essas chaves contêm identificadores para os certificados que são mais precisos do que para usar os campos Assunto/Emissor : pode haver 2 certificados com os mesmos campos Assunto/Emissor, mas um deles expirou e o outro ainda é válido. Ambos teriam um identificador de chave de assunto X509v3 diferente para que o Expressway/CUCM ainda possa determinar a cadeia de confiança correta.

Configuração

Passo 1: Obter a raiz e certificados intermediários que assinaram o certificado do servidor Expressway-C

Como uma boa prática, quando você inicialmente obteve o certificado de servidor de uma CA (CA raiz ou CA intermediária) que assinou esse certificado de servidor, você também obteve os certificados raiz e intermediários para esse certificado de servidor e os armazenou em algum lugar seguro. Se esse for o caso, você pode obter esses certificados raiz e intermediários e passar para a etapa 2, onde você pode encontrar instruções sobre como carregá-los no CUCM.

Se você não seguiu a prática recomendada para armazenar seus certificados raiz/intermediários em algum lugar seguro, podemos obtê-los no Expressway-C, como você teria carregado lá também antes de carregar o certificado do servidor. O primeiro passo seria procurar exatamente qual certificado precisamos. Para isso, no Expressway-C navegue para Manutenção > Segurança > Certificado de servidor e clique ou selecione o botão 'Mostrar (decodificado)' ao lado de 'Certificado de servidor'. Isso abre uma nova janela/guia com o conteúdo do certificado do servidor Expressway-C. Procuramos o campo 'Emissor' aqui:

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-cl.vngtp.lab

Subject Public Key Info:

...

Nosso certificado de servidor Expressway é emitido por uma organização DigiCert Inc com nome comum 'DigiCert Global CA-1'.

Vamos agora para Manutenção > Segurança > Certificado de CA confiável e verificamos na lista se temos um certificado com o mesmo valor exato (O=DigiCert Inc, CN=DigiCert Global CA-1) no campo 'Assunto'.

Type	Issuer	Subject
<input type="checkbox"/> Certificate	CN=vngtp-ACTIVE-DIR-CA	Matches Issuer
<input type="checkbox"/> Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer
<input type="checkbox"/> Certificate	O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root	Matches Issuer
<input type="checkbox"/> Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	Matches Issuer
<input type="checkbox"/> Certificate	O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority	Matches Issuer
<input type="checkbox"/> Certificate	O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2	Matches Issuer
<input type="checkbox"/> Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer
<input type="checkbox"/> Certificate	O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA	Matches Issuer
<input type="checkbox"/> 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
<input type="checkbox"/> Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	O=DigiCert Inc, CN=DigiCert Global CA-1

Armazenamento de confiança do Expressway

Vemos realmente que há um certificado no repositório de confiança do Expressway-C que tem um assunto que é idêntico ao 'Emissor' do certificado do servidor Expressway-C. Esse certificado (o último na lista como mostrado na imagem) é emitido por O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA. Isso é diferente de seu 'Assunto', portanto sabemos que não é um certificado CA raiz, mas um certificado CA intermediário.

Nota: Se você não encontrar um certificado nessa lista com um 'Assunto' que corresponda ao 'Emissor' do nosso certificado Expressway-C, verifique a coluna 'Emissor' na lista e veja se é possível encontrar uma correspondência lá. Se esse for o caso e a coluna 'Assunto' mostrar 'Corresponde ao Emissor' para esse certificado, significa que há um certificado raiz que assinou nosso certificado de servidor Expressway-C imediatamente, sem uma CA intermediária entre eles.

Depois que encontramos o certificado intermediário, ainda não terminamos. Precisamos ir até o certificado raiz. Portanto, precisamos encontrar o certificado da CA que emitiu o certificado intermediário de CA com o assunto O=DigiCert Inc, CN=DigiCert Global CA-1. Sabemos que a CA que emitiu esse certificado é O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA. Como não vemos uma correspondência para esta CA na coluna Assunto, verificamos na coluna Emissor e realmente vemos uma correspondência : o 4º certificado na lista tem um Emissor O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA e como seu 'Assunto' diz 'Corresponde ao Emissor' sabemos que este é o certificado raiz CA.

Conclusão: nosso certificado de servidor Expressway-C foi assinado pela intermediária CA O=DigiCert Inc, CN=DigiCert Global CA-1 que, por sua vez, foi assinado pela raiz CA O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA.

Para obter o certificado raiz e intermediário, clique ou selecione o botão 'Mostrar tudo (arquivo PEM)' na lista. Isso mostra todos os certificados raiz e intermediários no formato PEM. Role para baixo até o quarto e último certificado e copie o conteúdo. O 4º certificado é nosso certificado CA raiz:

```

...
Epn3o0WC4zxe9Z2etiefC7IpJ50CBRLbflwbWsaY71k5h+3zvDyny67G7fyUIhz
ksLi4xaNmjICq44Y3ekQEe5+NauQrz4wlHrQMz2nZQ/1/I6eYs9HRCwBXbsdtTLS
R9I4LtD+gdwyah6l7jzV/OeBHRnDJELqYzmp -----END CERTIFICATE----- O=DigiCert Inc, CN=DigiCert

```

```
Global Root CA -----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvGvPBCRRGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLEwB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDEwEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAEFw0WnjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTTo1eqUKKPC3eQyaKl7hL0l1sB
CSDMAZOnTjC3U/dXGkAV53iJSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2taveg5BmV/S10fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYmq1lGNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMTom10/4
gdW7jVg/trVoSSiicNoxBN33shbyTApOB6jtSjletX+jkMOvJwIDAQABO2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBGwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgTleXkIoyQY/Esr
hMatudXH/vTBH1jLuG2cenTnmCmrEbXjckChzUyImZOMkXDiqw8cvpOp/2PV5Adg
060/nVsJ8dW041P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfV8NZ5YBberOgOzW6sRbc4L0na4UU+Krk2U886UAb3LuJEV01s
YSEY1QSteDwsOoBrp+uvFRTP2InBuThs4pFsiV9kuXclVzDAGySj4dZp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpG0X40KPMbp1ZWVbd4= -----END CERTIFICATE-----
O=The Go Daddy Group,
Inc. -----BEGIN CERTIFICATE-----
MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJh
MB8GA1UEChMYVGVhZEdvIERhZGR5IEdyb3VwLWVwLWVwLWVwLWVwLWVwLWVwLWVw
...

```

Para cada certificado raiz e eventual certificado intermediário, você copia tudo que começa com '-----BEGIN CERTIFICATE-----' e termina com (incluído) '-----END CERTIFICATE-----'. Coloque cada um deles em um arquivo de texto separado e adicione 1 linha vazia extra na parte inferior (após a linha com -----END CERTIFICATE-----). Salve esses arquivos com a extensão .pem : root.pem, intermediate1.pem, intermediate2.pem, ... Você precisa de um arquivo separado para cada certificado raiz/intermediário. Para um exemplo anterior, nosso arquivo root.pem conteria :

```
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvGvPBCRRGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLEwB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDEwEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAEFw0WnjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTTo1eqUKKPC3eQyaKl7hL0l1sB
CSDMAZOnTjC3U/dXGkAV53iJSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2taveg5BmV/S10fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYmq1lGNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMTom10/4
gdW7jVg/trVoSSiicNoxBN33shbyTApOB6jtSjletX+jkMOvJwIDAQABO2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBGwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgTleXkIoyQY/Esr
hMatudXH/vTBH1jLuG2cenTnmCmrEbXjckChzUyImZOMkXDiqw8cvpOp/2PV5Adg
060/nVsJ8dW041P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfV8NZ5YBberOgOzW6sRbc4L0na4UU+Krk2U886UAb3LuJEV01s
YSEY1QSteDwsOoBrp+uvFRTP2InBuThs4pFsiV9kuXclVzDAGySj4dZp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpG0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----

```

(observe que há 1 linha vazia na parte inferior)

Passo 2: Carregar a raiz e os certificados intermediários (se houver) no CUCM

- Faça login na página Cisco Unified OS Administration do editor do CUCM
- Navegue até Segurança > Gerenciamento de certificados
- Clique ou selecione o botão "Carregar certificado/cadeia de certificados"
- Na nova janela, comece a carregar o certificado root.pem que você obteve da Etapa 1. Carregue-o primeiro como 'Tomcat Trust' :

Upload Certificate/Certificate chain

Upload Close

Status

 Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*	<input type="text" value="tomcat-trust"/>
Description(friendly name)	<input type="text" value="DigiCert root CA Certificate"/>
Upload File	<input type="button" value="Browse..."/> root.pem

Upload Close

 *- indicates required item.

- Clique ou selecione o botão 'Upload' e, em seguida, você deverá ver "Success: Certificate Uploaded" (Certificado carregado). Ignore a mensagem sobre como reiniciar o Tomcat por enquanto.
- Carregue o mesmo arquivo root.pem agora como 'CallManager-trust' para o 'Certificate Purpose'.
- Repita as etapas anteriores (carregue como 'tomcat-trust' e 'CallManager-trust') para todos os certificados intermediários que você tiver.

Passo 3: Reinicie os serviços necessários no CUCM

Esses serviços precisam ser reiniciados em cada nó do CUCM no cluster do CUCM:

- Cisco CallManager
- Cisco TFTP
- Cisco Tomcat

Os dois primeiros podem ser reiniciados nas páginas Cisco Unified Serviceability do CUCM:

- Faça login na página de facilidade de manutenção do Cisco Unified do editor do CUCM
- Navegue até Ferramentas > Centro de controle - Serviços de recurso
- Selecione o Publicador como o servidor
- Selecione o serviço 'Cisco CallManager' e clique no botão 'Reiniciar'
- Depois que o serviço Cisco CallManager for reiniciado, selecione o serviço 'Cisco TFTP' e clique no botão 'Reiniciar'.
- Aguarde até que o serviço Cisco TFTP seja reiniciado
- Repita as etapas anteriores para cada editor

O Cisco Tomcat só pode ser reiniciado a partir do CLI:

- Abra uma conexão de linha de comando para o Editor do CUCM
- Use o comando: **utils service restart Cisco Tomcat**

- Repita as etapas anteriores em cada um dos nós do assinante