Cargar certificados raíz/intermedios de Expressway-Core en CUCM

Contenido

Introducción

Este documento describe cómo cargar los certificados raíz e intermedios de las CA que firmaron los certificados de Expressway-C en el editor de CUCM.

Antecedentes

Debido a las mejoras en el servicio de servidor de tráfico en Expressway en X14.0.2, Expressway-C envía su certificado de cliente cada vez que un servidor (CUCM) lo solicita para servicios que se ejecutan en puertos distintos de 8443 (por ejemplo, 6971.6972), incluso si CUCM está en modo no seguro. Debido a este cambio, se requiere que la autoridad de certificación (CA) de firma de certificados de Expressway-C se agregue en CUCM como tomcat-trust y callmanager-trust.

Si no se carga la CA de firma de Expressway-C en CUCM, el inicio de sesión de MRA fallará después de una actualización de Expressways a X14.0.2 o superior.

Para que CUCM confíe en el certificado que envía Expressway-C, tomcat-trust y callmanager-trust deben incluir la CA raíz y cualquier CA intermediaria involucrada en la firma del certificado de Expressway-C.

Configuración

Paso 1. Obtenga los certificados raíz e intermedio que firmaron el certificado de servidor de Expressway-C

Cuando recibió inicialmente el certificado de servidor de una CA que firmó ese certificado de servidor, también tiene los certificados raíz e intermedios para ese certificado de servidor y los almacena en un lugar seguro. Si todavía tiene estos archivos o puede volver a descargarlos

desde su CA, puede ir al paso 2, donde encontrará instrucciones sobre cómo cargarlos en CUCM.

Si ya no tiene estos archivos, puede descargarlos de la interfaz web de Expressway-C. Esto es un poco complicado, por lo que se recomienda encarecidamente ponerse en contacto con la CA para descargar el almacén de confianza de ellos, si es posible.

En Expressway-C, vaya a Mantenimiento > Seguridad > Certificado de servidor y haga clic en el botón Mostrar (descodificado) junto a Certificado de servidor. Se abre una nueva ventana o ficha con el contenido del certificado de servidor de Expressway-C. Aquí busca el campo Emisor:

<#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:
...
```

En este ejemplo, el certificado de servidor de Expressway-C lo emite una organización, DigiCert Inc. con el nombre común DigiCert Global CA-1.

Ahora, navegue hasta Mantenimiento > Seguridad > Certificado de CA de confianza, y busque en la lista para ver si tiene un certificado allí con el mismo valor exacto en el campo Asunto. En este ejemplo, O=DigiCert Inc, CN=DigiCert Global CA-1 en el campo Subject (Asunto). Si encuentra una coincidencia, significa que se trata de una CA intermedia. Necesita este archivo y debe continuar buscando hasta encontrar la CA raíz.

Si no puede encontrar una coincidencia, busque un certificado con este valor en el campo Emisor con un emisor Asunto de coincidencias. Si encuentra una coincidencia, significa que este es el archivo de la CA raíz y este es el único archivo que necesitaremos.

	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

Almacén de confianza de Expressway

En este ejemplo, después de buscar el certificado, observará que el campo Asunto no coincide con el campo Emisor. Esto significa que se trata de un certificado de CA intermedio. Necesita este certificado además del certificado raíz. Si el Sujeto dijo Coincide con el Emisor, entonces sabría que esta es la autoridad de certificados raíz y el único certificado en el que debería confiar.

Si tiene un certificado intermedio, debe continuar hasta que encontremos el certificado raíz. Para ello, consulte el campo Emisor del certificado intermedio. A continuación, busque un certificado con el mismo valor en el campo Asunto. En nuestro caso, es O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA: busca un certificado con este valor en el campo Subject (Asunto). Si no puede encontrar un certificado coincidente, busque este valor en el campo Emisor con un asunto de coincidencias Emisor.

En este ejemplo, puede ver que nuestro certificado de servidor de Expressway-C fue firmado por la CA intermedia O=DigiCert Inc, CN=DigiCert Global CA-1 que fue firmado por la CA raíz O=DigiCert Inc. OU=www.digicert.com, CN=DigiCert Global Root CA. Ya que ha encontrado la CA raíz, ha terminado. Sin embargo, si encuentra otra CA intermedia, debe continuar este proceso hasta que haya identificado todas las CA intermedias y la CA raíz.

Para descargar los archivos de certificado raíz e intermedio, haga clic en el botón Show all (archivo PEM) en la lista. Muestra todos los certificados raíz e intermedios en formato PEM. Desplácese hacia abajo hasta encontrar un certificado que coincida con uno de sus certificados intermedios o el certificado raíz. En este ejemplo, el primero que encuentra es O=DigiCert Inc, CN=DigiCert Global Root CA; va a copiar este certificado en un archivo y guardarlo localmente.

```
...
Epn3o0WC4zxe9Z2etiefC7IpJ5OCBRLbf1wbWsaY71k5h+3zvDyny67G7fyUIhz
ksLi4xaNmjICq44Y3ekQEe5+NauQrz4wlHrQMz2nZQ/1/I6eYs9HRCwBXbsdtTLS
R9I4LtD+gdwyah617jzV/OeBHRnDJELqYzmp
-----END CERTIFICATE-----

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

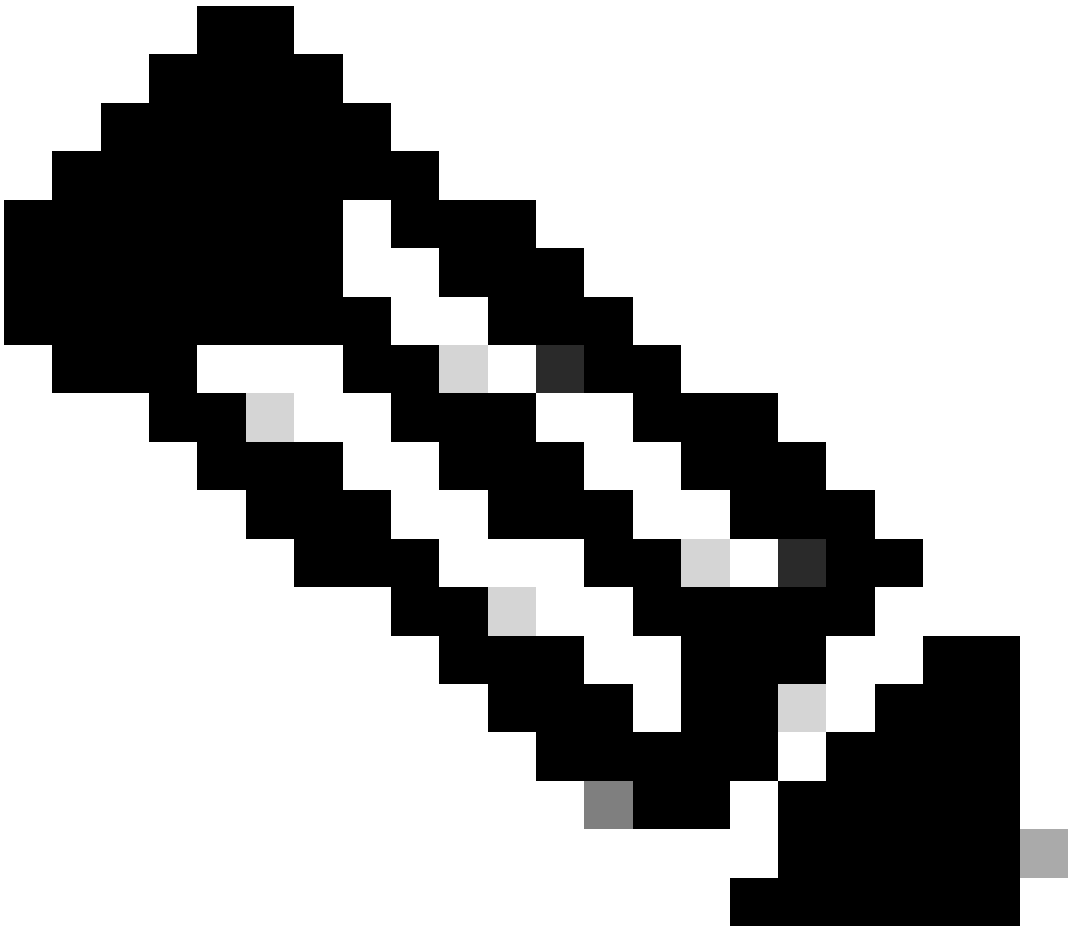
```
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
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
...
```

Para cada uno de los certificados raíz e intermedios eventuales, copie todo lo que comience con (incluido) -----BEGIN CERTIFICATE----- y termine con (incluido) -----END CERTIFICATE-----. Coloque cada uno de ellos en un archivo de texto separado y agregue 1 línea vacía adicional en la parte inferior (después de la línea con -----END CERTIFICATE-----). Guarde estos archivos con la extensión .pem: root.pem, intermediate1.pem, intermediate2.pem, ... Necesita un archivo independiente para cada certificado raíz/intermedio. Para el ejemplo anterior, nuestro archivo root.pem contendría:

```
-----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
```

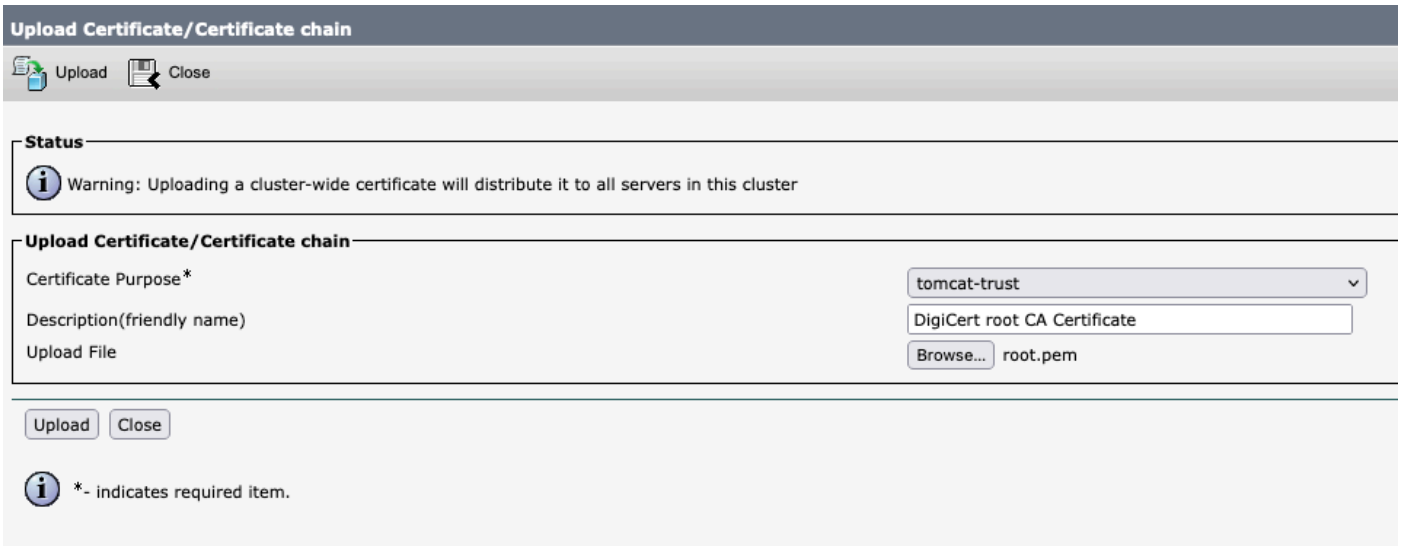
```
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----
```



Nota: Debe haber una sola línea vacía en la parte inferior.

Paso 2. Cargue los certificados raíz e intermedio en CUCM (si procede)

- Inicie sesión en la página Administración de Cisco Unified OS del publicador de CUCM.
- Navegue hasta Seguridad > Administración de certificados.
- Haga clic en el botón Cargar certificado/cadena de certificado.
- En la nueva ventana, comience a cargar el certificado raíz desde el paso 1. Cargarlo a tomcat-trust.



- Haga clic en el botón Upload y, a continuación, debe ver Success: Certificate Uploaded. Ignore el mensaje que le solicita que reinicie Tomcat por ahora.
- Cargue el mismo archivo raíz ahora con CallManager-trust para el propósito del certificado.
- Repita los pasos anteriores (carga en tomcat-trust y CallManager-trust) para todos los certificados intermedios en uso en Expressway-C.

Paso 3. Reinicie los servicios necesarios en CUCM

Es necesario reiniciar estos servicios en cada nodo de CUCM del clúster de CUCM:

- CallManager de Cisco
- Cisco TFTP
- Tomcat de Cisco

Cisco CallManager y Cisco TFTP se pueden reiniciar desde las páginas de Serviciabilidad de Cisco Unified de CUCM:

- Inicie sesión en la página Serviciabilidad de Cisco Unified del publicador de CUCM.
- Vaya a Herramientas > Centro de control - Servicios de funciones.
- Elija Publisher como servidor.
- Elija el servicio Cisco CallManager, y haga clic en el botón Restart.
- Después de reiniciar el servicio Cisco CallManager, elija el servicio Cisco TFTP y haga clic en el botón Restart.

Cisco Tomcat solo se puede reiniciar desde CLI:

- Abra una conexión de línea de comandos con el publicador de CUCM.
- Utilice el comando utils service restart Cisco Tomcat.

Información Relacionada

Asistencia técnica y documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).