Genere un certificado de Expressway nuevo con la información del certificado actual.

Contenido

Introducción

Este documento describe cómo generar una nueva solicitud de firma de certificado (CSR) con la información del certificado de Expressway existente.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Atributos de certificado
- Expressway o Video Communication Server (VCS)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

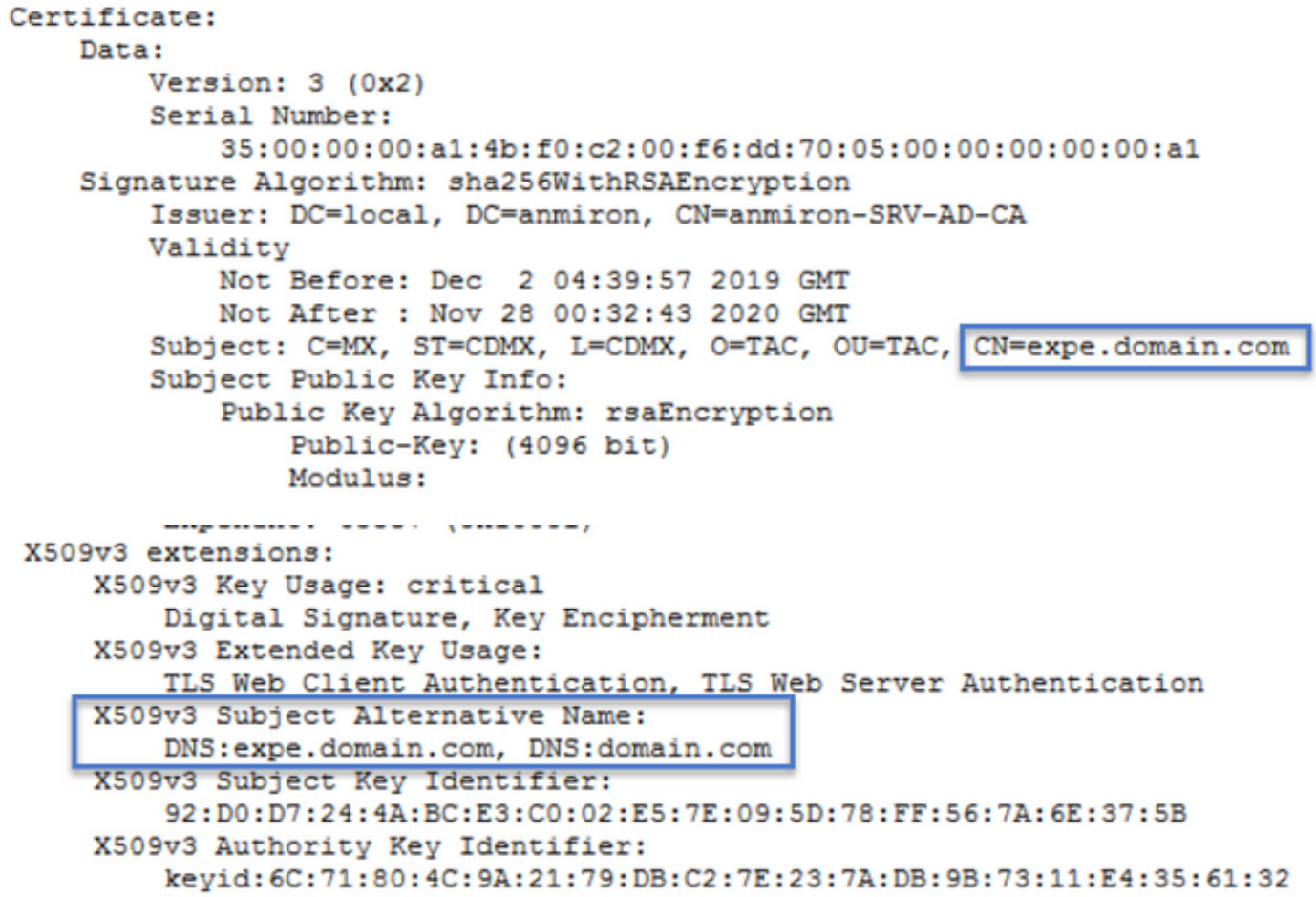
Configurar

Paso 1. Localice la información actual del certificado.

Para obtener la información contenida en el certificado actual, navegue hasta **Mantenimiento > Seguridad > Certificado de servidor** en la interfaz gráfica de usuario (GUI) de Expressway.

Localice la sección **Datos del certificado del servidor** y seleccione **Mostrar (descodificado)**.

Busque la información en el **Nombre común (CN)** y **Nombre alternativo del sujeto (SAN)** como se muestra en la imagen:



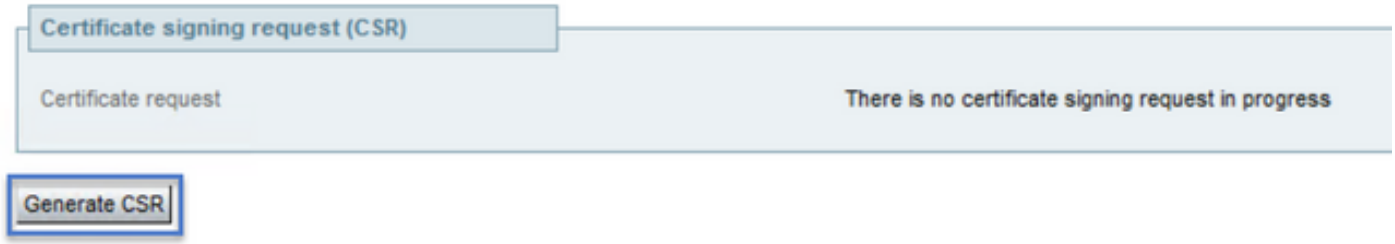
Ahora que conoce el CN y la SAN, cópielos para que se puedan agregar al nuevo CSR.

Opcionalmente, puede copiar la información adicional para el certificado que es País (C), Estado (ST), Localidad (L), Organización (O), Unidad organizativa (OU). Esta información está junto a la CN.

Paso 2. Cree una nueva CSR con la información obtenida anteriormente.

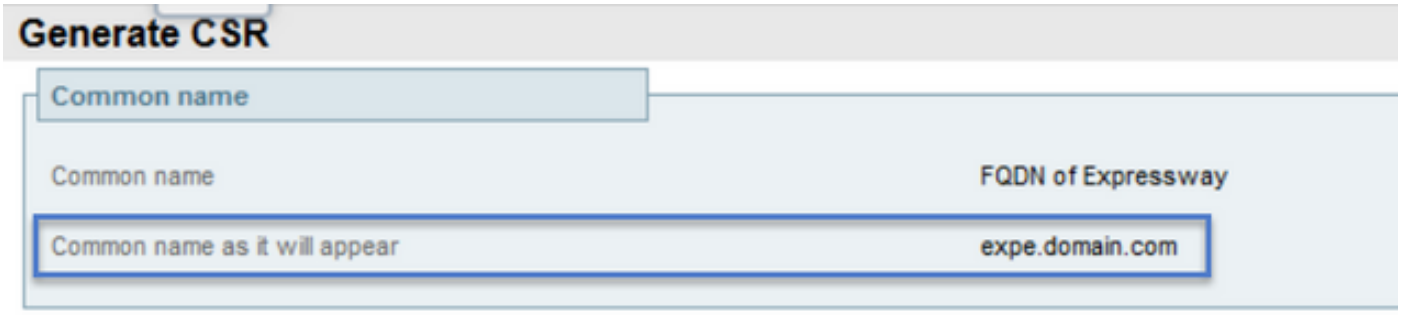
Para crear la CSR, navegue hasta **Mantenimiento > Seguridad > Certificado de servidor**.

Busque la sección **Solicitud de firma de certificado (CSR)** y seleccione **Generar CSR** como se muestra en la imagen:

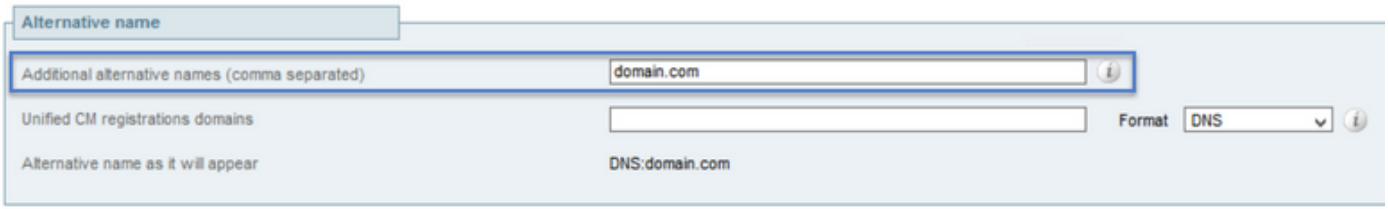


Introduzca los valores recopilados del certificado actual.

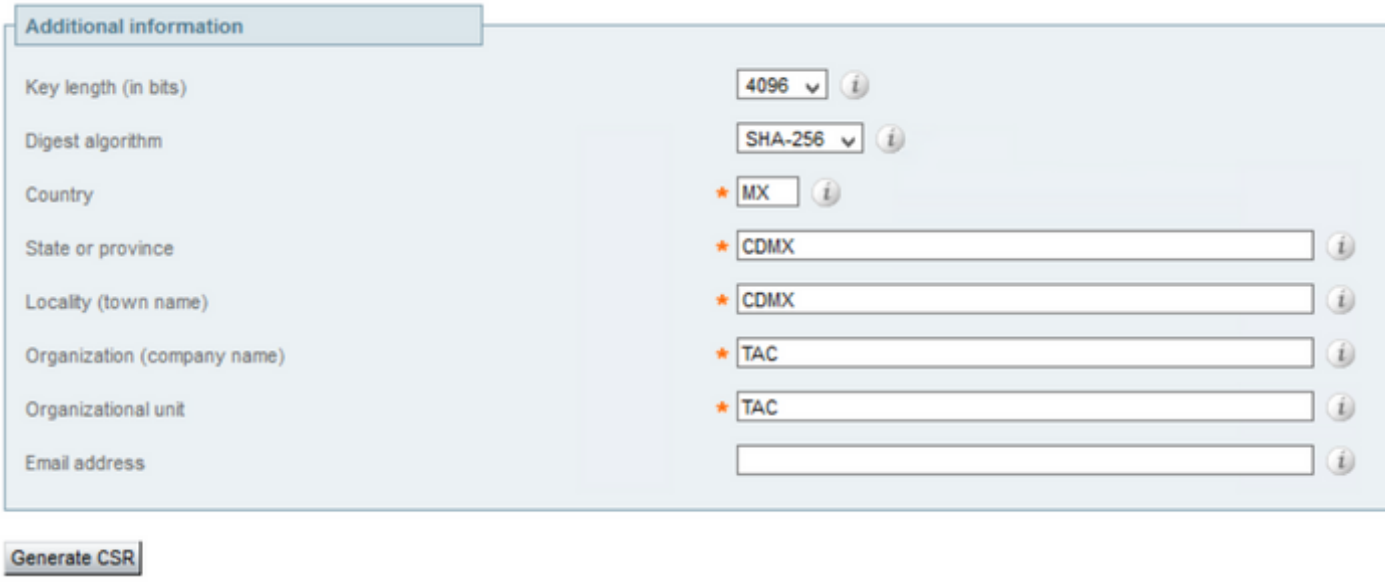
El CN no puede modificarse a menos que sea un clúster. En el caso de un clúster, puede seleccionar el CN para que sea el nombre de dominio completo (FQDN) de Expressway o el FQDN del clúster. En este documento se utiliza un único servidor y, por lo tanto, el CN corresponde a lo que obtuvo del certificado actual, como se muestra en la imagen:



Para las SANs, debe ingresar los valores manualmente en caso de que no se rellenen automáticamente, para hacerlo puede ingresar los valores en los **nombres alternativos adicionales**, si tiene varias SANs deben estar separadas por comas, por ejemplo: ejemplo1.dominio.com, ejemplo2.dominio.com, ejemplo3.dominio.com. Una vez agregadas, las SAN se enumeran en la sección **Nombre alternativo, ya que** aparecerá, como se muestra en la imagen:



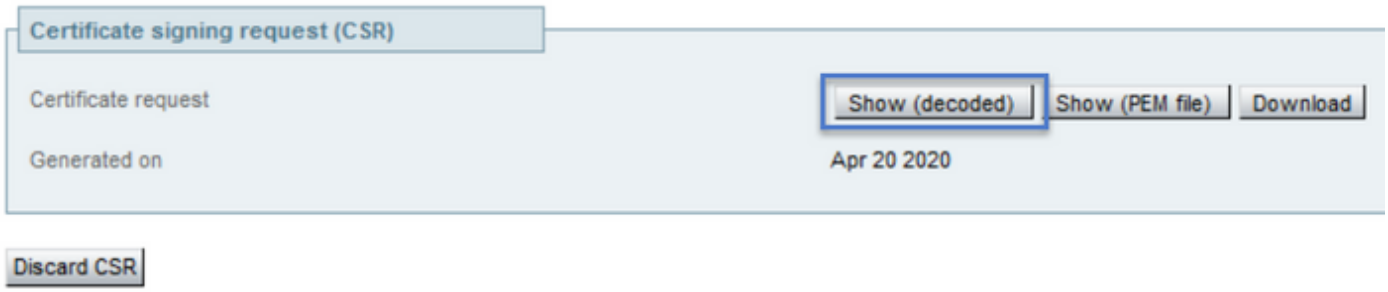
La **información adicional** es obligatoria, si no se rellena automáticamente o hay que cambiarla, debe introducirse manualmente como se muestra en la imagen:



Una vez finalizado, seleccione **Generar CSR**.

Paso 3. Verifique y descargue la nueva CSR.

Ahora que se genera la CSR, puede seleccionar **Mostrar (decodificado)** en la sección **Solicitud de firma de certificado (CSR)** para verificar que todas las SAN estén presentes, como se muestra en la imagen:



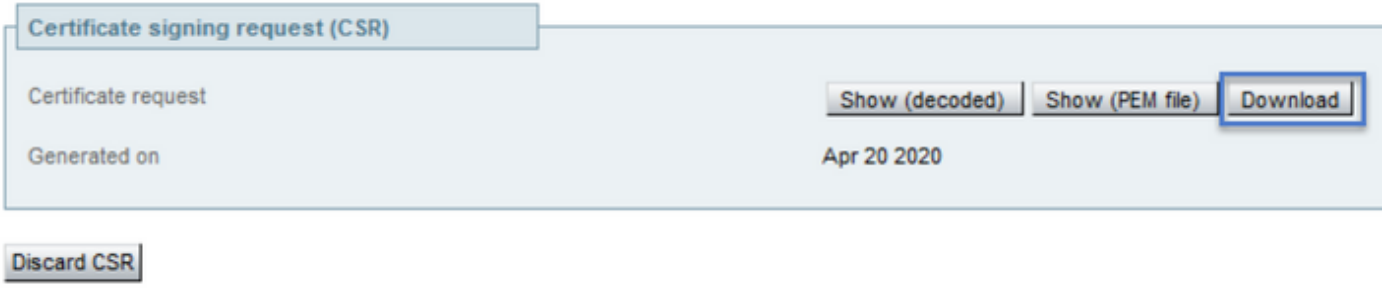
En la nueva ventana, busque el **CN** y el **nombre alternativo del sujeto** como se muestra en la imagen:

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: OU=TAC, O=TAC, CN=expe.domain.com, ST=CDMX, C=MX, L=CDMX
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
```

La CN siempre se agrega como una SAN automáticamente:

```
        X509v3 Extended Key Usage:
            TLS Web Server Authentication, TLS Web Client Authentication
        X509v3 Subject Alternative Name:
            DNS:expe.domain.com, DNS:domain.com
Signature Algorithm: sha256WithRSAEncryption
```

Ahora que se ha verificado el CSR, puede cerrar la nueva ventana y seleccionar **Descargar (descodificado)** en la sección **Solicitud de firma de certificado (CSR)** como se muestra en la imagen:

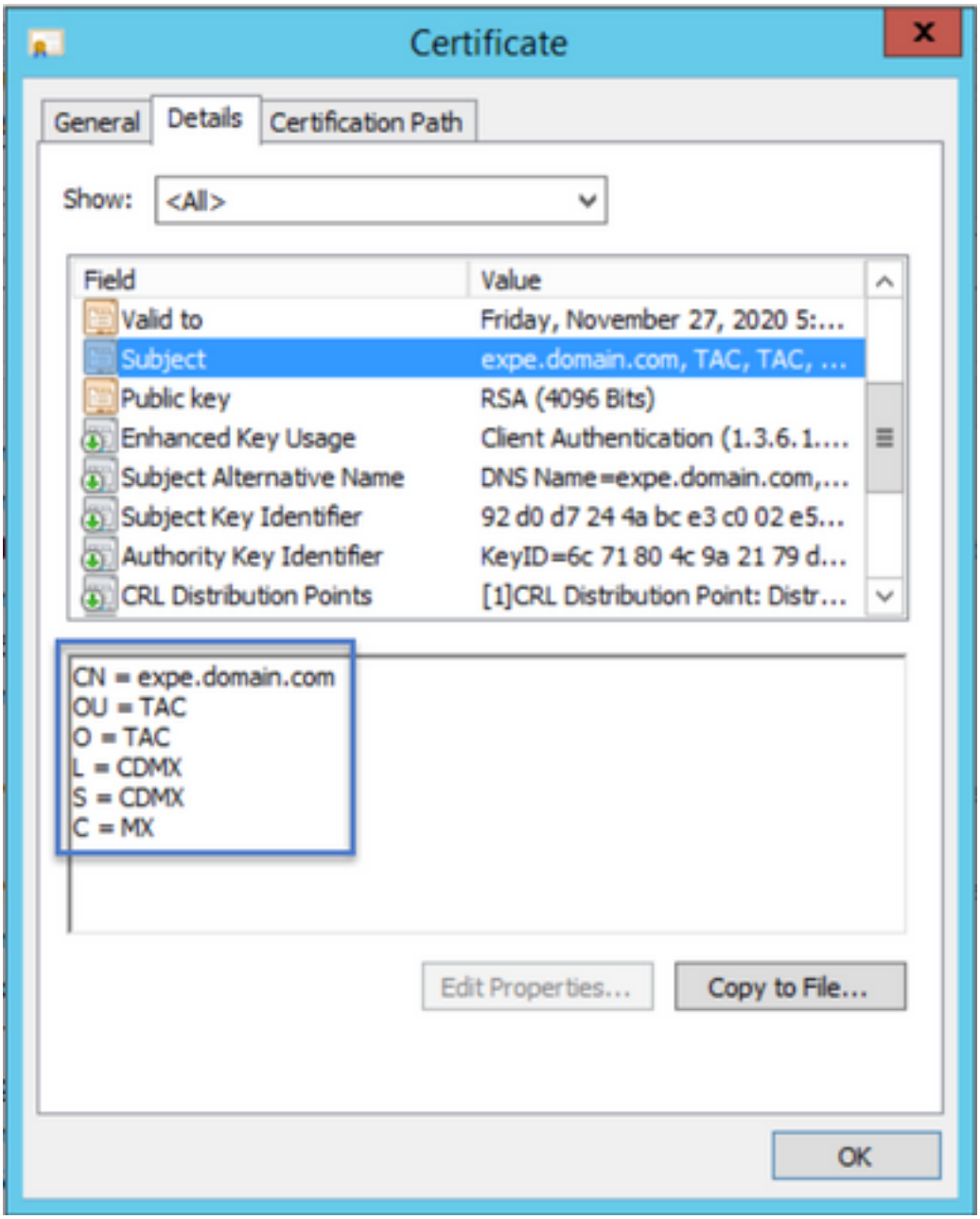


Después de descargarlo, puede enviar la nueva CSR a su Autoridad de Certificación (CA) para que la firme.

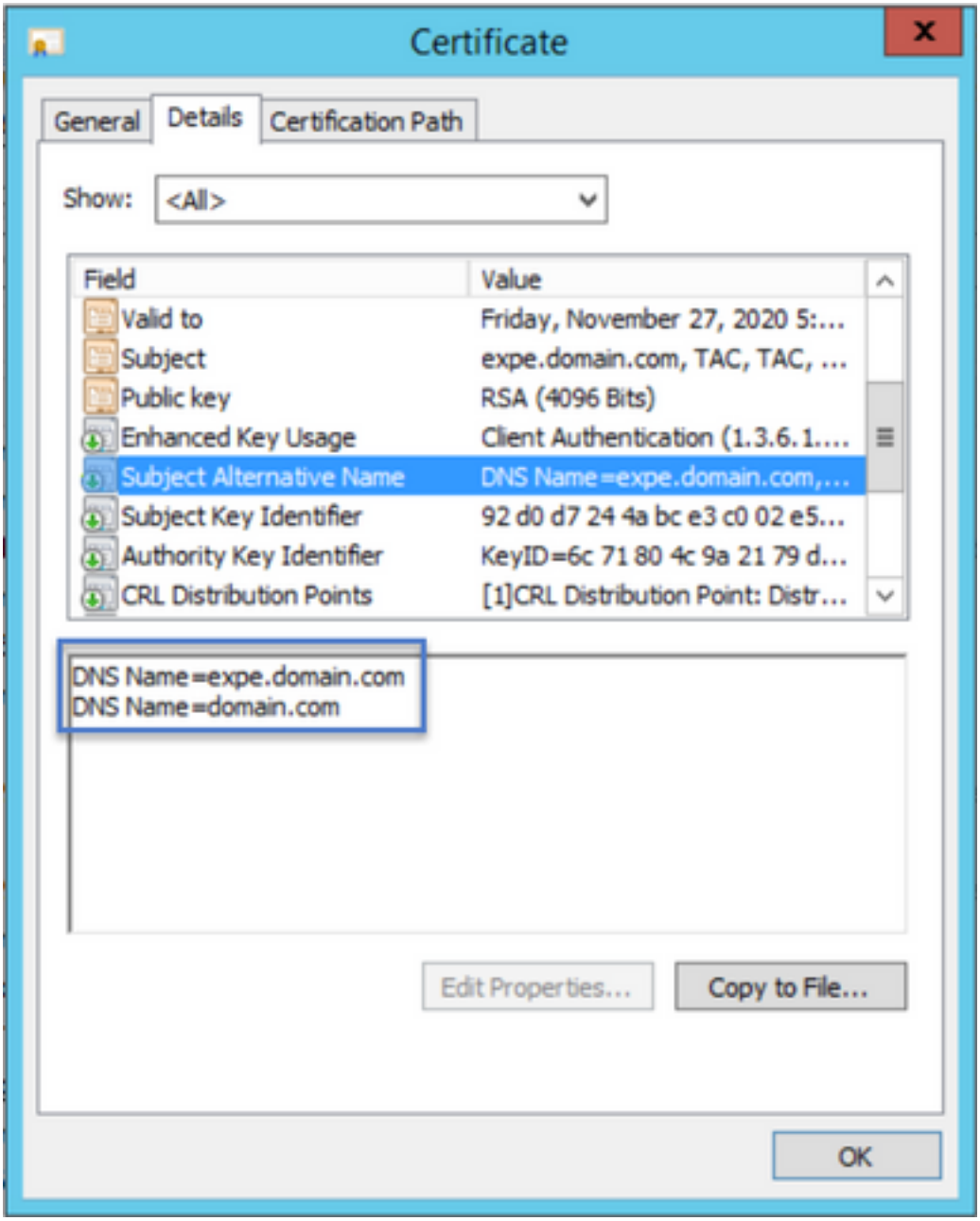
Paso 4. Verifique la información contenida en el nuevo certificado.

Una vez que el nuevo certificado se devuelve de la CA, puede verificar si todas las SAN están presentes en el certificado. Para ello, puede abrir el certificado y buscar los atributos de SAN. En este documento se utiliza un equipo de Windows para ver los atributos, este no es el único método siempre y cuando pueda abrir o descodificar el certificado para revisar los atributos.

Abra el certificado y navegue hasta la pestaña **Detalles** y busque **Asunto**, debe contener la CN y la Información Adicional como se muestra en la imagen:



También busque la sección **Nombre alternativo del asunto**, debe contener las SAN que ingresó en la CSR como se muestra en la imagen:



Si todas las SAN que ha introducido en la CSR no están presentes en el nuevo certificado, póngase en contacto con su CA para ver si se permiten SAN adicionales para su certificado.

Paso 5. Cargue los nuevos certificados de CA en el almacén de confianza de servidores si procede.

Si la CA es la misma que firmó el certificado antiguo de Expressway, puede descartar este paso. Si se trata de una CA diferente, debe cargar los nuevos certificados de CA en la lista de CA de confianza en cada uno de los servidores de Expressway. Si tiene zonas de seguridad de la capa de transporte (TLS) entre Expressway, por ejemplo entre Expressway-C y Expressway-E, debe cargar las nuevas CA en ambos servidores para que puedan confiar entre sí.

Para hacerlo, puede cargar sus certificados de CA uno por uno. Vaya a **Mantenimiento > Seguridad > Certificados CA de confianza** en Expressway.

1. Seleccione **Examinar.**
2. En la nueva página, seleccione el certificado de CA.
3. Seleccione **Agregar certificado de CA.**

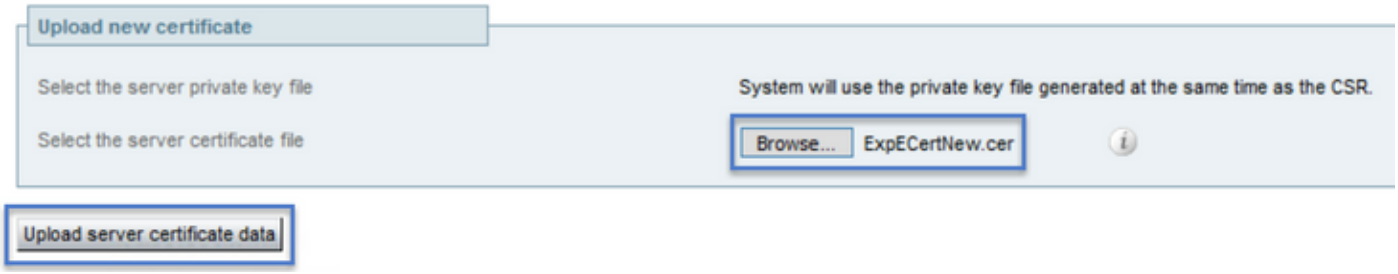
Este procedimiento debe realizarse para cada certificado de CA en la cadena de certificados (raíz e intermedio) y debe hacerse en todos los servidores de Expressway incluso si están agrupados.

Paso 6. Cargue el nuevo certificado en el servidor de Expressway.

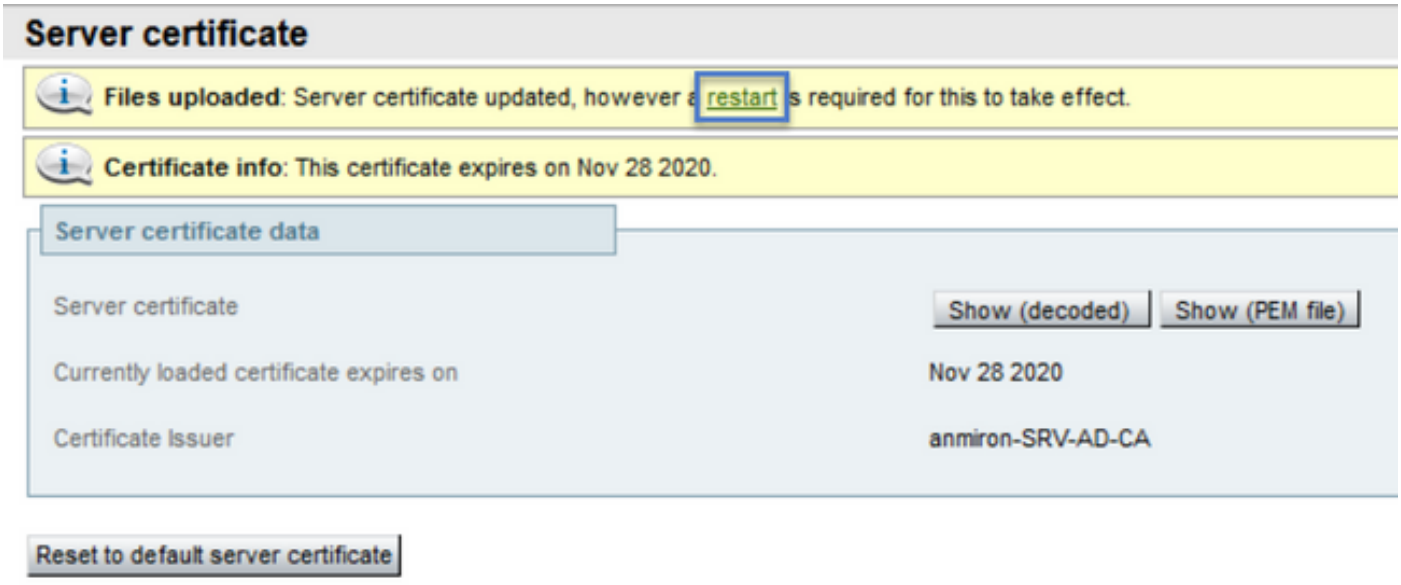
Si toda la información en el nuevo certificado es correcta, para cargar el nuevo certificado navegue a: **Mantenimiento > Seguridad > Certificado de servidor.**

Localice la sección **Cargar certificado nuevo** como se muestra en la imagen:

1. Seleccione **Browse** en la sección **Select the server certificate file** .
2. Seleccione el nuevo certificado.
3. Seleccione **Cargar datos del certificado de servidor.**



Si Expressway acepta el nuevo certificado, Expressway solicita un reinicio para aplicar los cambios y el mensaje muestra la nueva fecha de vencimiento del certificado, como se muestra en la imagen:



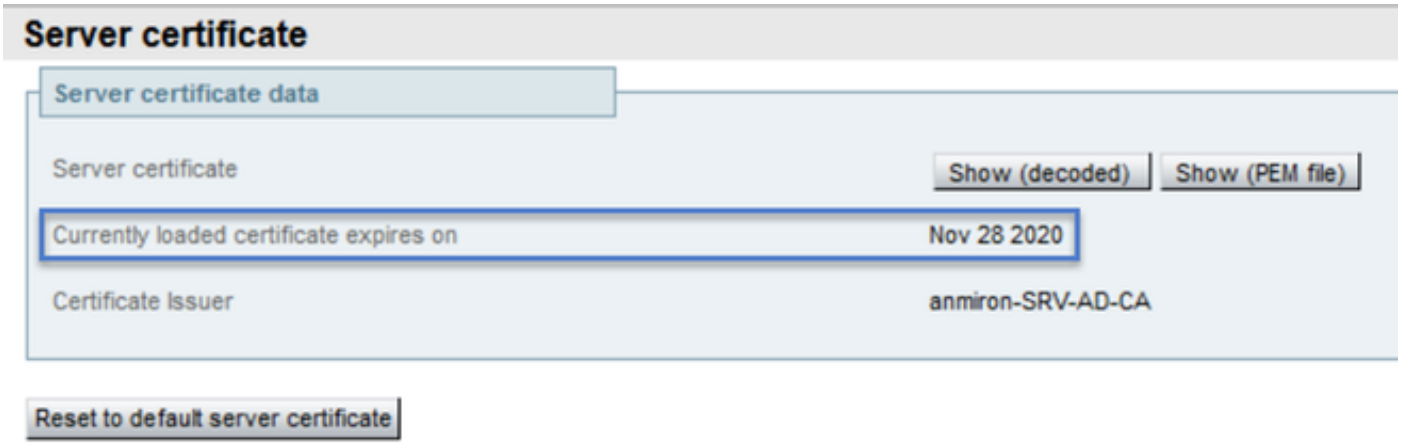
Para reiniciar Expressway seleccione **reinicio**.

Verificación

Una vez que el servidor haya recuperado el nuevo certificado debe haber sido instalado, puede navegar a: **Mantenimiento > Seguridad > Certificado de servidor** para confirmar.

Localice los **datos del certificado del servidor** y busque la sección **El certificado cargado actualmente caduca en**, muestra la nueva fecha de vencimiento del certificado como se muestra

en la imagen:



Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.