Renovar certificado de Expressway

Contenido

Introducción

Este documento describe el proceso de renovación del certificado de Expressway/Video Communication Server (VCS).

La información de este documento se aplica tanto a Expressway como a VCS. El documento hace referencia a Expressway, pero se puede intercambiar con VCS.

> **Nota:** Si bien este documento está diseñado para ayudarlo con el proceso de renovación de certificados, es una buena idea consultar también la Guía de creación y uso de certificados de Cisco Expressway para su versión.

Antecedentes

Siempre que se renueve un certificado, hay dos puntos principales que deben tenerse en cuenta para asegurarse de que el sistema continúa funcionando correctamente después de instalar el nuevo certificado:

1. Los atributos del nuevo certificado deben coincidir con los del certificado antiguo (principalmente el nombre alternativo del sujeto y el uso de clave ampliada)

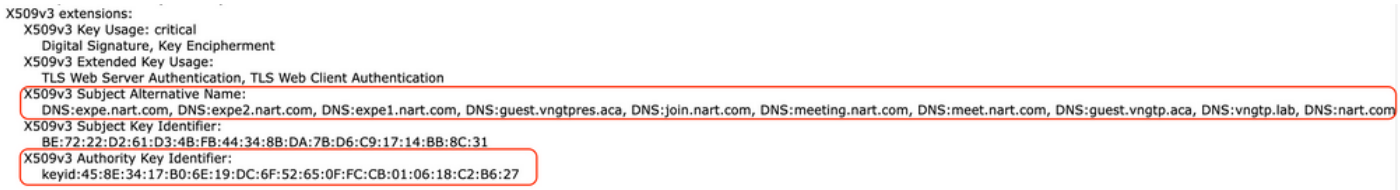
2. La CA (entidad de certificación) que se utilizará para firmar el nuevo certificado debe ser de confianza para otros servidores que se comuniquen directamente con Expressway (por ejemplo, CUCM, Expressway-C, Expressway-E, etc.)

Proceso

A) Obtener información del certificado actual

1. Abra Expressway Webpage **Maintenance > Security > Server certificate > Show decoded.**

2. En la nueva ventana que se abre, copie las extensiones X509v3 "Nombre alternativo del asunto" y "Identificador de clave de autoridad" en un documento del bloc de notas.

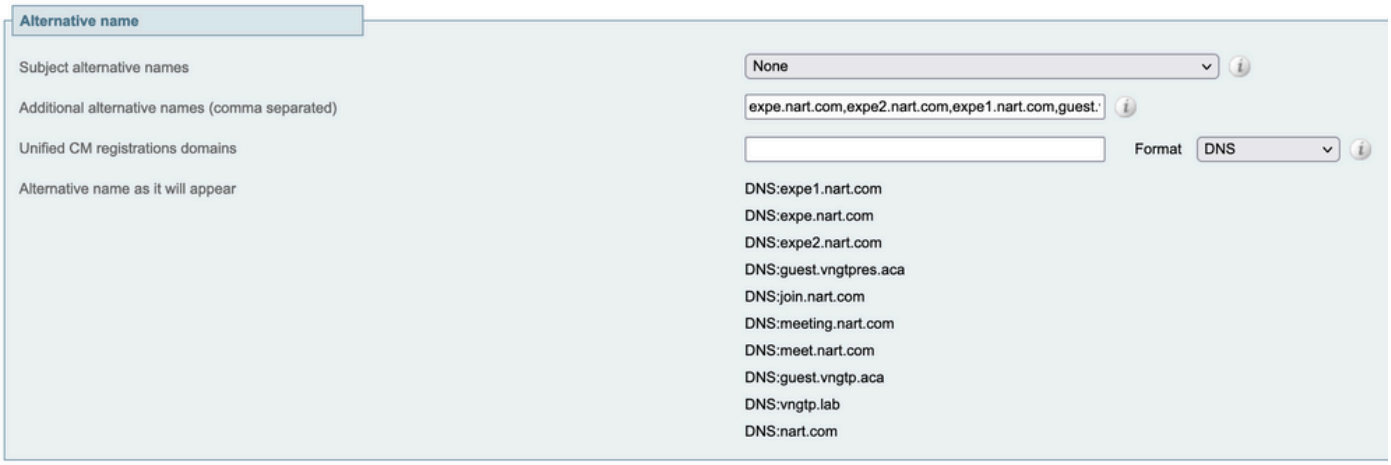


Ventana "Mostrar certificado descodificado"

B) Generar la CSR (Solicitud de firma de certificado) y enviarla a la CA (Autoridad de certificación) para su firma.

1. En **Mantenimiento** de páginas web de Expressway **> Seguridad > Certificado de servidor > Generar CSR.**

2. En la ventana Generar CSR, en el campo **Nombres alternativos adicionales (separados por comas)**, rellene todos los valores de "Nombres alternativos de asunto" que guardamos en la sección A, y asegúrese de eliminar "DNS:" y separar la lista con comas, consulte la imagen (Junto a "Nombre alternativo tal y como aparecerá" puede ver una lista de todas las SAN que se utilizarán en el certificado):



Generar entradas de CSR SAN

3. Rellene el resto de la información en la sección **Información Adicional** como país, empresa, estado, etc. y haga clic en **Generar CSR.**

4. Una vez que haya generado el CSR, la página **Mantenimiento > Seguridad > Certificado de servidor** muestra una opción para **Descartar CSR** y **Descargar**, debe elegir **Descargar** y enviar el CSR a la CA para la firma.

> **Nota:** Asegúrese de no **Descartar CSR** antes de instalar el nuevo certificado; si se realizó **Descartar CSR** y luego se intenta instalar un certificado firmado con el CSR que se descartó, la instalación del certificado falla.

C) Compruebe la lista SAN y el atributo de uso de claves extendido/mejorado en el nuevo certificado

Abra el certificado recién firmado en el administrador de certificados de Windows y compruebe si hay:

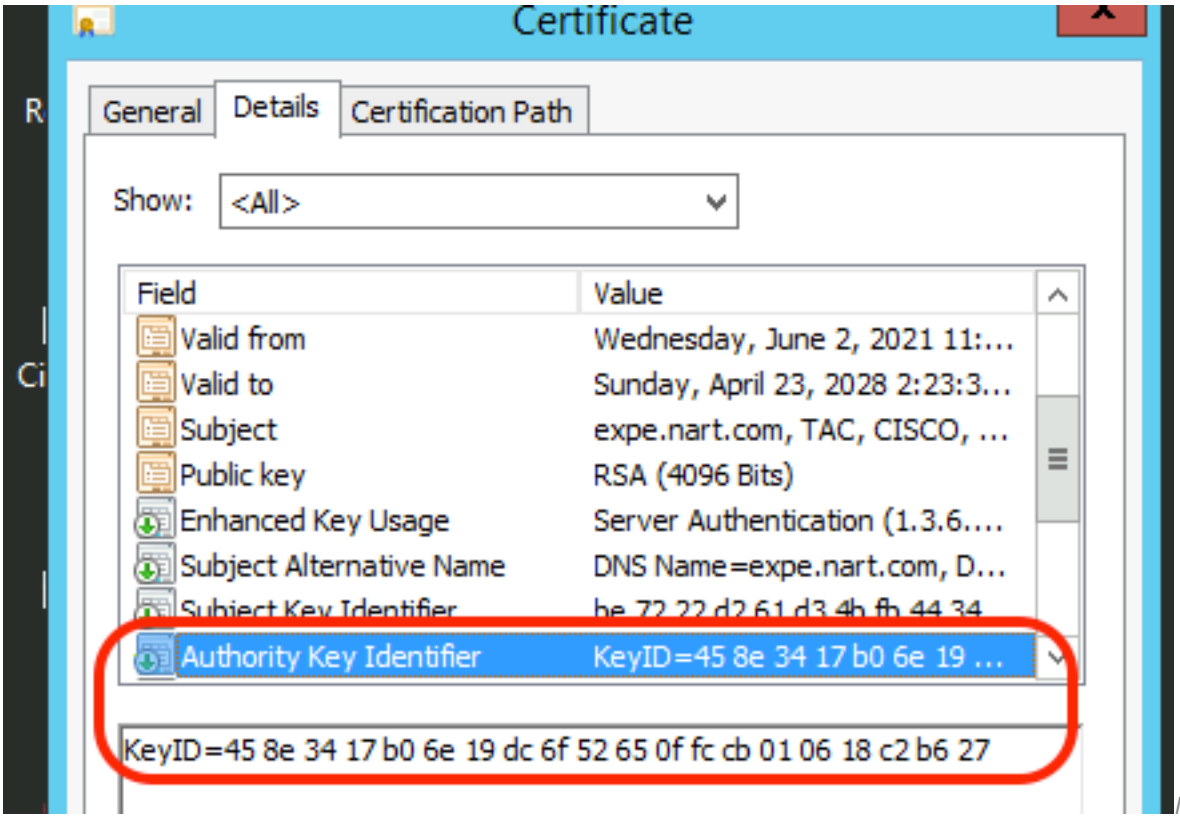
1. La lista de SAN coincide con la lista de SAN que guardamos en la sección A que usamos para generar la CSR.

2. El atributo "Extended/Enhanced key usage" debe incluir "Client Authentication" y "Server Authentication".

> **Nota:** Si el certificado tiene la extensión .pem, cámbiele el nombre a .cer o .crt para poder abrirlo con el Administrador de certificados de Windows. Una vez abierto el certificado con el Administrador de certificados de Windows, puede ir a la pestaña **Detalles > Copiar en archivo** y exportarlo como un archivo codificado Base64, un archivo codificado base64 normalmente tiene "-----BEGIN CERTIFICATE-----" en la parte superior y "-----END CERTIFICATE-----" en la parte inferior cuando se abre en un editor de texto

D) Compruebe si la CA que firmó el nuevo certificado es la misma que la CA que firmó el antiguo certificado

Abra el certificado recién firmado en el administrador de certificados de Windows, copie el valor "Identificador de clave de autoridad" y compárelo con el valor "Identificador de clave de autoridad" que guardamos en la sección A.



Nuevo certificado abierto con el Administrador de certificados de Windows

Si ambos valores son iguales, significa que se utilizó la misma CA para firmar el nuevo certificado que la que se utilizó para firmar el antiguo, y puede continuar con la sección E para cargar el nuevo certificado.

Si los valores son diferentes, esto significa que la CA utilizada para firmar el nuevo certificado es diferente de la CA utilizada para firmar el antiguo certificado, y los pasos que debe seguir antes

de continuar con la sección E son:

1. Obtenga todos los certificados de CA intermedia (si los hubiera) y el certificado de CA raíz.

2. Vaya a **Mantenimiento > Seguridad > Certificado de CA de confianza** , haga clic en **Examinar** y busque el certificado de CA intermedio en su computadora y cárguelo. Haga lo mismo con cualquier otro certificado de CA intermedio y el certificado de CA raíz.

3. Haga lo mismo en cualquier Expressway-E (si el certificado que se va a renovar es un certificado de Expressway-C) que se conecte a este servidor o en cualquier Expressway-C (si el certificado que se va a renovar es un certificado de Expressway-E) que se conecte a este servidor.

4. Si el certificado que se va a renovar es un certificado de Expressway-C y tiene MRA o zonas seguras para CUCM, debe asegurarse de que CUCM confía en la nueva CA raíz e intermedia y cargar los certificados de CA raíz e intermedia en los almacenes de confianza de CUCM tomcat y callmanager y, a continuación, reiniciar los servicios relevantes en CUCM.

E) Instalar el nuevo certificado

Una vez que se hayan verificado todos los puntos anteriores, ahora puede instalar el nuevo certificado en Expressway desde **Mantenimiento > Seguridad > Certificado de servidor**, haga clic en **Examinar** y seleccione el nuevo archivo de certificado de su computadora y cárguelo.

Debe reiniciar Expressway después de instalar un nuevo certificado.

> **Nota:** Asegúrese de que el certificado que carga en Expressway desde **Mantenimiento > Seguridad > Certificado de servidor** contenga solamente el certificado de servidor de Expressway y NO la cadena de certificados completa y asegúrese de que sea un certificado Base64

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).