Renovar certificado de Expressway

Contenido

Introducción

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

Antecedentes

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

Nota: aunque este documento está diseñado para ayudarle 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.

Siempre que se renueve un certificado, deben tenerse en cuenta dos puntos principales para verificar que el sistema sigue 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).

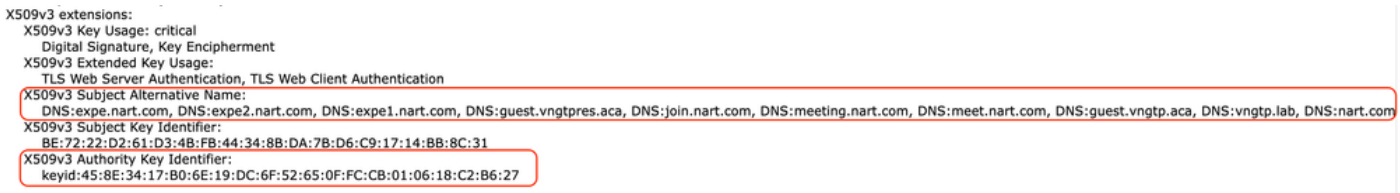
2. La CA (entidad de certificación) que firma el nuevo certificado debe ser de confianza para otros servidores que se comuniquen directamente con Expressway (por ejemplo, CUCM, Expressway-C, Expressway-E,...).

Proceso

A) Obtener información del certificado actual

1. Abra Expressway Web Page Maintenance > Security > Server certificate > Show decoded.

2. En la nueva ventana que se abre, copie el nombre alternativo del sujeto y las extensiones del identificador de clave de autoridad X509v3 en un documento del bloc de notas.



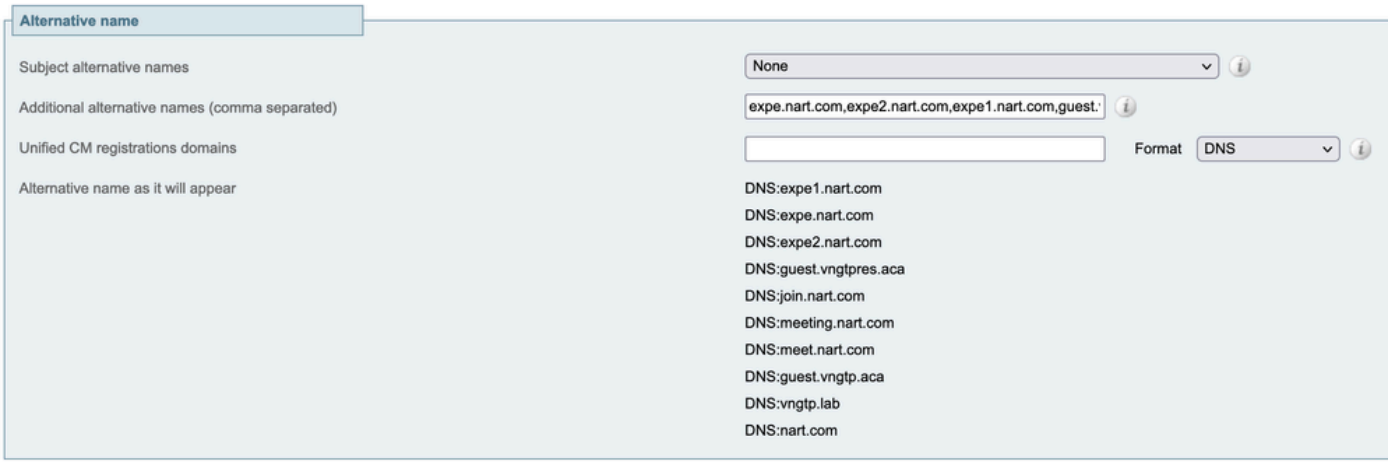
Ventana de certificado "Mostrar descodificado"

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), introduzca todos los valores de Nombres alternativos de asunto que se guardaron en la sección A y elimine DNS: y separe la lista con comas.

En esta imagen, junto a Nombre alternativo tal como aparece, hay una lista de todas las SAN que se utilizarán en el certificado):



Generar entradas de CSR SAN

3. Introduzca el resto de la información en la sección Información adicional (como país, empresa, estado, etc.) y haga clic en Generar CSR.

4. Después de generar el CSR, la página Mantenimiento > Seguridad > Certificado de servidor muestra una opción para Descartar CSR y Descargar. Elija Download y envíe el CSR a la CA para la firma.

Nota: no descarte CSR antes de instalar el nuevo certificado. Si se realizó Discard 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:

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

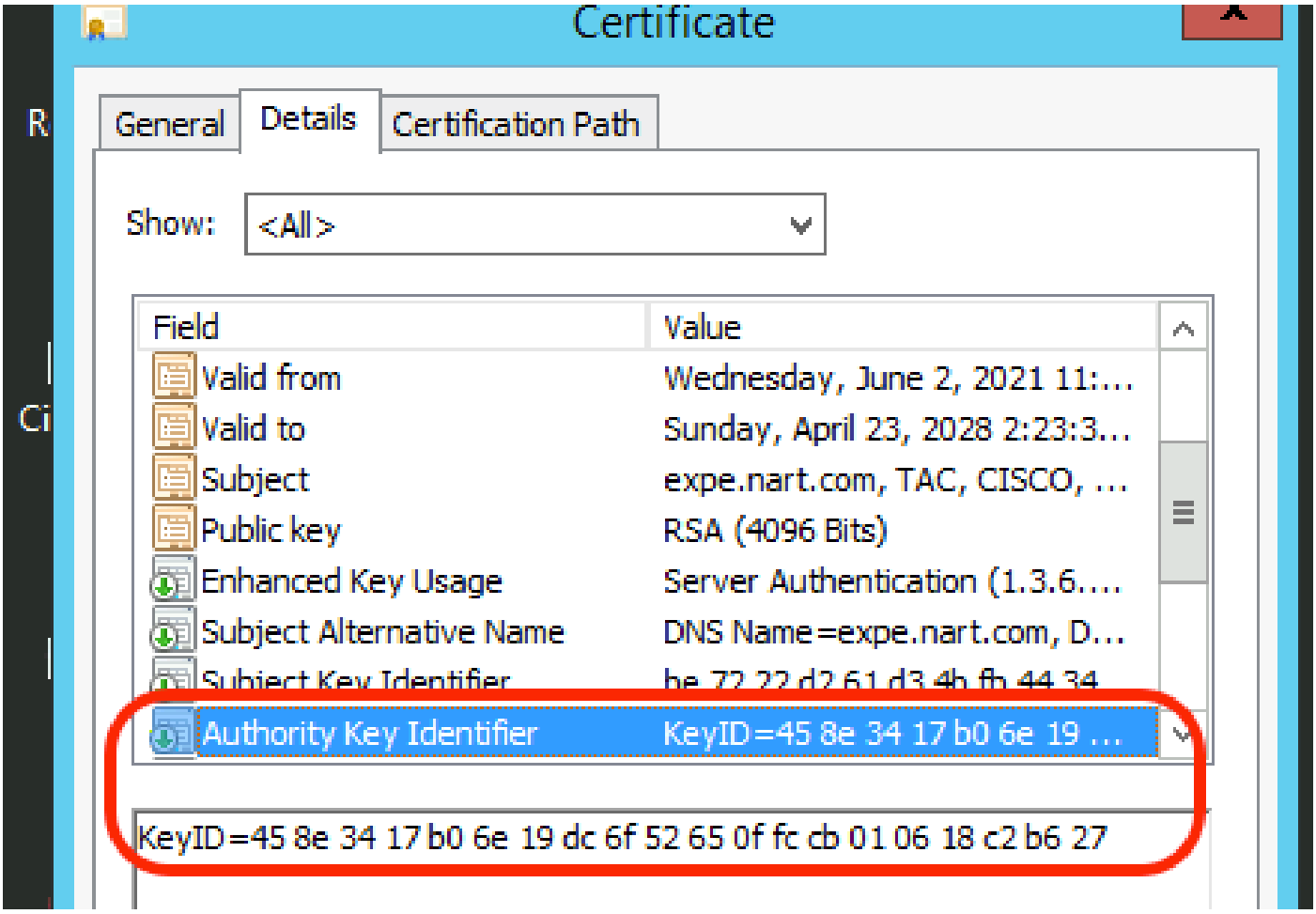
2. El atributo "Uso de clave extendido/mejorado" debe incluir tanto Autenticación de cliente como Autenticación de servidor.

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 y 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 certificado antiguo, y los pasos a 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

- Verifique que CUCM confíe en la nueva CA raíz e intermedia.

- Cargue los certificados de CA raíz e intermedia en los almacenes de confianza de CUCM tomcat y callmanager.
- Reinicie los servicios relevantes en CUCM.

E) Instalar el nuevo certificado

Una vez verificados todos los puntos anteriores, puede instalar el nuevo certificado en Expressway desde Mantenimiento > Seguridad > Certificado de servidor .

Haga clic en Browse y seleccione el nuevo archivo de certificado de su computadora y cárguelo.

Debe reiniciar Expressway después de instalar un nuevo certificado.

Nota: compruebe que el certificado que se va a cargar en Expressway desde Mantenimiento > Seguridad > Certificado de servidor contiene solo el certificado de servidor de Expressway y no la cadena de certificados completa y compruebe que es un certificado Base64.

Adición de un solo certificado a varias Expressway:

- Cree un único certificado para todo el clúster de expressway-e.
- Cree una CSR que contenga todos los FQDN más las funciones adicionales que utiliza en las autopistas (si es CMS webtc, la url y el dominio de unión, si es MRA, sus registros/dominios de inicio de sesión)

  Ejemplo:
  Exwycluster.domain
  Exway1.domain
  Exway2.domain
  Exway3.domain
  Exway4.domain
  Funciones adicionales (dominios o URL de CMS)

- Después de que el CSR está hecho, usted puede extraer la clave privada de este CSR usando un programa SFTP (le recomiendo WinSCP, lo usamos mucho)
- Abra WinSCP y conéctese a Expressway-e que creó el CSR
- Vaya a tandberg/persistent/certs/ CSR o a la solicitud de firma de certificado (puede mostrarse así como pendiente)
- Copie la clave privada de expressway-e en el escritorio,
- Una vez hecho esto, podemos utilizar el mismo certificado para todos sus 4 nodos.

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).