Gestiona certificados de seguridad

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/es-es/active-iq-unified-manager-918/config/task_view_https_security_certificate_ocf.html on November 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestiona certificados de seguridad . . . 1
- Ver el certificado de seguridad HTTPS en Active IQ Unified Manager . . . 1
- Descargar una solicitud de firma de certificado HTTPS en Active IQ Unified Manager . . . 1
- Instala un certificado HTTPS firmado por una autoridad de certificación (CA) en Active IQ Unified Manager . . . 2
  - Ejemplo de cadena de certificados . . . 2
- Conoce los certificados HTTPS generados mediante herramientas externas en Active IQ Unified Manager Unified Manager . . . 3
  - Formato para cargar un certificado con un par de claves EC . . . 3
  - Formato para cargar un certificado con un par de claves RSA . . . 4
  - Comprobaciones durante la carga de certificados generados externamente . . . 4
- Descripciones de las páginas para la gestión de certificados . . . 5
  - Conoce la página de certificados HTTPS en Active IQ Unified Manager . . . 5
  - Cuadro de diálogo Regenerar un certificado HTTPS en Active IQ Unified Manager . . . 6

Gestiona certificados de seguridad

Ver el certificado de seguridad HTTPS en Active IQ Unified Manager

Puedes comparar los datos del certificado HTTPS con el certificado recuperado en tu navegador para asegurarte de que la conexión cifrada de tu navegador con Unified Manager no está siendo interceptada.

Antes de empezar

Debes tener el rol de Operator, Application Administrator o Storage Administrator.

Ver el certificado te permite comprobar el contenido de un certificado regenerado o ver los nombres alternativos del sujeto (SAN) desde los que puedes acceder a Unified Manager.

Paso

1. En el panel de navegación de la izquierda, haz clic en **General** > **Certificado HTTPS**.

   El certificado HTTPS aparece en la parte superior de la página

Si necesitas consultar información más detallada sobre el certificado de seguridad, además de la que se muestra en la página «HTTPS Certificate», puedes consultar el certificado de conexión en tu navegador.

Descargar una solicitud de firma de certificado HTTPS en Active IQ Unified Manager

Puedes descargar una solicitud de firma de certificado para el certificado de seguridad HTTPS actual, de modo que puedas proporcionar el archivo a una autoridad de certificación para que lo firme. Un certificado firmado por una autoridad de certificación ayuda a prevenir ataques de intermediario y ofrece una mejor protección de seguridad que un certificado autofirmado.

Antes de empezar

Debes tener el rol de Application Administrator.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Certificado HTTPS**.
2. Haz clic en **Descargar solicitud de firma de certificado HTTPS**.
3. Guarda el archivo `<hostname>.csr`.

Puedes enviar el archivo a una autoridad de certificación para que lo firme y, a continuación, instalar el certificado firmado.

Instala un certificado HTTPS firmado por una autoridad de certificación (CA) en Active IQ Unified Manager

Puedes cargar e instalar un certificado de seguridad una vez que una autoridad de certificación lo haya firmado y devuelto. El archivo que cargues e instales debe ser una versión firmada del certificado autofirmado existente. Un certificado firmado por una autoridad de certificación ayuda a prevenir los ataques man-in-the-middle y ofrece una mayor protección de seguridad que un certificado autofirmado.

*Qué. Antes de empezar

Debes haber realizado las siguientes acciones:

- Descargué el archivo de solicitud de firma de certificado e hice que una autoridad de certificación lo firmara
- Se guardó la cadena de certificados en formato PEM
- Se incluyeron todos los certificados de la cadena, desde el certificado del servidor de Unified Manager hasta el certificado de firma raíz, incluidos los certificados intermedios presentes

Debes tener el rol de Application Administrator.

Si la validez del certificado para el que se ha creado una CSR es superior a 397 días, la CA reducirá dicha validez a 397 días antes de firmar y devolver el certificado

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Certificado HTTPS**.
2. Haz clic en **Install HTTPS Certificate**.
3. En el cuadro de diálogo que aparece, haz clic en **Seleccionar archivo…** para localizar el archivo que quieres cargar.
4. Selecciona el archivo y luego haz clic en **Instalar** para instalarlo.

   Para más información, consulta "Instalación de un certificado HTTPS generado con herramientas externas".

Ejemplo de cadena de certificados

El siguiente ejemplo muestra cómo podría verse el archivo de la cadena de certificados:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Conoce los certificados HTTPS generados mediante herramientas externas en Active IQ Unified Manager Unified Manager

Puedes instalar certificados autofirmados o firmados por una autoridad de certificación (CA), generados con una herramienta externa como OpenSSL, BoringSSL, LetsEncrypt.

Debes cargar la clave privada junto con la cadena de certificados, ya que estos certificados son un par de claves pública y privada generado externamente. Los algoritmos permitidos para los pares de claves son “RSA” y “EC”. La opción **Install HTTPS Certificate** está disponible en la página HTTPS Certificates en la sección General. El archivo que subas debe tener el siguiente formato de entrada.

1. Clave privada del servidor que pertenece al host de Active IQ Unified Manager
2. Certificado del servidor que coincide con la clave privada
3. Certificado de las CA en orden inverso hasta la raíz, que se usan para firmar el certificado anterior

Formato para cargar un certificado con un par de claves EC

Las curvas permitidas son “prime256v1” y “secp384r1”. Ejemplo de certificado con un par EC generado externamente:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Formato para cargar un certificado con un par de claves RSA

Los tamaños de clave permitidos para el par de claves RSA correspondiente al certificado del host son 2048, 3072 y 4096. certificado con un **par de claves RSA** generado externamente:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Una vez subido el certificado, debes reiniciar la instancia de Active IQ Unified Manager para que los cambios surtan efecto.

Comprobaciones durante la carga de certificados generados externamente

El sistema realiza comprobaciones durante la carga de un certificado generado con herramientas externas. Si alguna de las comprobaciones falla, el certificado se rechaza. También se incluyen comprobaciones de validación para los certificados generados a partir de la CSR dentro del producto y para los certificados generados con herramientas externas.

- La clave privada de la entrada se valida con el certificado de host de la entrada.
- El nombre común (CN) del certificado del host se compara con el nombre de dominio completo (FQDN) del host.
- El nombre común (CN) del certificado del host no debe estar vacío ni en blanco y no debe establecerse como localhost.
- La fecha de inicio de validez no debe estar en el futuro y la fecha de caducidad del certificado no debe estar en el pasado.
- Si existe una CA intermedia o una CA, la fecha de inicio de validez del certificado no debe estar en el futuro y la fecha de vencimiento de la validez no debe estar en el pasado.

La clave privada en la entrada no debe estar cifrada. Si hay claves privadas cifradas, el sistema las rechazará.

Ejemplo 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
```

```
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Ejemplo 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Ejemplo 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Si falla la instalación del certificado, consulta el artículo de la base de conocimientos (KB): "ActiveIQ Unified Manager no consigue instalar un certificado generado externamente"

Descripciones de las páginas para la gestión de certificados

Conoce la página de certificados HTTPS en Active IQ Unified Manager

La página «Certificado HTTPS» te permite consultar el certificado de seguridad actual, descargar una solicitud de firma de certificado, generar un nuevo certificado HTTPS autofirmado o instalar un nuevo certificado HTTPS.

Si no has generado un nuevo certificado HTTPS autofirmado, el certificado que aparece en esta página es el que se generó durante la instalación.

Botones de comando

Los botones de comando te permiten realizar las siguientes operaciones:

- **Descargar solicitud de firma de certificado HTTPS**

  Descarga una solicitud de certificación para el certificado HTTPS actualmente instalado. Tu navegador te pedirá que guardes el archivo <hostname>.csr para que puedas enviarlo a una autoridad de certificación para que lo firme.

- **Instalar un certificado HTTPS**

  Te permite cargar e instalar un certificado de seguridad una vez que una autoridad de certificación lo haya firmado y devuelto. El nuevo certificado entra en vigor después de reiniciar el servidor de gestión.

- **Regenerar certificado HTTPS**

  Te permite generar un nuevo certificado HTTPS autofirmado, que sustituye al certificado de seguridad actual. El nuevo certificado entrará en vigor tras reiniciar Unified Manager.

Cuadro de diálogo Regenerar un certificado HTTPS en Active IQ Unified Manager

El cuadro de diálogo «Regenerar certificado HTTPS» te permite personalizar la información de seguridad y a continuación generar un nuevo certificado HTTPS con dicha información.

En esta página aparece la información actual del certificado.

Las opciones “Regenerate Using Current Certificate Attributes” y “Update the Current Certificate Attributes” te permiten regenerar el certificado con la información actual o generar un certificado con información nueva.

- **Nombre común**

  Obligatorio. El nombre de dominio completo (FQDN) que deseas proteger.

  En las configuraciones de alta disponibilidad de Unified Manager, utiliza la dirección IP virtual.

- **Correo electrónico**

  Opcional. Una dirección de correo electrónico para contactar con tu organización; normalmente la dirección de correo electrónico del administrador de certificados o del departamento de TI.

- **Empresa**

  Opcional. Normalmente el nombre legal de tu empresa.

- **Departamento**

  Opcional. El nombre del departamento de tu empresa.

- **Ciudad**

  Opcional. La ciudad en la que se encuentra tu empresa.

- **Estado**

  Opcional. El estado o la provincia donde se encuentra tu empresa, sin abreviaturas.

- **País**

  Opcional. El país donde se encuentra tu empresa. Suele ser un código ISO de dos letras del país.

- **Nombres alternativos**

  Obligatorio. Nombres de dominio adicionales, distintos del principal, que puedes usar para acceder a este servidor además de localhost u otras direcciones de red existentes. Separa cada nombre alternativo con una coma.

  Marca la casilla «`Excluir información de identificación local (p. ej., localhost)`» si quieres eliminar la información de identificación local del campo Nombres alternativos del certificado.

Cuando esta casilla está marcada, en el campo Nombres alternativos solo se usa lo que introduzcas en el campo. Si se deja en blanco, el certificado resultante no tendrá ningún campo Nombres alternativos.

- **TAMAÑO DE LA CLAVE (algoritmo de la clave: RSA)**

  El algoritmo de clave está configurado en RSA. Puedes seleccionar uno de estos tamaños de clave: 2048, 3072 o 4096 bits. El tamaño de clave predeterminado está configurado en 2048 bits.

- **PERÍODO DE VALIDEZ**

  El periodo de validez predeterminado es de 397 días. Si has actualizado desde una versión anterior, es posible que veas que la validez del certificado anterior no ha cambiado.

Para obtener más información, consulta "Generar certificados HTTPS".

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.