Gestiona la configuración de la autenticación SAML

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/concept_manage_saml_authentication_settings_um.html on November 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestiona la configuración de la autenticación SAML . . . 1
- Habilita la autenticación SAML en Active IQ Unified Manager . . . 1
- Usa un proveedor de identidad en Active IQ Unified Manager . . . 1
  - Estándares de cifrado compatibles . . . 1
  - Proveedores de identidad validados . . . 1
  - Requisitos de configuración de ADFS . . . 1
  - Otros requisitos de configuración . . . 2
- Habilita la autenticación SAML en Active IQ Unified Manager . . . 2
- Cambiar el proveedor de identidad de autenticación SAML en Active IQ Unified Manager . . . 3
- Actualiza la configuración de autenticación SAML después de un cambio en el certificado de seguridad de Active IQ Unified Manager . . . 4
- Desactivar la autenticación SAML en Active IQ Unified Manager . . . 5
- Desactivar la autenticación SAML desde la consola de mantenimiento de Active IQ Unified Manager . . . 6
- Utiliza la página de autenticación SAML en Active IQ Unified Manager . . . 7

Gestiona la configuración de la autenticación SAML

Habilita la autenticación SAML en Active IQ Unified Manager

Después de configurar los ajustes de autenticación remota, puedes habilitar la autenticación mediante el Lenguaje de Marcado para Confirmaciones de Seguridad (SAML) para que un proveedor de identidades (IdP) seguro autentique a los usuarios remotos antes de que puedan acceder a la interfaz de usuario web de Unified Manager.

Ten en cuenta que, una vez habilitada la autenticación SAML, solo los usuarios remotos tendrán acceso a la interfaz de usuario gráfica de Unified Manager. Los usuarios locales y los usuarios de mantenimiento no podrán acceder a la interfaz de usuario. Esta configuración no afecta a los usuarios que acceden a la consola de mantenimiento.

Usa un proveedor de identidad en Active IQ Unified Manager

Al configurar Unified Manager para que utilice un proveedor de identidad (IdP) con el fin de realizar la autenticación SAML para todos los usuarios remotos, es necesario tener en cuenta algunos ajustes de configuración obligatorios para que la conexión con Unified Manager funcione correctamente.

Debes introducir el URI y los metadatos de Unified Manager en el servidor IdP. Puedes copiar esta información de la página Unified ManagerSAML Authentication. Unified Manager se considera el proveedor de servicios (SP) en el estándar Security Assertion Markup Language (SAML).

Estándares de cifrado compatibles

- Estándar de cifrado avanzado (AES): AES-128 y AES-256
- Algoritmo de hash seguro (SHA): SHA-1 y SHA-256

Proveedores de identidad validados

- Shibboleth
- Servicios de federación de Active Directory (ADFS)

Requisitos de configuración de ADFS

- Debes definir tres reglas de notificación en el siguiente orden, que son necesarias para que Unified Manager analice las respuestas SAML de ADFS para esta entrada de confianza de usuario autenticado.

Regla de reclamación	Valor
SAM-account-name	ID de nombre
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1

Regla de reclamación	Valor
Grupos de tokens — nombre no calificado	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Debes establecer el método de autenticación en “Forms Authentication” o los usuarios podrían recibir un error al cerrar sesión en Unified Manager. Sigue estos pasos:
  a. Abre la consola de administración de ADFS.
  b. Haz clic en la carpeta «Políticas de autenticación» en la vista de árbol de la izquierda.
  c. En Acciones, a la derecha, haz clic en Edit Global Primary Authentication Policy.
  d. Configura el método de autenticación de la intranet como «`Forms Authentication`» en lugar de la opción predeterminada «`Windows Authentication`».
- En algunos casos, el inicio de sesión a través del IdP se rechaza cuando el certificado de seguridad de Unified Manager está firmado por una autoridad de certificación (CA). Existen dos soluciones provisionales para resolver este problema:
  - Sigue las instrucciones que figuran en el enlace para desactivar la comprobación de revocación en el servidor ADFS para la parte de confianza asociada al certificado de CA encadenado:

    "Desactivar la comprobación de revocación por Relying Party Trust"

  - Aloja el servidor CA en el servidor ADFS para firmar la solicitud de certificado del servidor Unified Manager.

Otros requisitos de configuración

- La desviación horaria de Unified Manager está configurada en 5 minutos, por lo que la diferencia horaria entre el servidor IdP y el servidor Unified Manager no puede ser superior a 5 minutos; de lo contrario, la autenticación fallará.

Habilita la autenticación SAML en Active IQ Unified Manager

Puedes habilitar la autenticación mediante Security Assertion Markup Language (SAML) para que un proveedor de identidad (IdP) seguro autentique a los usuarios remotos antes de que puedan acceder a la interfaz de usuario web de Unified Manager.

Antes de empezar

- Debes haber configurado la autenticación remota y haber comprobado que funciona correctamente.
- Debes haber creado al menos un Usuario remoto o un Grupo remoto con el rol de administrador de aplicaciones.
- El proveedor de identidad (IdP) debe ser compatible con Unified Manager y debe estar configurado.
- Debes disponer de la URL del IdP y de los metadatos.
- Debes tener acceso al servidor IdP.

Después de habilitar la autenticación SAML desde Unified Manager, los usuarios no podrán acceder a la interfaz de usuario gráfica hasta que configures el IdP con la información del host del servidor de Unified Manager. Por lo tanto, debes tener todo listo para completar ambas partes de la conexión antes de iniciar el proceso de configuración. Puedes configurar el IdP antes o después de configurar Unified Manager.

Solo los usuarios remotos tendrán acceso a la interfaz gráfica de usuario de Unified Manager una vez que se haya habilitado la autenticación SAML. Los usuarios locales y los usuarios de Maintenance no podrán acceder a la interfaz de usuario. Esta configuración no afecta a los usuarios que acceden a la consola de mantenimiento, a los comandos de Unified Manager ni a las ZAPIs.

Unified Manager se reinicia automáticamente después de que completes la configuración de SAML en esta página.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **SAML Authentication**.
2. Marca la casilla **Enable SAML authentication**.

   Se muestran los campos necesarios para configurar la conexión con el IdP.

3. Introduce la URI del IdP y los metadatos del IdP necesarios para conectar el servidor de Unified Manager al servidor del IdP.

   Si puedes acceder al servidor IdP directamente desde el servidor Unified Manager, puedes hacer clic en el botón **Obtener metadatos del IdP** después de introducir la URI del IdP para que el campo «Metadatos del IdP» se complete automáticamente.

4. Copia el URI de los metadatos del host de Unified Manager o guarda los metadatos del host en un archivo de texto XML.

   Ya puedes configurar el servidor IdP con esta información.

5. Haz clic en **Guardar**.

   Aparece un cuadro de diálogo para confirmar que deseas completar la configuración y reiniciar Unified Manager.

6. Haz clic en **Confirm and Logout** y Unified Manager se reinicia.

La próxima vez que los usuarios remotos autorizados intenten acceder a la interfaz gráfica de Unified Manager introducirán sus credenciales en la página de inicio de sesión del IdP en lugar de en la página de inicio de sesión de Unified Manager.

Si aún no lo has hecho, accede a tu IdP e introduce el URI del servidor de Unified Manager y los metadatos para completar la configuración.

Cuando usas ADFS como proveedor de identidad, la GUI de Unified Manager no respeta el tiempo de espera de ADFS y seguirá funcionando hasta que se alcance el tiempo de espera de la sesión de Unified Manager. Puedes cambiar el tiempo de espera de la sesión de la GUI haciendo clic en **General** > **Feature Settings** > **Inactivity Timeout**.

Cambiar el proveedor de identidad de autenticación SAML en Active IQ Unified Manager

Puedes cambiar el proveedor de identidad (IdP) que utiliza Unified Manager para autenticar a los usuarios remotos.

Antes de empezar

- Debes disponer de la URL del IdP y de los metadatos.
- Debes tener acceso al IdP.

Puedes configurar el nuevo IdP antes o después de configurar Unified Manager.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **SAML Authentication**.
2. Introduce la nueva URI de IdP y los metadatos de IdP necesarios para conectar el servidor de Unified Manager al IdP.

   Si se puede acceder al IdP directamente desde el servidor de Unified Manager, puedes hacer clic en el botón **Obtener metadatos del IdP** después de introducir la URL del IdP para que el campo «Metadatos del IdP» se rellene automáticamente.

3. Copia el URI de metadatos de Unified Manager o guarda los metadatos en un archivo de texto XML.
4. Haz clic en **Guardar configuración**.

   Aparece un cuadro de diálogo para confirmar que deseas cambiar la configuración.

5. Haz clic en **OK**.

Accede al nuevo IdP e introduce la URI del servidor de Unified Manager y los metadatos para completar la configuración.

La próxima vez que los usuarios remotos autorizados intenten acceder a la interfaz gráfica de Unified Manager, introducirán sus credenciales en la nueva página de inicio de sesión del IdP en lugar de en la antigua página de inicio de sesión del IdP.

Actualiza la configuración de autenticación SAML después de un cambio en el certificado de seguridad de Active IQ Unified Manager

Cualquier cambio en el certificado de seguridad HTTPS instalado en el servidor de Unified Manager requiere que actualices la configuración de autenticación SAML. El certificado se actualiza si cambias el nombre del sistema host, asignas una nueva dirección IP al sistema host o modificas manualmente el certificado de seguridad del sistema.

Una vez cambiado el certificado de seguridad y reiniciado el servidor de Unified Manager, la autenticación SAML dejará de funcionar y los usuarios no podrán acceder a la interfaz gráfica de Unified Manager. Debes actualizar la configuración de autenticación SAML tanto en el servidor IdP como en el servidor de Unified Manager para volver a habilitar el acceso a la interfaz de usuario.

Pasos

1. Inicia sesión en la consola de mantenimiento.
2. En el **Menú principal**, introduce el número correspondiente a la opción **Desactivar la autenticación SAML**.

   Aparece un mensaje para confirmar que deseas desactivar la autenticación SAML y reiniciar Unified Manager.

3. Inicia la interfaz de usuario de Unified Manager con el FQDN o la dirección IP actualizados, acepta el certificado del servidor actualizado en tu navegador e inicia sesión con las credenciales del usuario de mantenimiento.
4. En la página **Configuración/Autenticación**, selecciona la pestaña **Autenticación SAML** y configura la conexión con el IdP.
5. Copia el URI de los metadatos del host de Unified Manager o guarda los metadatos del host en un archivo de texto XML.
6. Haz clic en **Guardar**.

   Aparece un cuadro de diálogo para confirmar que deseas completar la configuración y reiniciar Unified Manager.

7. Haz clic en **Confirm and Logout** y Unified Manager se reinicia.
8. Accede a tu servidor IdP e introduce el URI y los metadatos del servidor de Unified Manager para completar la configuración.

Proveedor de identidad	Pasos de configuración
ADFS	a. Elimina la entrada de confianza de usuario autenticado existente en la GUI de administración de ADFS. b. Añade una nueva entrada de confianza de parte dependiente utilizando el `saml_sp_metadata.xml` del servidor Unified Manager actualizado. c. Define las tres reglas de reclamaciones necesarias para que Unified Manager analice las respuestas SAML de ADFS para esta entrada de confianza de la parte dependiente. d. Reinicia el servicio ADFS de Windows.
Shibboleth	a. Actualiza el nuevo FQDN del servidor Unified Manager en los archivos `attribute-filter.xml` y `relying-party.xml`. b. Reinicia el servidor web Apache Tomcat y espera a que el puerto 8005 esté en línea.

9. Inicia sesión en Unified Manager y comprueba que la autenticación SAML funciona correctamente a través de tu proveedor de identidad (IdP).

Desactivar la autenticación SAML en Active IQ Unified Manager

Puedes desactivar la autenticación SAML cuando desees dejar de autenticar a los usuarios remotos a través de un proveedor de identidad (IdP) seguro antes de que puedan iniciar sesión en la interfaz de usuario web de Unified Manager. Cuando la autenticación SAML está desactivada, los proveedores de servicios de directorio configurados, como Active Directory o LDAP, realizan la autenticación de inicio de sesión.

Una vez que desactives la autenticación SAML, los usuarios locales y los usuarios de mantenimiento podrán acceder a la interfaz gráfica de usuario, además de los usuarios remotos configurados.

También puedes desactivar la autenticación SAML mediante la consola de mantenimiento de Unified Manager si no tienes acceso a la interfaz gráfica de usuario.

Unified Manager se reinicia automáticamente tras desactivar la autenticación SAML.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **SAML Authentication**.
2. Desmarca la casilla **Habilitar autenticación SAML**.
3. Haz clic en **Guardar**.

   Aparece un cuadro de diálogo para confirmar que deseas completar la configuración y reiniciar Unified Manager.

4. Haz clic en **Confirm and Logout** y Unified Manager se reinicia.

La próxima vez que los usuarios remotos intenten acceder a la interfaz gráfica de Unified Manager, introducirán sus credenciales en la página de inicio de sesión de Unified Manager en lugar de en la página de inicio de sesión del IdP.

Accede a tu IdP y elimina el URI y los metadatos del servidor de Unified Manager.

Desactivar la autenticación SAML desde la consola de mantenimiento de Active IQ Unified Manager

Es posible que tengas que desactivar la autenticación SAML desde la consola de mantenimiento cuando no haya acceso a la GUI de Unified Manager. Esto podría ocurrir en casos de configuración incorrecta o si no se puede acceder al IdP.

Antes de empezar

Debes tener acceso a la consola de mantenimiento como el usuario de mantenimiento.

Cuando la autenticación SAML está desactivada, los proveedores de servicios de directorio configurados, como Active Directory o LDAP, realizan la autenticación de inicio de sesión. Los usuarios locales y los usuarios de mantenimiento podrán acceder a la interfaz gráfica de usuario, además de los usuarios remotos configurados.

También puedes desactivar la autenticación SAML desde la página Setup/Authentication de la interfaz de usuario.

Unified Manager se reinicia automáticamente tras desactivar la autenticación SAML.

Pasos

1. Inicia sesión en la consola de mantenimiento.
2. En el **Menú principal**, introduce el número correspondiente a la opción **Desactivar la autenticación SAML**.

   Aparece un mensaje para confirmar que deseas desactivar la autenticación SAML y reiniciar Unified

Manager.

3. Escribe **y** y, a continuación, pulsa Enter y Unified Manager se reinicia.

La próxima vez que los usuarios remotos intenten acceder a la interfaz gráfica de Unified Manager, introducirán sus credenciales en la página de inicio de sesión de Unified Manager en lugar de en la página de inicio de sesión del IdP.

Si es necesario, accede a tu IdP y elimina la URL del servidor de Unified Manager y los metadatos.

Utiliza la página de autenticación SAML en Active IQ Unified Manager

Puedes usar la página «Autenticación SAML» para configurar Unified Manager para que autentique a los usuarios remotos mediante SAML a través de un proveedor de identidad (IdP) seguro antes de que puedan iniciar sesión en la interfaz web de Unified Manager.

- Debes tener el rol Application Administrator para crear o modificar la configuración de SAML.
- Debes haber configurado la autenticación remota.
- Debes haber configurado al menos un usuario remoto o un grupo remoto.

Después de configurar la autenticación remota y los usuarios remotos, puedes marcar la casilla «Enable SAML authentication» para habilitar la autenticación mediante un proveedor de identidad seguro.

- **URI del IdP**

  El URI para acceder al IdP desde el servidor de Unified Manager. A continuación se enumeran algunos ejemplos de URI.

  URI de ejemplo de ADFS:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  URI de ejemplo de Shibboleth:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Metadatos del IdP**

  Los metadatos del IdP en formato XML.

  Si se puede acceder a la URL del IdP desde el servidor de Unified Manager, puedes hacer clic en el botón **Obtener metadatos del IdP** para rellenar este campo.

- **Sistema host (FQDN)**

  El nombre de dominio completo (FQDN) del sistema host de Unified Manager, tal y como se definió durante la instalación. Puede modificar este valor si es necesario.

- **URI del host**

El URI para acceder al sistema host de Unified Manager desde el IdP.

- **Metadatos del host**

  Los metadatos del sistema host en formato XML.

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.