



Habilite las cuentas de autenticación multifactor (MFA)

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

- Habilite las cuentas de autenticación multifactor (MFA) 1
 - Obtenga más información sobre la autenticación multifactor de ONTAP 1
 - Habilite la autenticación multifactor de ONTAP con SSH y TOTP 2
 - Habilite MFA con clave pública SSH y contraseña de usuario 3
 - Habilite MFA con TOTP 3
 - Configure cuentas de usuario locales de ONTAP para MFA con TOTP 5
 - Restablezca la clave secreta TOTP para una cuenta de usuario de ONTAP 6
 - Restablezca TOTP si su clave está comprometida 6
 - Restablezca TOTP si se pierde la clave 7
 - Deshabilite la clave secreta TOTP para una cuenta de usuario de ONTAP 7

Habilite las cuentas de autenticación multifactor (MFA)

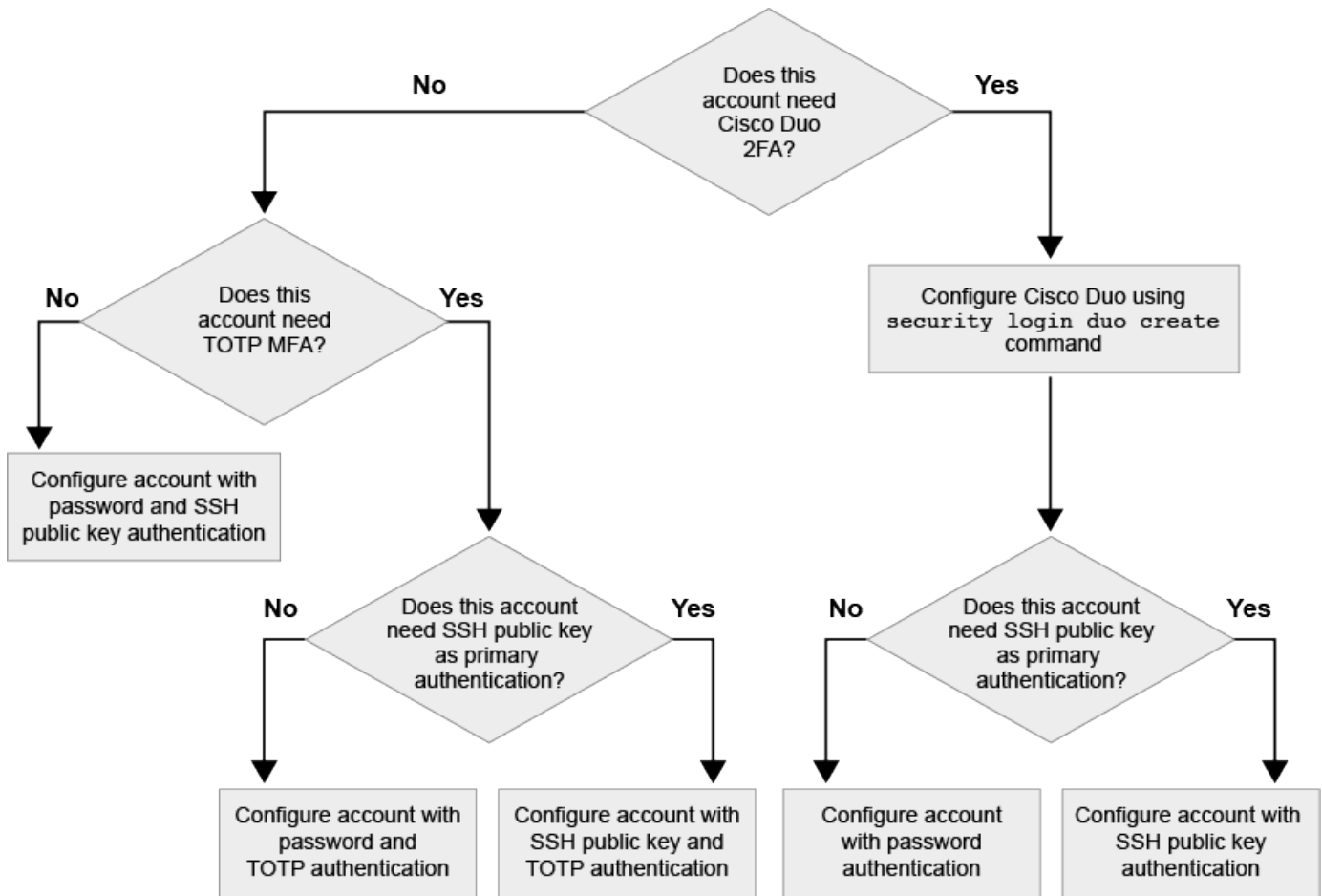
Obtenga más información sobre la autenticación multifactor de ONTAP

La autenticación multifactor (MFA) permite mejorar la seguridad al requerir que los usuarios proporcionen dos métodos de autenticación para iniciar sesión en un administrador o en un equipo virtual de almacenamiento de datos.

Dependiendo de la versión de ONTAP, puede utilizar una combinación de una clave pública SSH, una contraseña de usuario y una contraseña de un solo uso basada en el tiempo (TOTP) para la autenticación multifactor. Al habilitar y configurar Cisco Duo (ONTAP 9.14.1 y posterior), sirve como un método de autenticación adicional, que complementa los métodos existentes para todos los usuarios.

Disponible empezando por...	Primer método de autenticación	Segundo método de autenticación
ONTAP 9.14.1	Clave pública SSH	TOTP
	Contraseña de usuario	TOTP
	Clave pública SSH	Cisco Duo
	Contraseña de usuario	Cisco Duo
ONTAP 9.13.1	Clave pública SSH	TOTP
	Contraseña de usuario	TOTP
ONTAP 9,3	Clave pública SSH	Contraseña de usuario

Si se configura MFA, el administrador del clúster primero debe habilitar la cuenta de usuario local, entonces el usuario local debe configurar la cuenta.



Habilite la autenticación multifactor de ONTAP con SSH y TOTP

La autenticación multifactor (MFA) permite mejorar la seguridad al requerir que los usuarios proporcionen dos métodos de autenticación para iniciar sesión en un administrador o una SVM de datos.

Acerca de esta tarea

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Si no está seguro del rol de control de acceso que desea asignar a la cuenta de inicio de sesión, puede utilizar `security login modify` el comando para añadir el rol más adelante.

Obtenga más información sobre `security login modify` en el ["Referencia de comandos del ONTAP"](#).

["Modificar el rol asignado a un administrador"](#)

- Si utiliza una clave pública para la autenticación, debe asociar la clave pública con la cuenta para que la cuenta pueda acceder a la SVM.

["Asociar una clave pública a una cuenta de usuario"](#)

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- A partir de ONTAP 9.12.1, puede usar dispositivos de autenticación de hardware Yubikey para la MFA del

cliente SSH mediante los estándares de autenticación FIDO2 (Fast Identity Online) o de verificación de identidad personal (PIV).

Habilite MFA con clave pública SSH y contraseña de usuario

A partir de ONTAP 9,3, un administrador de clúster puede configurar cuentas de usuario locales para iniciar sesión con MFA mediante una clave pública SSH y una contraseña de usuario.

1. Habilite MFA en cuenta de usuario local con clave pública SSH y contraseña de usuario:

```
security login create -vserver <svm_name> -user-or-group-name  
<user_name> -application ssh -authentication-method <password|publickey>  
-role admin -second-authentication-method <password|publickey>
```

El siguiente comando requiere que la cuenta de administrador de SVM `admin2` con `admin` el rol predefinido inicie sesión en la SVM `engData1` con una clave pública SSH y una contraseña de usuario:

```
cluster-1::> security login create -vserver engData1 -user-or-group-name  
admin2 -application ssh -authentication-method publickey -role admin  
-second-authentication-method password  
  
Please enter a password for user 'admin2':  
Please enter it again:  
Warning: To use public-key authentication, you must create a public key  
for user "admin2".
```

Obtenga más información sobre `security login create` en el ["Referencia de comandos del ONTAP"](#).

Habilite MFA con TOTP

A partir de ONTAP 9.13.1, puede mejorar la seguridad al requerir que los usuarios locales inicien sesión en un administrador o una SVM de datos con una clave pública SSH o una contraseña de usuario y una contraseña de un solo uso basada en un tiempo (TOTP). Una vez que la cuenta se habilita para MFA con TOTP, el usuario local debe iniciar sesión en ["complete la configuración"](#).

TOTP es un algoritmo informático que utiliza la hora actual para generar una contraseña de un solo uso. Si se utiliza TOTP, siempre es la segunda forma de autenticación después de la clave pública SSH o la contraseña de usuario.

Antes de empezar

Debe ser un administrador de almacenamiento para realizar estas tareas.

Pasos

Puede configurar MFA con una contraseña de usuario o una clave pública SSH como primer método de autenticación y TOTP como segundo método de autenticación.

Habilite MFA con contraseña de usuario y TOTP

1. Habilite una cuenta de usuario para la autenticación multifactor con una contraseña de usuario y TOTP.

Para nuevas cuentas de usuario

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

Para cuentas de usuario existentes

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Compruebe que MFA con TOTP está activado:

```
security login show
```

Habilite MFA con clave pública SSH y TOTP

1. Habilite una cuenta de usuario para la autenticación multifactor con una clave pública SSH y TOTP.

Para nuevas cuentas de usuario

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

Para cuentas de usuario existentes

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

Obtenga más información sobre `security login modify` en el ["Referencia de comandos del ONTAP"](#).

2. Compruebe que MFA con TOTP está activado:

```
security login show
```

Obtenga más información sobre `security login show` en el ["Referencia de comandos del ONTAP"](#).

Después de terminar

- Si no ha asociado una clave pública a la cuenta de administrador, debe hacerlo para que la cuenta pueda acceder a la SVM.

["Asociación de una clave pública con una cuenta de usuario"](#)

- El usuario local debe iniciar sesión para completar la configuración MFA con TOTP.

["Configure la cuenta de usuario local para MFA con TOTP"](#)

Información relacionada

- ["Autenticación multifactor en ONTAP 9 \(TR-4647\)"](#)
- ["Referencia de comandos del ONTAP"](#)

Configure cuentas de usuario locales de ONTAP para MFA con TOTP

A partir de ONTAP 9.13.1, las cuentas de usuario se pueden configurar con autenticación multifactor (MFA) con una contraseña de un solo uso basada en tiempo (TOTP).

Antes de empezar

- El administrador de almacenamiento debe ["Habilite MFA con TOTP"](#) como segundo método de autenticación para su cuenta de usuario.
- El método de autenticación de la cuenta de usuario principal debe ser una contraseña de usuario o una clave SSH pública.
- Debes configurar tu aplicación TOTP para que funcione con tu smartphone y crear tu clave secreta TOTP.

Microsoft Authenticator, Google Authenticator, Authy y cualquier otro autenticador compatible con TOTP son compatibles.

Pasos

1. Inicie sesión en su cuenta de usuario con el método de autenticación actual.

Su método de autenticación actual debe ser una contraseña de usuario o una clave pública SSH.

2. Cree la configuración de TOTP en su cuenta:

```
security login totp create -vserver "<svm_name>" -username  
"<account_username >"
```

3. Compruebe que la configuración de TOTP está activada en su cuenta:

```
security login totp show -vserver "<svm_name>" -username  
"<account_username>"
```

Información relacionada

- ["Inicio de sesión de seguridad totp create"](#)
- ["Inicio de sesión de seguridad totp show"](#)

Restablezca la clave secreta TOTP para una cuenta de usuario de ONTAP

Para proteger la seguridad de su cuenta, si su clave secreta TOTP se ve comprometida o se pierde, debe deshabilitarla y crear una nueva.

Restablezca TOTP si su clave está comprometida

Si tu clave secreta TOTP está comprometida, pero aún tienes acceso a ella, puedes quitar la clave comprometida y crear una nueva.

1. Inicie sesión en su cuenta de usuario con su contraseña de usuario o clave pública SSH y su clave secreta TOTP comprometida.
2. Elimine la clave secreta TOTP comprometida:

```
security login totp delete -vserver <svm_name> -username  
<account_username>
```

3. Cree una nueva clave secreta de TOTP:

```
security login totp create -vserver <svm_name> -username  
<account_username>
```

4. Compruebe que la configuración de TOTP está activada en su cuenta:

```
security login totp show -vserver <svm_name> -username  
<account_username>
```


Restablezca TOTP si se pierde la clave

Si se pierde la clave secreta de TOTP, póngase en contacto con el administrador de almacenamiento para ["tener la clave desactivada"](#). Una vez desactivada la clave, puede utilizar el primer método de autenticación para iniciar sesión y configurar un nuevo TOTP.

Antes de empezar

La clave secreta de TOTP debe ser deshabilitada por un administrador de almacenamiento. Si no tiene una cuenta de administrador de almacenamiento, póngase en contacto con su administrador de almacenamiento para deshabilitar la clave.

Pasos

1. Una vez que un administrador de almacenamiento haya desactivado el secreto TOTP, utilice el método de autenticación principal para iniciar sesión en su cuenta local.
2. Cree una nueva clave secreta de TOTP:

```
security login totp create -vserver <svm_name> -username  
<account_username >
```

3. Compruebe que la configuración de TOTP está activada en su cuenta:

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

Información relacionada

- ["inicio de sesión de seguridad totp create"](#)
- ["inicio de sesión de seguridad totp eliminar"](#)
- ["Inicio de sesión de seguridad totp show"](#)

Deshabilite la clave secreta TOTP para una cuenta de usuario de ONTAP

Si se pierde la clave secreta de una sola vez basada en el tiempo (TOTP) de un usuario local, el administrador de almacenamiento debe desactivar la clave perdida antes de que el usuario pueda crear una nueva clave secreta TOTP.

Acerca de esta tarea

Esta tarea solo se puede realizar desde una cuenta de administrador de clúster.

Paso

1. Desactive la clave secreta TOTP:

```
security login totp modify -vserver <svm_name> -username  
<account_username> -enabled false
```

Obtenga más información sobre `security login totp modify` en el ["Referencia de comandos del ONTAP"](#).

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.