



Enable multifactor authentication (MFA) accounts

ONTAP 9

NetApp
November 01, 2023

Table of Contents

- Enable multifactor authentication (MFA) accounts..... 1
 - Multifactor authentication overview 1
 - Set up multifactor authentication 1
 - Enable multifactor authentication..... 3
 - Configure local user account for MFA with TOTP 6
 - Reset TOTP secret key 7
 - Disable TOTP secret key for local account 8

Enable multifactor authentication (MFA) accounts

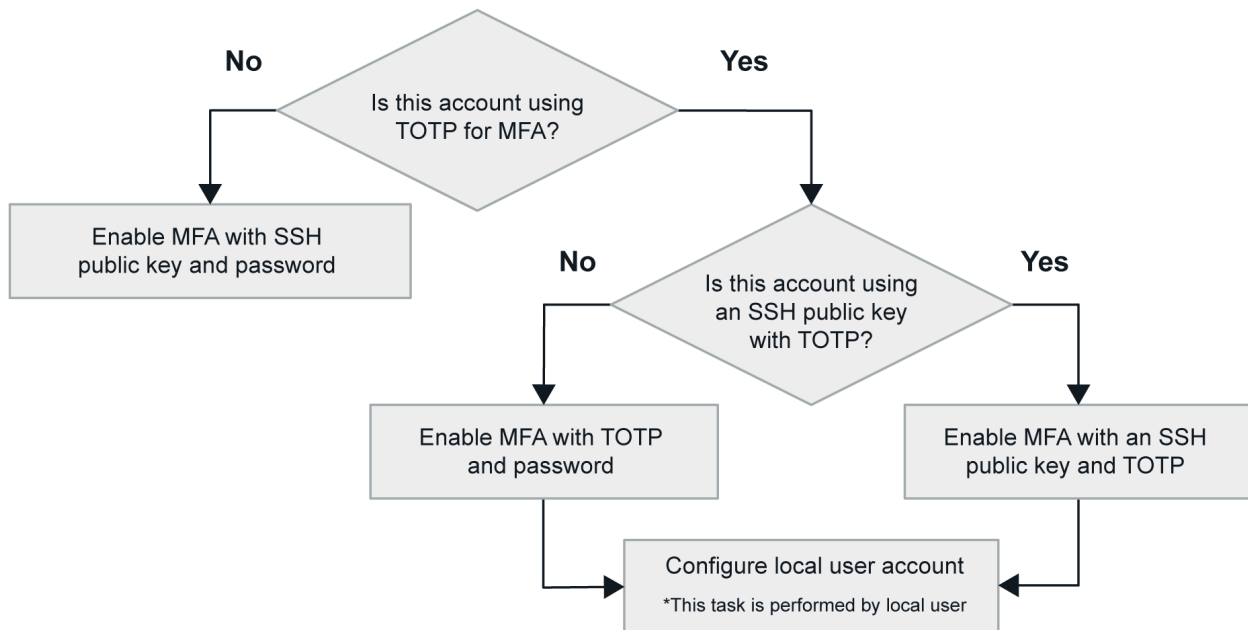
Multifactor authentication overview

Multifactor authentication (MFA) allows you to enhance security by requiring users to provide two authentication methods to log in to an admin or data SVM.

Depending upon your version of ONTAP, you can use a combination of an SSH public key, user password, and time-based one-time password (TOTP) to set up multifactor authentication.

ONTAP version	First authentication method	Second authentication method
9.13.1 and later	SSH public key	TOTP
	User password	TOTP
9.3 and later	SSH public key	User password

If MFA is configured with TOTP, the cluster administrator must first enable the local user account, then the account must be configured by the local user.



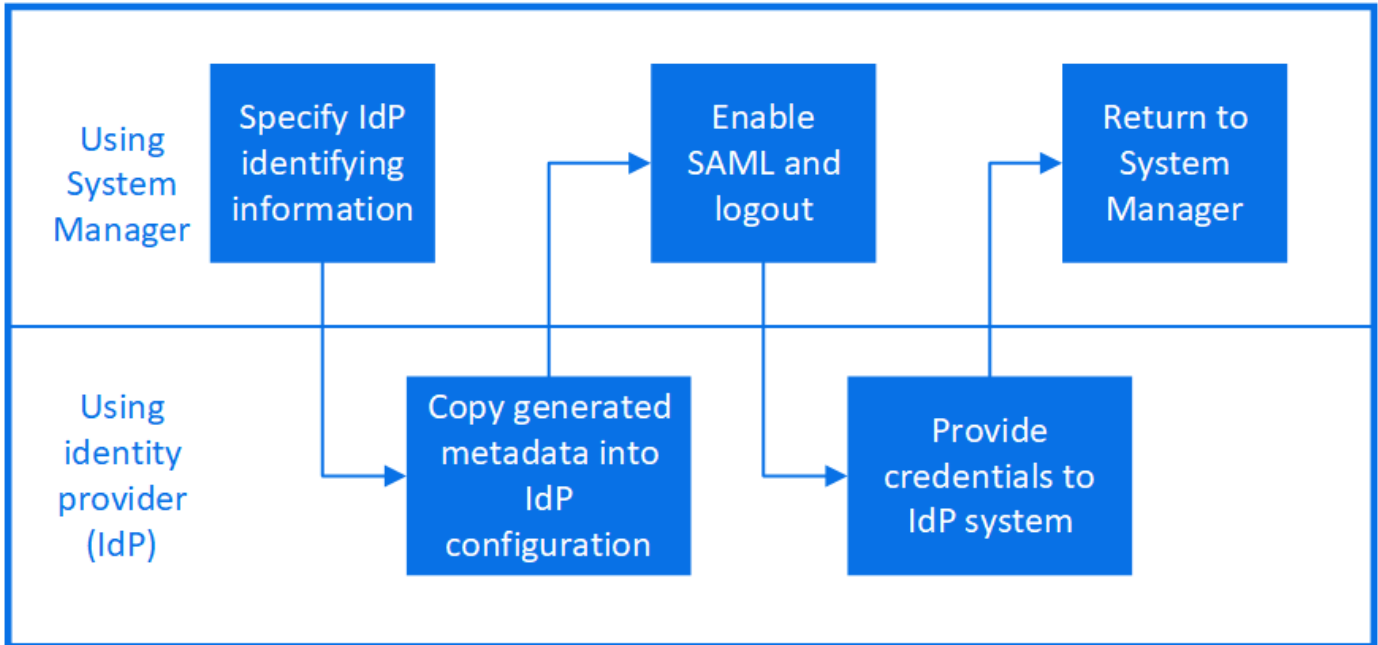
Set up multifactor authentication

Security Assertion Markup Language (SAML) authentication allows users to log in to an application by using a secure identity provider (IdP).

In System Manager, in addition to standard ONTAP authentication, SAML-based authentication is provided as an option for multifactor authentication.


Security Assertion Markup Language (SAML) is an XML-based framework for authentication and authorization between two entities: a service provider and an identity provider.

Enable SAML authentication



To enable SAML authentication, perform the following steps:


Steps

1. Click **Cluster > Settings**.
2. Next to **SAML Authentication**, click .
3. Ensure there is a check in the **Enable SAML Authentication** checkbox.
4. Enter the URL of the IdP URI (including "https://").
5. Modify the host system address, if needed.
6. Ensure the correct certificate is being used:
 - If your system was mapped with only one certificate with type "server", then that certificate is considered the default and it isn't displayed.
 - If your system was mapped with multiple certificates as type "server", then one of the certificates is displayed. To select a different certificate, click **Change**.
7. Click **Save**. A confirmation window displays the metadata information, which has been automatically copied to your clipboard.
8. Go to the IdP system you specified and copy the metadata from your clipboard to update the system metadata.
9. Return to the confirmation window (in System Manager) and check the checkbox **I have configured the IdP with the host URI or metadata**.
10. Click **Logout** to enable SAML-based authentication. The IdP system will display an authentication screen.
11. In the IdP system, enter your SAML-based credentials. After your credentials are verified, you will be directed to the System Manager home page.

Disable SAML authentication

To disable SAML authentication, perform the following steps:

Steps

1. Click **Cluster > Settings**.
2. Under **SAML Authentication**, click the **Enabled** toggle button.
3. *Optional:* You can also click  next to **SAML Authentication**, and then uncheck the **Enable SAML Authentication** checkbox.

Enable multifactor authentication

Multifactor authentication (MFA) allows you to enhance security by requiring users to provide two authentication methods to log in to an admin or data SVM.

About this task

- You must be a cluster administrator to perform this task.
- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

[Modifying the role assigned to an administrator](#)

- If you are using a public key for authentication, you must associate the public key with the account before the account can access the SVM.

[Associate a public key with a user account](#)

You can perform this task before or after you enable account access.

- Beginning with ONTAP 9.12.1, you can use Yubikey hardware authentication devices for SSH client MFA using the FIDO2 (Fast Identity Online) or Personal Identity Verification (PIV) authentication standards.

Enable MFA with SSH public key and user password

Beginning with ONTAP 9.3, a cluster administrator can set up local user accounts to log in with MFA using an SSH public key and a user password.

1. Enable MFA on local user account with SSH public key and user password:

```
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>
```

The following command requires the SVM administrator account `admin2` with the predefined `admin` role to log in to the SVM `engData1` with both an SSH public key and a user password:

```
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".

Enable MFA with TOTP

Beginning with ONTAP 9.13.1, you can enhance security by requiring local users to log in to an admin or data SVM with both an SSH public key or user password and a time-based one-time password (TOTP). After the account is enabled for MFA with TOTP, the local user must log in to [complete the configuration](#).

TOTP is a computer algorithm that uses the current time to generate a one-time password. If TOTP is used, it is always the second form of authentication after the SSH public key or the user password.

Before you begin

You must be a storage administrator to perform these tasks.

Steps

You can set up MFA to with a user password or an SSH public key as the first authentication method and TOTP as the second authentication method.

Enable MFA with user password and TOTP

1. Enable a user account for multifactor authentication with a user password and TOTP.

For new user accounts

```
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>
```

For existing user accounts

```
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. Verify that MFA with TOTP is enabled:

```
security login show
```

Enable MFA with SSH public key and TOTP

1. Enable a user account for multifactor authentication with an SSH public key and TOTP.

For new user accounts

```
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>
```

For existing user accounts

```
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>
```

2. Verify that MFA with TOTP is enabled:

```
security login show
```

After you finish

- If you have not associated a public key with the administrator account, you must do so before the account can access the SVM.

[Associating a public key with a user account](#)

- The local user must log in to complete MFA configuration with TOTP.

[Configure local user account for MFA with TOTP](#)

Related information

Learn more about [Multifactor Authentication in ONTAP 9 \(TR-4647\)](#).

Configure local user account for MFA with TOTP

Beginning in ONTAP 9.13.1, user accounts can be configured with multifactor authentication (MFA) using a time-based one-time password (TOTP).

Before you begin

- The storage administrator must [enable MFA with TOTP](#) as a second authentication method for your user account.
- Your primary user account authentication method should be a user password or public SSH key.
- You must configure your TOTP app to work with your smartphone and create your TOTP secret key.

TOTP is supported by various authenticator apps such as Google Authenticator.

Steps

1. Log in to your user account with your current authentication method.

Your current authentication method should be a user password or an SSH public key.

2. Create the TOTP configuration on your account:

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

3. Verify that the TOTP configuration is enabled on your account:

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


Reset TOTP secret key

To protect your account security, if your TOTP secret key is compromised or lost, you should disable it and create a new one.

Reset TOTP if your key is compromised

If your TOTP secret key is compromised, but you still have access to it, you can remove the compromised key and create a new one.

1. Log in to your user account with your user password or SSH public key and your compromised TOTP secret key.
2. Remove the compromised TOTP secret key:

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

3. Create a new TOTP secret key:

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

4. Verify that the TOTP configuration is enabled on your account:

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

Reset TOTP if your key is lost

If your TOTP secret key is lost, contact your storage administrator to [have the key disabled](#). After your key is disabled, you can use your first authentication method to log in and configure a new TOTP.

Before you begin

The TOTP secret key must be disabled by a storage administrator.

If you do not have a storage administrator account, contact your storage administrator to have the key disabled.

Steps

1. After the TOTP secret is disabled by a storage administrator, use your primary authentication method to log in into your local account.
2. Create a new TOTP secret key:

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

3. Verify that the TOTP configuration is enabled on your account:

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

Disable TOTP secret key for local account

If a local user's time-based one-time password (TOTP) secret key is lost, the lost key must be disabled by a storage administrator before the user can create a new TOTP secret key.

About this task

This task can only be performed from a cluster administrator account.

Step

1. Disable the TOTP secret key:

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

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.