Enable local account access

ONTAP 9

NetApp
January 23, 2026

Table of Contents

Enable local account access

Learn about enabling local ONTAP account access

A local account is one in which the account information, public key, or security certificate resides on the storage system. You can use the `security login create` command to enable local accounts to access an admin or data SVM.

Related information

- security login create

Enable ONTAP account password access

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with a password. You are prompted for the password after you enter the command.

About 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.

Learn more about `security login modify` in the ONTAP command reference.

Before you begin

You must be a cluster administrator to perform this task.

Step

1. Enable local administrator accounts to access an SVM using a password:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   The following command enables the cluster administrator account `admin1` with the predefined `backup` role to access the admin SVM`engCluster` using a password. You are prompted for the password after you enter the command.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

   Learn more about `security login create` in the ONTAP command reference.

Enable ONTAP account SSH public key access

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with an SSH public key.

About this task

- You must associate the public key with the account before the account can access the SVM.

  Associating a public key with a user account

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

- 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.

  Learn more about `security login modify` in the ONTAP command reference.

If you want to enable FIPS mode on your cluster, existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type. The accounts should be reconfigured before you enable FIPs or the administrator authentication will fail.

The following table indicates host key type algorithms that are supported for ONTAP SSH connections. These key types do not apply to configuring SSH public authentication.

ONTAP release	Key types supported in FIPS mode	Key types supported in non-FIPS mode
9.11.1 and later	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa

Support for the ssh-ed25519 host key algorithm is removed beginning with ONTAP 9.11.1.

For more information, see Configure network security using FIPS.

Before you begin

You must be a cluster administrator to perform this task.

Step

1. Enable local administrator accounts to access an SVM using an SSH public key:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name user_or_group_name -application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   The following command enables the SVM administrator account `svmadmin1` with the predefined `vsadmin-volume` role to access the SVM`engData1` using an SSH public key:

```
cluster1::>security login create -vserver engData1 -user-or-group-name
svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

Learn more about `security login create` in the ONTAP command reference.

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

Enable multifactor authentication (MFA) accounts

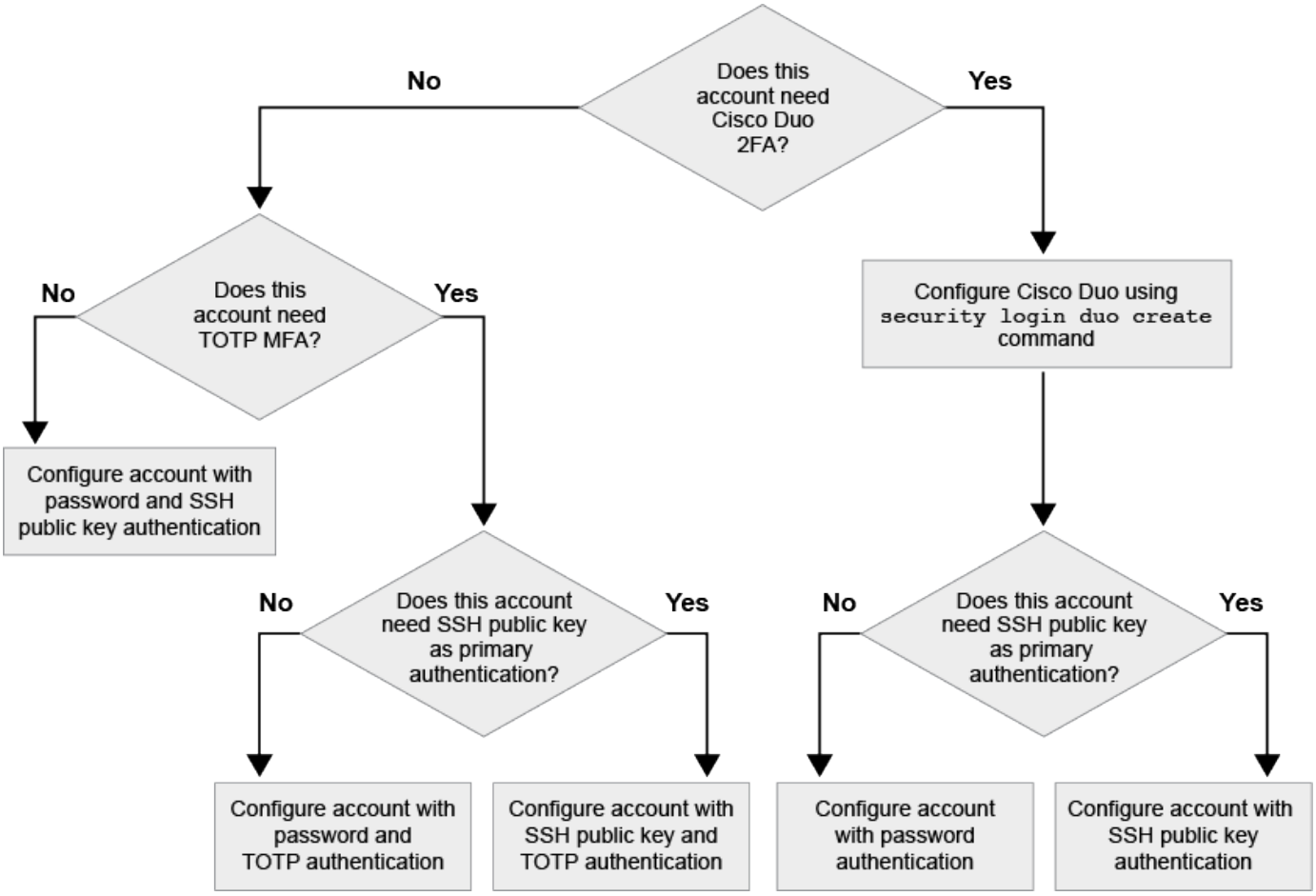
Learn about ONTAP multifactor authentication

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

Depending upon your version of ONTAP, you can use a combination of an SSH public key, a user password, and a time-based one-time password (TOTP) for multifactor authentication. When you enable and configure Cisco Duo (ONTAP 9.14.1 and later), it serves as an additional authentication method, supplementing the existing methods for all users.

Available beginning with…	First authentication method	Second authentication method
ONTAP 9.14.1	SSH public key	TOTP
	User Password	TOTP
	SSH public key	Cisco Duo
	User password	Cisco Duo
ONTAP 9.13.1	SSH public key	TOTP
	User password	TOTP
ONTAP 9.3	SSH public key	User password

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



Enable ONTAP multifactor authentication with SSH and TOTP

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.

  Learn more about `security login modify` in the ONTAP command reference.

  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".
```

Learn more about `security login create` in the ONTAP command reference.

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>
   ```

   Learn more about `security login modify` in the ONTAP command reference.

2. Verify that MFA with TOTP is enabled:

```
security login show
```

Learn more about `security login show` in the ONTAP command reference.

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

- Multifactor Authentication in ONTAP 9 (TR-4647)
- ONTAP command reference

Configure local ONTAP user accounts for MFA with TOTP

Beginning with 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.

  Microsoft Authenticator, Google Authenticator, Authy and any other TOTP-compatible authenticator is supported.

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>"
```

Related information

- security login totp create
- security login totp show

Reset the TOTP secret key for an ONTAP user account

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>
```

Related information

- security login totp create
- security login totp delete
- security login totp show

Disable the TOTP secret key for an ONTAP user 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 modify -vserver <svm_name> -username
<account_username> -enabled false
```

Learn more about `security login totp modify` in the ONTAP command reference.

Enable SSL certificate ONTAP account access

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with an SSL certificate.

About this task

- You must install a CA-signed server digital certificate before the account can access the SVM.

  Generating and installing a CA-signed server certificate

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

- If you are unsure of the access control role you want to assign to the login account, you can add the role later with the `security login modify` command.

  Modifying the role assigned to an administrator

> For cluster administrator accounts, certificate authentication is supported with the `http`, `ontapi`, and `rest` applications. For SVM administrator accounts, certificate authentication is supported only with the `ontapi` and `rest` applications.

Step

1. Enable local administrator accounts to access an SVM using an SSL certificate:

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   The following command enables the SVM administrator account `svmadmin2` with the default `vsadmin` role to access the SVM`engData2` using an SSL digital certificate.

   ```
   cluster1::>security login create -vserver engData2 -user-or-group-name
   svmadmin2 -application ontapi -authmethod cert
   ```

   Learn more about `security login create` in the ONTAP command reference.

After you finish

If you have not installed a CA-signed server digital certificate, you must do so before the account can access the SVM.

Generating and installing a CA-signed server certificate

Learn more about the commands described in this procedure in the ONTAP command reference.

Copyright information

Trademark information