Authentication and authorization using WebAuthn MFA

ONTAP 9

NetApp
December 21, 2024

Table of Contents

Authentication and authorization using WebAuthn MFA

WebAuthn multi-factor authentication overview

Beginning with ONTAP 9.16.1, administrators can enable WebAuthn multi-factor authentication (MFA) for users that log in to System Manager. This enables System Manager logins using a FIDO2 key (such as a YubiKey) as a second form of authentication. By default, WebAuthn MFA is disabled for new and existing ONTAP users.

WebAuthn MFA is supported for users and groups that use the following types of authentication for the first authentication method:

- Users: password, domain, or nsswitch
- Groups: domain or nsswitch

After you enable WebAuthn MFA as the second authentication method for a user, the user is asked to register a hardware authenticator upon logging in to System Manager. After registration, the private key is stored in the authenticator, and the public key is stored in ONTAP.

ONTAP supports one WebAuthn credential per user. If a user loses an authenticator and needs to have it replaced, the ONTAP administrator needs to delete the WebAuthn credential for the user so that the user can register a new authenticator upon the next login.

> Users that have WebAuthn MFA enabled as a second authentication method need to use the FQDN (for example, "https://myontap.example.com") instead of the IP address (for example, "https://192.168.100.200") to access System Manager. For users with WebAuthn MFA enabled, attempts to log in to the System Manager using the IP address are rejected.

Enable WebAuthn MFA for ONTAP System Manager users or groups

As an ONTAP administrator, you can enable WebAuthn MFA for a System Manager user or group by either adding a new user or group with the WebAuthn MFA option enabled or enabling the option for an existing user or group.

> After you enable WebAuthn MFA as the second authentication method for a user or group, the user (or all users in that group) will be asked to register a hardware FIDO2 device upon the next login to System Manager. This registration is handled by the user's local operating system, and usually consists of inserting the security key, creating a passkey, and touching the security key (if supported).

Enable WebAuthn MFA when creating a new user or group

You can create a new user or group with WebAuthn MFA enabled using either System Manager or the ONTAP CLI.

System Manager

1. Select **Cluster > Settings**.
2. Select the arrow icon next to **Users and Roles**.
3. Select **Add** under **Users**.
4. Specify a user or group name and select a role in the drop-down menu for **Role**.
5. Specify a login method and password for the user or group.

   WebAuthn MFA supports login methods of "password", "domain", or "nsswitch" for users, and "domain" or "nsswitch" for groups.

6. In the **MFA for HTTP** column, select **Enabled**.
7. Select **Save**.

CLI

1. Create a new user or group with WebAuthn MFA enabled.

   In the following example, WebAuthn MFA is enabled by choosing "publickey" for the second authentication method:

```
security login create -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

Enable WebAuthn MFA for an existing user or group

You can enable WebAuthn MFA for an existing user or group.

System Manager

1. Select **Cluster > Settings**.
2. Select the arrow icon next to **Users and Roles**.
3. In the list of users and groups, select the option menu for the user or group you want to edit.

   WebAuthn MFA supports login methods of "password", "domain", or "nsswitch" for users, and "domain" or "nsswitch" for groups.

4. In the **MFA for HTTP** column for that user, select **Enabled**.
5. Select **Save**.

CLI

1. Modify an existing user or group to enable WebAuthn MFA for that user or group.

   In the following example, WebAuthn MFA is enabled by choosing "publickey" for the second authentication method:

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

Learn more

Visit the ONTAP manual pages for these commands:

- security login create
- security login modify

Disable WebAuthn MFA for ONTAP System Manager users

As an ONTAP administrator, you can disable WebAuthn MFA for a user or group by editing the user or group with System Manager or the ONTAP CLI.

Disable WebAuthn MFA for an existing user or group

You can disable WebAuthn MFA for an existing user or group at any time.

> If you disable registered credentials, the credentials are retained. If you enable the credentials again in the future, the same credentials are used, so the user doesn't need to re-register upon logging in.

System Manager

1. Select **Cluster > Settings**.
2. Select the arrow icon next to **Users and Roles**.
3. In the list of users and groups, select the user or group you want to edit.
4. In the **MFA for HTTP** column for that user, select **Disabled**.
5. Select **Save**.

CLI

1. Modify an existing user or group to disable WebAuthn MFA for that user or group.

   In the following example, WebAuthn MFA is disabled by choosing "none" for the second authentication method.

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method none \
                      -application http \
                      -role admin
```

Learn more

Visit the ONTAP manual pages for this command:

- security login modify

View ONTAP WebAuthn MFA settings and manage credentials

As an ONTAP administrator, you can view cluster-wide WebAuthn MFA settings and manage user and group credentials for WebAuthn MFA.

View cluster settings for WebAuthn MFA

You can view the cluster settings for WebAuthn MFA using the ONTAP CLI.

Steps

1. View the cluster settings for WebAuthn MFA. You can optionally specify a storage VM using the `vserver` argument:

```
security webauthn show -vserver <storage_vm_name>
```

View supported public key WebAuthn MFA algorithms

You can view the supported public key algorithms for WebAuthn MFA for a storage VM or for a cluster.

Steps

1. List the supported public key WebAuthn MFA algorithms. You can optionally specify a storage VM using the `vserver` argument:

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

View the registered WebAuthn MFA credentials

As an ONTAP administrator, you can view the registered WebAuthn credentials for all users. Non-administrator users that use this procedure can only view their own registered WebAuthn credentials.

Steps

1. View the registered WebAuthn MFA credentials:

```
security webauthn credentials show
```

Remove a registered WebAuthn MFA credential

You can remove a registered WebAuthn MFA credential. This is useful when a user's hardware key was lost, stolen, or is no longer in use. You can also remove a registered credential when the user still has the original hardware authenticator, but wants to replace it with a new one. After removing the credential, the user will be prompted to register the replacement authenticator.

Removing a registered credential for a user doesn't disable WebAuthn MFA for the user. If a user loses a hardware authenticator and needs to log in before replacing it, you need to remove the credential using these steps and also Disable WebAuthn MFA for the user.

System Manager

1. Select **Cluster > Settings**.
2. Select the arrow icon next to **Users and Roles**.
3. In the list of users and groups, select the option menu for the user or group whose credentials you want to remove.
4. Select **Remove MFA for HTTP credentials**.
5. Select **Remove**.

CLI

1. Delete the registered credentials. Note the following:
   - You can optionally specify a storage VM of the user. If omitted, the credential is removed at the cluster level.
   - You can optionally specify a username of the user for whom you are deleting the credential. If omitted, the credential is removed for the current user.

```
security webauthn credentials delete -vserver <storage_vm_name>
-username <username>
```

Learn more

Visit the ONTAP manual pages for these commands:

- security webauthn show
- security webauthn supported-algorithms show
- security webauthn credentials show
- security webauthn credentials delete

Copyright information

Trademark information