# 使用WebAuthn MFA进行身份验证和授权

ONTAP 9

NetApp
January 17, 2025

# 目录

# 使用WebAuthn MFA进行身份验证和授权

## WebAuthn多因素身份验证概述

从ONTAP 9 Manager.16开始、管理员可以为登录到System Manager的用户启用WebAuthn多因素身份验证(MFA)。这样、System Manager就可以使用FIDO2密钥(例如YukiKey)作为第二种身份验证形式进行登录。默认情况下、对于新用户和现有ONTAP用户、WebAuthn MFA处于禁用状态。

对于对第一种身份验证方法使用以下类型的身份验证的用户和组、支持WebAuthn MFA：

- 用户：密码、域或nsswitch
- 组：domain或nsswitch

在为用户启用WebAuthn MFA作为第二种身份验证方法后、系统会要求用户在登录到System Manager时注册硬件身份验证程序。注册后、私钥存储在身份验证程序中、公共密钥存储在ONTAP中。

ONTAP支持每个用户一个WebAuthn凭据。如果用户丢失了身份验证程序并需要更换它、ONTAP管理员需要删除该用户的WebAuthn凭据、以便该用户可以在下次登录时注册新的身份验证程序。

> 启用了WebAuthn MFA作为第二种身份验证方法的用户需要使用FQDN (例如"<a href="https://myontap.example.com"" class="bare">https://myontap.example.com"</a>)而不是IP地址(例如"<a href="https://192.168.100.200"" class="bare">https://192.168.100.200"</a>)来访问System Manager。对于启用了WebAuthn MFA的用户、使用IP地址登录到System Manager的尝试将被拒绝。

# 为ONTAP System Manager用户或组启用WebAuthn MFA

作为ONTAP管理员、您可以通过添加启用了WebAuthn MFA选项的新用户或组或为现有用户或组启用WebAuthn MFA选项来为System Manager用户或组启用WebAuthn MFA。

> 在为用户或组启用WebAuthn MFA作为第二种身份验证方法后、下次登录到System Manager时、系统将要求该用户(或该组中的所有用户)注册硬件FIDO2设备。此注册由用户的本地操作系统处理、通常包括插入安全密钥、创建密钥以及触摸安全密钥(如果支持)。

### 创建新用户或组时启用WebAuthn MFA

您可以使用System Manager或ONTAP命令行界面创建启用了WebAuthn MFA的新用户或组。

**System Manager**

1. 选择*集群>设置*。
2. 选择*用户和角色*旁边的箭头图标。
3. 在*USERS*下选择*ADD*。
4. 指定用户或组名称，然后在下拉菜单中为*rouser*选择一个角色。
5. 指定用户或组的登录方法和密码。

   WebAuthn MFA支持用户使用"password"、"domain"或"nsswitch"登录方法、组使用"domain"或"nsswitch"登录方法。

6. 在“* HTTP的MFA”列中，选择“已启用”。
7. 选择 * 保存 * 。

命令行界面

1. 创建启用了WebAuthn MFA的新用户或组。

   在以下示例中、通过为第二种身份验证方法选择"publickey"来启用WebAuthn MFA：

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

## 为现有用户或组启用**WebAuthn MFA**

您可以为现有用户或组启用WebAuthn MFA。

**System Manager**

1. 选择*集群>设置*。
2. 选择*用户和角色*旁边的箭头图标。
3. 在用户和组列表中、选择要编辑的用户或组的选项菜单。

   WebAuthn MFA支持用户使用"password"、"domain"或"nsswitch"登录方法、组使用"domain"或"nsswitch"登录方法。

4. 在该用户的*MFA for HTTP/*列中，选择*Enabled"。
5. 选择 * 保存 * 。

命令行界面

1. 修改现有用户或组、以便为该用户或组启用WebAuthn MFA。

   在以下示例中、通过为第二种身份验证方法选择"publickey"来启用WebAuthn MFA：

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

## 了解更多信息。

有关这些命令、请访问ONTAP手册页：

- "创建安全登录"
- "security login修改"

# 为ONTAP System Manager用户禁用WebAuthn MFA

作为ONTAP管理员、您可以通过使用System Manager或ONTAP命令行界面编辑用户或组来为用户或组禁用WebAuthn MFA。

## 为现有用户或组禁用WebAuthn MFA

您可以随时为现有用户或组禁用WebAuthn MFA。

> 如果禁用已注册的凭据、这些凭据将保留下来。如果您将来再次启用这些凭据、则会使用相同的凭据、因此用户无需在登录时重新注册。

**System Manager**

1. 选择*集群>设置*。
2. 选择*用户和角色*旁边的箭头图标。
3. 在用户和组列表中、选择要编辑的用户或组。
4. 在该用户的*MFA for HTTP/*列中，选择*Disabled。
5. 选择 * 保存 * 。

命令行界面

1. 修改现有用户或组以禁用该用户或组的WebAuthn MFA。

   在以下示例中、通过为第二种身份验证方法选择"none"来禁用WebAuthn MFA。

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

## 了解更多信息。

请访问此命令的ONTAP手册页：

- "security login修改"

# 查看ONTAP WebAuthn MFA设置并管理凭据

作为ONTAP管理员、您可以查看集群范围的WebAuthn MFA设置、并管理WebAuthn MFA的用户和组凭据。

## 查看WebAuthn MFA的集群设置

您可以使用ONTAP命令行界面查看WebAuthn MFA的集群设置。

步骤

1. 查看WebAuthn MFA的集群设置。您也可以使用参数指定Storage VM `vserver`：

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

## 查看支持的公共密钥WebAuthn MFA算法

您可以查看Storage VM或集群的WebAuthn MFA支持的公共密钥算法。

步骤

1. 列出支持的公共密钥WebAuthn MFA算法。您也可以使用参数指定Storage VM `vserver`：

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

## 查看已注册的WebAuthn MFA凭据

作为ONTAP管理员、您可以查看所有用户的已注册WebAuthn凭据。使用此过程的非管理员用户只能查看其自己注册的WebAuthn凭据。

步骤

1. 查看已注册的WebAuthn MFA凭据：

```
security webauthn credentials show
```

## 删除已注册的WebAuthn MFA凭据

您可以删除已注册的WebAuthn MFA凭据。当用户的硬件密钥丢失、被盗或不再使用时、这很有用。如果用户仍具有原始硬件身份验证程序、但希望将其替换为新身份验证程序、您也可以删除已注册的凭据。删除凭据后、系统将提示用户注册替代身份验证程序。

> 删除用户的已注册凭据不会为此用户禁用WebAuthn MFA。如果用户丢失了硬件身份验证程序并需要在更换之前登录、则您需要使用这些步骤删除该用户的凭据"禁用WebAuthn MFA"。

**System Manager**

1. 选择*集群>设置*。
2. 选择*用户和角色*旁边的箭头图标。
3. 在用户和组列表中、选择要删除其凭据的用户或组的选项菜单。
4. 选择*删除HTTP凭据的MFA *。
5. 选择 * 删除 * 。

命令行界面

1. 删除已注册的凭据。请注意以下事项：
   - 您可以选择指定用户的Storage VM。如果省略此参数、则会在集群级别删除此凭据。
   - 您可以选择指定要删除其凭据的用户的用户名。如果省略、则会删除当前用户的凭据。

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

## 了解更多信息。

有关这些命令、请访问ONTAP手册页：

- "security webauthn show"
- "security webauthn supported-al算法show"
- "security webauthn credcredcredcredcredcred凭 据show"
- "security webauthn凭据删除"