



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	1
WebAuthn多因素身份验证概述	1
为ONTAP System Manager用户或组启用WebAuthn MFA	1
为ONTAP System Manager用户禁用WebAuthn MFA	3
查看ONTAP WebAuthn MFA设置并管理凭据	4

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"<https://myontap.example.com>")而不是IP地址(例如"<https://192.168.100.200>")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 credcredcredcredcred凭据show"](#)
- ["security webauthn凭据删除"](#)

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。