



# WebAuthn MFAを使用した認証と許可

## ONTAP 9

NetApp  
December 20, 2024

# 目次

WebAuthn MFAを使用した認証と許可 .....	1
WebAuthn多要素認証の概要 .....	1
ONTAP System Managerのユーザまたはグループに対してWebAuthn MFAを有効にする .....	1
ONTAP System ManagerユーザのWebAuthn MFAを無効にする .....	3
ONTAP WebAuthn MFA設定の表示とクレデンシャルの管理 .....	4

# WebAuthn MFAを使用した認証と許可

## WebAuthn多要素認証の概要

ONTAP 9.16.1以降では、管理者がログインするユーザに対してWebAuthn多要素認証(MFA)を有効にすることができます。これにより、2つ目の認証形式としてFIDO2キー(YubiKeyなど)を使用したSystem Managerログインが有効になります。デフォルトでは、新規および既存のONTAPユーザに対してWebAuthn MFAは無効になっています。

WebAuthn MFAは、最初の認証方式に次のタイプの認証を使用するユーザおよびグループでサポートされません。

- ユーザ: パスワード、ドメイン、またはnsswitch
- グループ: ドメインまたはnsswitch

ユーザの2つ目の認証方式としてWebAuthn MFAを有効にすると、System Managerにログインしたときにハードウェア認証サーバを登録するように求められます。登録後、秘密鍵はオーセンティケータに格納され、公開鍵はONTAPに格納されます。

ONTAPは、ユーザごとに1つのWebAuthnクレデンシャルをサポートします。ユーザがオーセンティケータを失い、オーセンティケータを交換する必要がある場合、ONTAP管理者はそのユーザのWebAuthnクレデンシャルを削除して、ユーザが次のログイン時に新しいオーセンティケータを登録できるようにする必要があります。



2つ目の認証方式としてWebAuthn MFAを有効にしているユーザは"<https://myontap.example.com>、IPアドレス(など"<https://192.168.100.200>"</a>)ではなくFQDN(など)を使用してSystem Managerにアクセスする必要があります。WebAuthn MFAが有効なユーザの場合、IPアドレスを使用してSystem Managerにログインしようとすると拒否されます。

## ONTAP System Managerのユーザまたはグループに対してWebAuthn MFAを有効にする

ONTAP管理者は、[WebAuthn MFA]オプションを有効にして新しいユーザまたはグループを追加するか、既存のユーザまたはグループに対してオプションを有効にすることで、System Managerのユーザまたはグループに対してWebAuthn MFAを有効にできます。



ユーザまたはグループの2番目の認証方式としてWebAuthn MFAを有効にすると、System Managerに次回ログインしたときに、ユーザ(またはそのグループ内のすべてのユーザ)にハードウェアFIDO2デバイスの登録が求められます。この登録はユーザーのローカルオペレーティングシステムによって処理され、通常はセキュリティキーの挿入、パスキーの作成、セキュリティキーのタッチ(サポートされている場合)で構成されます。

## 新しいユーザまたはグループの作成時に**WebAuthn MFA**を有効にする

System ManagerまたはONTAP CLIを使用して、WebAuthn MFAを有効にして新しいユーザまたはグループを作成できます。

### System Manager

1. [\* Cluster]>[Settings] (設定) \*を選択します。
2. [ユーザとロール]\*の横にある矢印アイコンを選択します。
3. [Users]\*で[Add]\*を選択します。
4. ユーザまたはグループの名前を指定し、\* Role \*のドロップダウンメニューでロールを選択します。
5. ユーザまたはグループのログイン方法とパスワードを指定します。

WebAuthn MFAは、ユーザに対しては「password」、「domain」、または「nsswitch」、グループに対しては「domain」または「nsswitch」のログイン方法をサポートしています。

6. [MFA for HTTP]列で、\*[Enabled]\*を選択します。
7. [保存 ( Save ) ]を選択します。

### CLI

1. WebAuthn MFAを有効にして新しいユーザまたはグループを作成します。

次の例では、2番目の認証方式として「publickey」を選択してWebAuthn MFAを有効にしています。

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

## 既存のユーザまたはグループに対して**WebAuthn MFA**を有効にする

既存のユーザまたはグループに対してWebAuthn MFAを有効にすることができます。

## System Manager

1. [\* Cluster]>[Settings] (設定) \*を選択します。
2. [ユーザとロール]\*の横にある矢印アイコンを選択します。
3. ユーザとグループのリストで、編集するユーザまたはグループのオプションメニューを選択します。

WebAuthn MFAは、ユーザに対しては「password」、「domain」、または「nsswitch」、グループに対しては「domain」または「nsswitch」のログイン方法をサポートしています。

4. そのユーザの\* MFA for HTTP 列で Enabled \*を選択します。
5. [保存 ( Save ) ]を選択します。

## CLI

1. 既存のユーザまたはグループを変更して、そのユーザまたはグループに対してWebAuthn MFAを有効にします。

次の例では、2番目の認証方式として「publickey」を選択してWebAuthn MFAを有効にしています。

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

## 詳細

これらのコマンドについては、ONTAPのマニュアルページを参照してください。

- "security login create"
- "security login modify"

## ONTAP System ManagerユーザのWebAuthn MFAを無効にする

ONTAP管理者は、System ManagerまたはONTAP CLIでユーザまたはグループを編集することで、ユーザまたはグループのWebAuthn MFAを無効にできます。

### 既存のユーザまたはグループに対してWebAuthn MFAを無効にする

既存のユーザまたはグループのWebAuthn MFAはいつでも無効にできます。



登録済みクレデンシャルを無効にしても、クレデンシャルは保持されます。今後クレデンシャルを再度有効にすると、同じクレデンシャルが使用されるため、ユーザがログイン時に再登録する必要はありません。

## System Manager

1. [\* Cluster]>[Settings] (設定) \*を選択します。
2. [ユーザとロール]\*の横にある矢印アイコンを選択します。
3. ユーザとグループのリストで、編集するユーザまたはグループを選択します。
4. そのユーザの\* MFA for HTTP 列で Disabled \*を選択します。
5. [保存 ( Save ) ]を選択します。

## CLI

1. 既存のユーザまたはグループを変更して、そのユーザまたはグループのWebAuthn MFAを無効にします。

次の例では、2番目の認証方式として「none」を選択してWebAuthn MFAを無効にしています。

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

## 詳細

このコマンドについては、ONTAPのマニュアルページを参照してください。

- ["security login modify"](#)

## ONTAP WebAuthn MFA設定の表示とクレデンシャルの管理

ONTAP管理者は、クラスタ全体のWebAuthn MFA設定を表示し、WebAuthn MFAのユーザおよびグループのクレデンシャルを管理できます。

**WebAuthn MFA**のクラスタ設定を表示します。

ONTAP CLIを使用して、WebAuthn MFAのクラスタ設定を表示できます。

### 手順

1. WebAuthn MFAのクラスタ設定を表示します。必要に応じて、引数を使用してStorage VMを指定できます  
vserver。

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

## サポートされている公開鍵WebAuthn MFAアルゴリズムの表示

Storage VMまたはクラスタのWebAuthn MFAでサポートされている公開鍵アルゴリズムを表示できます。

手順

1. サポートされている公開鍵WebAuthn MFAアルゴリズムを列挙します。必要に応じて、引数を使用してStorage VMを指定できます `vserver`。

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

## 登録済みWebAuthn MFAクレデンシャルの表示

ONTAP管理者は、すべてのユーザの登録済みWebAuthnクレデンシャルを表示できます。この手順を使用する管理者以外のユーザは、自分の登録済みWebAuthnクレデンシャルのみを表示できます。

手順

1. 登録されたWebAuthn MFAクレデンシャルを表示します。

```
security webauthn credentials show
```

## 登録済みWebAuthn MFAクレデンシャルの削除

登録済みのWebAuthn MFAクレデンシャルを削除できます。これは、ユーザーのハードウェアキーが紛失したり、盗まれたり、使用されなくなったりした場合に便利です。ユーザーが元のハードウェアオーセンティケータを持っていて、新しいものに置き換えたい場合は、登録されたクレデンシャルを削除することもできます。クレデンシャルを削除すると、ユーザは交換用オーセンティケータを登録するように求められます。



ユーザの登録済みクレデンシャルを削除しても、そのユーザのWebAuthn MFAは無効になりません。ユーザがハードウェアオーセンティケータを紛失し、交換する前にログインする必要がある場合は、次の手順とユーザの手順を使用してクレデンシャルを削除する"[WebAuthn MFAを無効にする](#)"必要があります。

## System Manager

1. [\* Cluster]>[Settings] (設定) \*を選択します。
2. [ユーザとロール]\*の横にある矢印アイコンを選択します。
3. ユーザとグループのリストで、クレデンシャルを削除するユーザまたはグループのオプションメニューを選択します。
4. [HTTPクレデンシャルのMFAを削除する]\*を選択します。
5. 「\* 削除」を選択します。

## CLI

1. 登録済みクレデンシャルを削除します。次の点に注意してください。
  - 必要に応じて、ユーザのStorage VMを指定できます。省略すると、クラスタレベルでクレデンシャルが削除されます。
  - 必要に応じて、クレデンシャルを削除するユーザのユーザ名を指定できます。省略すると、現在のユーザのクレデンシャルが削除されます。

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

## 詳細

これらのコマンドについては、ONTAPのマニュアルページを参照してください。

- ["security webauthn show"](#)
- ["サポートされるセキュリティwebauthn - algorithms show"](#)
- ["security webauthn credentials show"](#)
- ["セキュリティwebauthnクレデンシャルの削除"](#)



## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。