



# WebAuthn MFA를 사용한 인증 및 권한 부여

## ONTAP 9

NetApp  
January 17, 2025

# 목차

WebAuthn MFA를 사용한 인증 및 권한 부여 .....	1
WebAuthn 다중 요소 인증 개요 .....	1
ONTAP 시스템 관리자 사용자 또는 그룹에 대해 WebAuthn MFA를 활성화합니다 .....	1
ONTAP 시스템 관리자 사용자를 위한 WebAuthn MFA를 비활성화합니다 .....	3
ONTAP WebAuthn MFA 설정을 보고 자격 증명을 관리합니다 .....	4

# WebAuthn MFA를 사용한 인증 및 권한 부여

## WebAuthn 다중 요소 인증 개요

관리자는 ONTAP 9.16.1부터 System Manager에 로그인하는 사용자에게 WebAuthn MFA(다중 요소 인증)를 활성화할 수 있습니다. 이렇게 하면 FIDO2 키(예: YubiKey)를 두 번째 인증 형태로 사용하여 System Manager 로그인을 사용할 수 있습니다. 기본적으로 WebAuthn MFA는 신규 및 기존 ONTAP 사용자에게 대해 사용되지 않습니다.

WebAuthn MFA는 첫 번째 인증 방법에 대해 다음 유형의 인증을 사용하는 사용자 및 그룹에 대해 지원됩니다.

- 사용자: 암호, 도메인 또는 nsswitch
- 그룹: domain 또는 nsswitch

WebAuthn MFA를 사용자에게 대한 두 번째 인증 방법으로 설정한 후 System Manager에 로그인할 때 사용자에게 하드웨어 인증자를 등록하라는 메시지가 표시됩니다. 등록 후 개인 키는 인증자에 저장되고 공개 키는 ONTAP에 저장됩니다.

ONTAP는 사용자당 하나의 WebAuthn 자격 증명을 지원합니다. 사용자가 인증 프로그램을 분실하여 교체해야 하는 경우 ONTAP 관리자는 다음에 로그인할 때 새 인증 프로그램을 등록할 수 있도록 해당 사용자의 WebAuthn 자격 증명을 삭제해야 합니다.



두 번째 인증 방법으로 WebAuthn MFA를 사용하도록 설정한 사용자는 "<https://myontap.example.com>"</a> IP 주소(예: "<https://192.168.100.200>"</a>) 대신 FQDN(예:)을 사용하여 System Manager에 액세스해야 합니다. WebAuthn MFA가 활성화된 사용자의 경우 IP 주소를 사용하여 System Manager 로그인 시도가 거부됩니다.

## ONTAP 시스템 관리자 사용자 또는 그룹에 대해 WebAuthn MFA를 활성화합니다

ONTAP 관리자는 WebAuthn MFA 옵션이 활성화된 새 사용자 또는 그룹을 추가하거나 기존 사용자 또는 그룹에 대한 옵션을 활성화하여 시스템 관리자 사용자 또는 그룹에 대해 WebAuthn MFA를 활성화할 수 있습니다.



WebAuthn MFA를 사용자 또는 그룹에 대한 두 번째 인증 방법으로 활성화하면 사용자(또는 해당 그룹의 모든 사용자)는 다음에 System Manager에 로그인할 때 하드웨어 FIDO2 장치를 등록하라는 메시지가 표시됩니다. 이 등록은 사용자의 로컬 운영 체제에 의해 처리되며, 일반적으로 보안 키 삽입, 암호 작성 및 보안 키(지원되는 경우)로 구성됩니다.

### 새 사용자 또는 그룹을 만들 때 WebAuthn MFA를 활성화합니다

System Manager 또는 ONTAP CLI를 사용하여 WebAuthn MFA가 설정된 새 사용자 또는 그룹을 생성할 수 있습니다.

## 시스템 관리자

1. 클러스터 > 설정 \* 을 선택합니다.
2. 사용자 및 역할 \* 옆에 있는 화살표 아이콘을 선택합니다.
3. 사용자 \* 아래에서 \* 추가 \* 를 선택합니다.
4. 사용자 또는 그룹 이름을 지정하고 \* Role \* 의 드롭다운 메뉴에서 역할을 선택합니다.
5. 사용자 또는 그룹의 로그인 방법과 암호를 지정합니다.

WebAuthn MFA는 사용자를 위한 "password", "domain" 또는 "nsswitch", 그룹에 대한 "domain" 또는 "nsswitch"의 로그인 방법을 지원합니다.

6. HTTP \* 용 MFA 열에서 \* 사용 \* 을 선택합니다.
7. 저장 \* 을 선택합니다.

## CLI를 참조하십시오

1. WebAuthn MFA를 사용하도록 설정한 새 사용자 또는 그룹을 만듭니다.

다음 예제에서 WebAuthn MFA는 두 번째 인증 방법으로 "publickey"를 선택하여 사용할 수 있습니다.

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

## 기존 사용자 또는 그룹에 대해 WebAuthn MFA를 활성화합니다

기존 사용자 또는 그룹에 대해 WebAuthn MFA를 활성화할 수 있습니다.

## 시스템 관리자

1. 클러스터 > 설정 \* 을 선택합니다.
2. 사용자 및 역할 \* 옆에 있는 화살표 아이콘을 선택합니다.
3. 사용자 및 그룹 목록에서 편집할 사용자 또는 그룹의 옵션 메뉴를 선택합니다.

WebAuthn MFA는 사용자를 위한 "password", "domain" 또는 "nsswitch", 그룹에 대한 "domain" 또는 "nsswitch"의 로그인 방법을 지원합니다.

4. 해당 사용자의 \* MFA for HTTP \* 열에서 \* Enabled \* 를 선택합니다.
5. 저장 \* 을 선택합니다.

## CLI를 참조하십시오

1. 기존 사용자 또는 그룹을 수정하여 해당 사용자 또는 그룹에 대해 WebAuthn MFA를 활성화합니다.

다음 예제에서 WebAuthn MFA는 두 번째 인증 방법으로 "publickey"를 선택하여 사용할 수 있습니다.

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

## 자세한 정보

이러한 명령에 대한 자세한 내용은 ONTAP 설명서 페이지를 참조하십시오.

- ["보안 로그인 생성"](#)
- ["보안 로그인 수정"](#)

## ONTAP 시스템 관리자 사용자를 위한 WebAuthn MFA를 비활성화합니다

ONTAP 관리자는 System Manager 또는 ONTAP CLI를 사용하여 사용자 또는 그룹을 편집하여 사용자 또는 그룹에 대해 WebAuthn MFA를 사용하지 않도록 설정할 수 있습니다.

### 기존 사용자 또는 그룹에 대해 WebAuthn MFA를 비활성화합니다

언제든지 기존 사용자 또는 그룹에 대해 WebAuthn MFA를 비활성화할 수 있습니다.



등록된 자격 증명을 사용하지 않도록 설정하면 자격 증명에 유지됩니다. 나중에 자격 증명을 다시 활성화하면 동일한 자격 증명에 사용되므로 사용자가 로그인할 때 다시 등록할 필요가 없습니다.

## 시스템 관리자

1. 클러스터 > 설정 \* 을 선택합니다.
2. 사용자 및 역할 \* 옆에 있는 화살표 아이콘을 선택합니다.
3. 사용자 및 그룹 목록에서 편집할 사용자 또는 그룹을 선택합니다.
4. 해당 사용자의 \* MFA for HTTP \* 열에서 \* Disabled \* 를 선택합니다.
5. 저장 \* 을 선택합니다.

## CLI를 참조하십시오

1. 기존 사용자 또는 그룹을 수정하여 해당 사용자 또는 그룹에 대해 WebAuthn MFA를 비활성화합니다.

다음 예에서는 두 번째 인증 방법으로 "none"을 선택하여 WebAuthn MFA를 사용할 수 없습니다.

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

## 자세한 정보

이 명령에 대한 ONTAP 설명서 페이지를 참조하십시오.

- ["보안 로그인 수정"](#)

## ONTAP WebAuthn MFA 설정을 보고 자격 증명을 관리합니다

ONTAP 관리자는 클러스터 전체의 WebAuthn MFA 설정을 보고 WebAuthn MFA에 대한 사용자 및 그룹 자격 증명을 관리할 수 있습니다.

### WebAuthn MFA에 대한 클러스터 설정을 봅니다

ONTAP CLI를 사용하여 WebAuthn MFA에 대한 클러스터 설정을 볼 수 있습니다.

#### 단계

1. WebAuthn MFA에 대한 클러스터 설정을 봅니다. 선택적으로 인수를 사용하여 스토리지 VM을 지정할 수 `vserver` 있습니다.

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

## 지원되는 공개 키 WebAuthn MFA 알고리즘을 봅니다

스토리지 VM 또는 클러스터에 대해 WebAuthn MFA에 대해 지원되는 공개 키 알고리즘을 볼 수 있습니다.

단계

1. 지원되는 공개 키 WebAuthn MFA 알고리즘을 나열합니다. 선택적으로 인수를 사용하여 스토리지 VM을 지정할 수 `vserver` 있습니다.

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

## 등록된 WebAuthn MFA 자격 증명을 봅니다

ONTAP 관리자는 모든 사용자에게 대해 등록된 WebAuthn 자격 증명을 볼 수 있습니다. 이 절차를 사용하는 관리자가 아닌 사용자는 자신의 등록된 WebAuthn 자격 증명만 볼 수 있습니다.

단계

1. 등록된 WebAuthn MFA 자격 증명을 봅니다.

```
security webauthn credentials show
```

## 등록된 WebAuthn MFA 자격 증명을 제거합니다

등록된 WebAuthn MFA 자격 증명을 제거할 수 있습니다. 이 기능은 사용자의 하드웨어 키를 분실하거나 도난당했거나 더 이상 사용하지 않는 경우에 유용합니다. 사용자가 원래 하드웨어 인증기를 가지고 있지만 새 인증기로 교체하려는 경우 등록된 자격 증명을 제거할 수도 있습니다. 자격 증명을 제거하면 사용자에게 대체 인증자를 등록하라는 메시지가 표시됩니다.



사용자에게 대해 등록된 자격 증명을 제거해도 해당 사용자에게 대해 WebAuthn MFA가 해제되지 않습니다. 사용자가 하드웨어 인증 프로그램을 분실하여 교체하기 전에 로그인해야 하는 경우, 다음 단계를 사용하여 자격 증명을 제거해야 **"WebAuthn MFA를 비활성화합니다"**합니다.

## 시스템 관리자

1. 클러스터 > 설정 \* 을 선택합니다.
2. 사용자 및 역할 \* 옆에 있는 화살표 아이콘을 선택합니다.
3. 사용자 및 그룹 목록에서 자격 증명을 제거하려는 사용자 또는 그룹의 옵션 메뉴를 선택합니다.
4. Remove MFA for HTTP credentials \* 를 선택합니다.
5. 제거 \* 를 선택합니다.

## CLI를 참조하십시오

1. 등록된 자격 증명을 삭제합니다. 다음 사항에 유의하십시오.
  - 선택적으로 사용자의 스토리지 VM을 지정할 수 있습니다. 이 인수를 생략하면 클러스터 레벨에서 자격 증명이 제거됩니다.
  - 필요한 경우 자격 증명을 삭제할 사용자의 사용자 이름을 지정할 수 있습니다. 생략하면 현재 사용자에게 대한 자격 증명도 제거됩니다.

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

## 자세한 정보

이러한 명령에 대한 자세한 내용은 ONTAP 설명서 페이지를 참조하십시오.

- ["보안 webauthn 쇼"](#)
- ["보안 webauthn 지원 - 알고리즘이 표시됩니다"](#)
- ["보안 webauthn 자격 증명에 표시됩니다"](#)
- ["보안 webauthn 자격 증명을 삭제합니다"](#)



## 저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.