



# 기본 인터페이스

## SANtricity 11.8

NetApp  
December 16, 2024

# 목차

기본 인터페이스 .....	1
Unified Manager 인터페이스 개요 .....	1
지원되는 브라우저 .....	2
관리자 암호 보호를 설정합니다 .....	2
admin 암호를 변경합니다 .....	3
세션 시간 제한을 관리합니다 .....	3

# 기본 인터페이스

## Unified Manager 인터페이스 개요


Unified Manager는 웹 기반 인터페이스로, 단일 뷰에서 여러 스토리지 어레이를 관리할 수 있습니다.

### 기본 페이지

Unified Manager에 로그인하면 기본 페이지가 열리고 \* Manage - All \* 가 표시됩니다. 이 페이지에서는 네트워크에서 검색된 스토리지 배열의 목록을 스크롤하고, 해당 상태를 보고, 단일 배열 또는 어레이 그룹에서 작업을 수행할 수 있습니다.

### 탐색 사이드바

탐색 사이드바에서 Unified Manager 기능에 액세스할 수 있습니다.

영역	설명
관리	네트워크에서 스토리지 시스템을 검색하고, 어레이에 대한 SANtricity 시스템 관리자를 시작하고, 한 어레이에서 여러 어레이로 설정을 가져오고, 어레이 그룹을 관리합니다. 설정 가져오기 및 스토리지 그룹 생성과 같은 작업을 수행할 스토리지 이름 옆의 확인란을 선택합니다. 각 행의 끝에 있는 줄임표는 이름 바꾸기와 같은 단일 배열의 작업에 대한 인라인 메뉴를 제공합니다.
운영	한 어레이에서 다른 어레이로 설정을 가져오는 것과 같은 배치 작업의 진행률을 봅니다.   스토리지 배열의 상태가 최적이지 아닌 경우 일부 작업을 사용할 수 없습니다.
인증서 관리	브라우저와 클라이언트 간 인증을 위한 인증서를 관리합니다.
액세스 관리	Unified Manager 인터페이스에 대한 사용자 인증 설정
지원	기술 지원 옵션, 리소스 및 연락처를 봅니다.

### 인터페이스 설정 및 도움말

인터페이스 오른쪽 상단에서 도움말 및 기타 설명서에 액세스할 수 있습니다. 로그인 이름 옆의 드롭다운에서 사용할 수 있는 관리 옵션에 액세스할 수도 있습니다.

### 사용자 로그인 및 암호

시스템에 로그인한 현재 사용자가 인터페이스의 오른쪽 상단에 표시됩니다.

사용자 및 암호에 대한 자세한 내용은 다음을 참조하십시오.

- "관리자 암호 보호를 설정합니다"
- "admin 암호를 변경합니다"
- "로컬 사용자 프로필에 대한 암호를 변경합니다"

## 지원되는 브라우저

Unified Manager는 다양한 유형의 브라우저에서 액세스할 수 있습니다.

다음 브라우저 및 버전이 지원됩니다.

브라우저	최소 버전
Google Chrome	89
Mozilla Firefox	80
사파리	14
Microsoft Edge를 참조하십시오	90



웹 서비스 프록시는 설치되어 브라우저에서 사용할 수 있어야 합니다.

## 관리자 암호 보호를 설정합니다

관리자 암호를 사용하여 Unified Manager를 구성하여 무단 액세스로부터 보호해야 합니다.

### 관리자 암호 및 사용자 프로필

Unified Manager를 처음 시작하면 관리자 암호를 설정하라는 메시지가 표시됩니다. admin 암호를 가진 모든 사용자는 스토리지 배열에 대한 구성을 변경할 수 있습니다.

관리자 암호 외에도 Unified Manager 인터페이스에는 하나 이상의 역할이 매핑되어 있는 사전 구성된 사용자 프로필이 포함되어 있습니다. 자세한 내용은 ["액세스 관리 작동 방식"](#)참조하십시오.

사용자 및 매핑을 변경할 수 없습니다. 암호만 수정할 수 있습니다. 암호를 변경하려면 다음을 참조하십시오.

- "admin 암호를 변경합니다"
- "로컬 사용자 프로필에 대한 암호를 변경합니다"

### 세션 시간 초과

단일 관리 세션 중에 암호를 입력하라는 메시지가 한 번만 표시됩니다. 기본적으로 30분 동안 활동이 없으면 세션 시간이 초과되며, 이 경우 암호를 다시 입력해야 합니다. 다른 사용자가 다른 관리 클라이언트에서 소프트웨어에 액세스하고 세션이 진행되는 동안 암호를 변경하는 경우 다음에 구성 작업 또는 보기 작업을 시도할 때 암호를 입력하라는 메시지가 표시됩니다.

보안상의 이유로 소프트웨어가 "잠금" 상태가 되기 5회만 암호를 입력할 수 있습니다. 이 상태에서는 소프트웨어가 후속 암호 시도를 거부합니다. 암호를 다시 입력하기 전에 10분 정도 기다린 후 "정상" 상태로 재설정해야 합니다.

세션 시간 초과를 조정하거나 세션 시간 초과를 모두 비활성화할 수 있습니다. 자세한 내용은 ["세션 시간 제한을 관리합니다"](#) 참조하십시오.

## admin 암호를 변경합니다

Unified Manager에 액세스하는 데 사용되는 admin 암호를 변경할 수 있습니다.

시작하기 전에

- 루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.
- 현재 관리자 암호를 알아야 합니다.

이 작업에 대해

암호를 선택할 때는 다음 지침을 염두에 두십시오.

- 암호는 대/소문자를 구분합니다.
- 후행 공백은 암호가 설정되어 있을 때 암호에서 제거되지 않습니다. 암호에 공백이 포함된 경우 해당 공백을 포함해야 합니다.
- 보안을 강화하려면 15자 이상의 영숫자 문자를 사용하고 암호를 자주 변경하십시오.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 로컬 사용자 역할 \* 탭을 선택합니다.
3. 표에서 \* admin \* 사용자를 선택합니다.

암호 변경 단추를 사용할 수 있게 됩니다.

4. 암호 변경 \* 을 선택합니다.

암호 변경 대화 상자가 열립니다.

5. 로컬 사용자 암호에 대해 최소 암호 길이를 설정하지 않은 경우 사용자가 시스템에 액세스하기 위해 암호를 입력하도록 확인란을 선택합니다.
6. 두 필드에 새 암호를 입력합니다.
7. 이 작업을 확인하려면 로컬 관리자 암호를 입력한 다음 \* 변경 \* 을 클릭합니다.

## 세션 시간 제한을 관리합니다

Unified Manager에 대한 시간 초과를 구성하여 지정된 시간 이후에 비활성 세션의 연결을 끊을 수 있습니다.

이 작업에 대해

기본적으로 Unified Manager의 세션 제한 시간은 30분입니다. 이 시간을 조정하거나 세션 시간 초과를 모두 비활성화할 수 있습니다.



스토리지에 포함된 SAML(Security Assertion Markup Language) 기능을 사용하여 액세스 관리를 구성하는 경우 사용자의 SSO 세션이 최대 제한에 도달하면 세션 시간 초과가 발생할 수 있습니다. 이 문제는 System Manager 세션 시간이 초과되기 전에 발생할 수 있습니다.

#### 단계

1. 메뉴 표시줄에서 사용자 로그인 이름 옆에 있는 드롭다운 화살표를 선택합니다.
2. Enable/Disable session timeout \* 을 선택합니다.

Enable/Disable Session Timeout(세션 시간 제한 활성화/비활성화) 대화 상자가 열립니다.

3. 스피너 컨트롤을 사용하여 시간을 분 단위로 늘리거나 줄입니다.

설정할 수 있는 최소 시간 초과는 15분입니다.



세션 시간 초과를 비활성화하려면 \* 시간 길이 설정... \* 확인란의 선택을 취소합니다.

4. 저장 \* 을 클릭합니다.

## 저작권 정보

Copyright © 2024 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.