# 인증서
## SANtricity 11.7

NetApp
February 12, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/e-series-santricity-117/um-certificates/overview-certificates-um.html on February 12, 2024. Always check docs.netapp.com for the latest.

# 목차


인증서 . . . . . 1
- 인증서 개요 . . . . . 1
- 개념 . . . . . 1
- 관리 시스템에 CA 서명 인증서를 사용합니다 . . . . . 4
- 관리 인증서를 재설정합니다 . . . . . 6
- 스토리지 인증서를 사용합니다 . . . . . 6
- 인증서를 관리합니다 . . . . . 8

# 인증서

## 인증서 개요

인증서 관리를 사용하면 CSR(인증서 서명 요청)을 생성하고 인증서를 가져오고 기존 인증서를 관리할 수 있습니다.

### 인증서란 무엇입니까?

_Certificates_는 인터넷 보안 통신을 위해 웹 사이트 및 서버와 같은 온라인 엔터티를 식별하는 디지털 파일입니다. 인증서 유형에는 두 가지가 있습니다. CA(인증 기관)에서 _signed certificate_를 검증하고, 타사 대신 엔터티의 소유자가 _self-signed certificate_를 확인합니다.

자세한 내용:

- "인증서 작동 방식"
- "인증서 용어"

### 인증서를 구성하려면 어떻게 합니까?

인증서 관리에서 Unified Manager를 호스팅하는 관리 스테이션에 대한 인증서를 구성하고 스토리지 시스템의 컨트롤러에 대한 인증서를 가져올 수 있습니다.

자세한 내용:

- "관리 시스템에 CA 서명 인증서를 사용합니다"
- "스토리지에 대한 인증서를 가져옵니다"

# 개념

## 인증서 작동 방식

### 인증서는 인터넷 보안 통신을 위해 웹 사이트 및 서버와 같은 온라인 엔터티를 식별하는 디지털 파일입니다.

서명된 인증서

인증서는 웹 통신이 지정된 서버와 클라이언트 사이에서만 암호화된 형식으로 비공개로, 변경되지 않도록 합니다. Unified Manager를 사용하면 호스트 관리 시스템의 브라우저 인증서와 검색된 스토리지 시스템의 컨트롤러를 관리할 수 있습니다.

인증서는 신뢰할 수 있는 기관에서 서명할 수도 있고 자체 서명할 수도 있습니다. "서명"은 단순히 누군가가 소유자의 신원을 확인하고 자신의 장치를 신뢰할 수 있다는 것을 확인하는 것을 의미합니다. 스토리지 어레이에는 각 컨트롤러에서 자동으로 생성된 자체 서명 인증서가 함께 제공됩니다. 자체 서명된 인증서를 계속 사용하거나 컨트롤러와 호스트 시스템 간의 보다 안전한 연결을 위해 CA 서명 인증서를 얻을 수 있습니다.

CA 서명 인증서는 향상된 보안 보호 기능을 제공하지만(예: 중간의 공격 방지) 대규모 네트워크를 사용하는 경우 비용이 많이 들 수 있습니다. 반면 자체 서명된 인증서는 보안성이 떨어지지만 무료입니다. 따라서 자체 서명된 인증서는 프로덕션 환경이 아닌 내부 테스트 환경에 가장 많이 사용됩니다.

서명된 인증서는 신뢰할 수 있는 타사 조직인 CA(인증 기관)에서 유효성을 검사합니다. 서명된 인증서에는 개체 소유자(일반적으로 서버 또는 웹 사이트)에 대한 세부 정보, 인증서 발급 및 만료 날짜, 엔터티에 대한 유효한 도메인 및 문자와 숫자로 구성된 디지털 서명이 포함됩니다.

브라우저를 열고 웹 주소를 입력하면 시스템은 백그라운드에서 인증서 확인 프로세스를 수행하여 유효한 CA 서명 인증서가 포함된 웹 사이트에 연결 중인지 확인합니다. 일반적으로 서명된 인증서로 보호되는 사이트에는 자물쇠 아이콘과 주소에 https 지정이 포함되어 있습니다. CA 서명 인증서가 없는 웹 사이트에 연결하려고 하면 브라우저에 사이트가 안전하지 않음을 알리는 경고가 표시됩니다.

CA는 응용 프로그램 프로세스 중에 ID를 확인하는 단계를 수행합니다. 등록된 회사에 이메일을 보내고, 회사 주소를 확인하고, HTTP 또는 DNS 확인을 수행할 수 있습니다. 응용 프로그램 프로세스가 완료되면 CA는 호스트 관리 시스템에 로드할 디지털 파일을 보냅니다. 일반적으로 이러한 파일에는 다음과 같은 신뢰 체인이 포함됩니다.

- * 루트 * — 계층 구조의 맨 위에 루트 인증서가 있으며, 이 인증서에는 다른 인증서에 서명하는 데 사용되는 개인 키가 들어 있습니다. 루트는 특정 CA 조직을 식별합니다. 모든 네트워크 장치에 동일한 CA를 사용하는 경우 하나의 루트 인증서만 있으면 됩니다.
- * 중급 * — 루트에서 오프하는 것은 중간 인증서입니다. CA는 하나 이상의 중간 인증서를 발급하여 보호된 루트와 서버 인증서 간의 중간 역할을 수행합니다.
- * 서버 * — 체인 하단에 있는 서버 인증서는 웹 사이트 또는 기타 장치와 같은 특정 엔터티를 식별합니다. 스토리지 어레이의 각 컨트롤러에는 별도의 서버 인증서가 필요합니다.

### 자체 서명된 인증서

스토리지 어레이의 각 컨트롤러에는 사전 설치된 자체 서명된 인증서가 포함되어 있습니다. 자체 서명된 인증서는 타사 대신 개체 소유자가 유효성을 검사한다는 점을 제외하면 CA 서명 인증서와 비슷합니다. CA 서명 인증서와 마찬가지로 자체 서명된 인증서에는 자체 개인 키가 포함되어 있으며, 서버와 클라이언트 간의 HTTPS 연결을 통해 데이터가 암호화되고 전송되도록 합니다.

자체 서명된 인증서는 브라우저에서 "신뢰할 수 있는" 인증서가 아닙니다. 자체 서명된 인증서만 포함된 웹 사이트에 연결할 때마다 브라우저에 경고 메시지가 표시됩니다. 웹 사이트로 이동할 수 있는 경고 메시지의 링크를 클릭해야 합니다. 이렇게 하면 자체 서명된 인증서를 기본적으로 수락하게 됩니다.

### **Unified Manager**용 인증서

Unified Manager 인터페이스는 호스트 시스템의 웹 서비스 프록시와 함께 설치됩니다. 브라우저를 열고 Unified Manager에 연결하려고 하면 브라우저에서 디지털 인증서를 확인하여 호스트가 신뢰할 수 있는 소스인지 확인합니다. 브라우저에서 서버의 CA 서명 인증서를 찾지 못하면 경고 메시지가 열립니다. 이 페이지에서 웹 사이트로 이동하여 해당 세션에 대해 자체 서명된 인증서를 수락할 수 있습니다. 또는 CA로부터 서명된 디지털 인증서를 받을 수 있으므로 경고 메시지가 더 이상 표시되지 않습니다.

### 컨트롤러의 인증서

Unified Manager 세션 중에 CA 서명된 인증서가 없는 컨트롤러에 액세스하려고 하면 추가 보안 메시지가 표시될 수 있습니다. 이 경우 자체 서명된 인증서를 영구적으로 신뢰하거나 컨트롤러의 CA 서명 인증서를 가져올 수 있습니다. 그러면 웹 서비스 프록시 서버에서 이러한 컨트롤러의 들어오는 클라이언트 요청을 인증할 수 있습니다.

# 인증서 용어

다음 용어는 인증서 관리에 적용됩니다.

| 기간 | 설명 |
| --- | --- |
| CA | CA(인증 기관)는 인터넷 보안을 위해 디지털 인증서라는 전자 문서를 발급하는 신뢰할 수 있는 엔터티입니다. 이러한 인증서는 클라이언트와 서버 간의 보안 연결을 허용하는 웹사이트 소유자를 식별합니다. |
| CSR | CSR(인증서 서명 요청)은 신청자가 CA(인증 기관)로 보내는 메시지입니다. CSR은 CA가 인증서를 발급하는 데 필요한 정보를 확인합니다. |
| 인증서 | 인증서는 보안 목적으로 사이트의 소유자를 식별하므로 공격자가 사이트를 가장할 수 없습니다. 인증서에는 사이트 소유자에 대한 정보와 이 정보를 인증(서명)한 신뢰할 수 있는 엔터티의 ID가 포함되어 있습니다. |
| 인증서 체인 | 인증서에 보안 계층을 추가하는 파일의 계층 구조입니다. 일반적으로 체인은 계층 맨 위에 루트 인증서 하나, 중간 인증서 하나 이상 및 엔터티를 식별하는 서버 인증서를 포함합니다. |
| 중간 인증서 | 하나 이상의 중간 인증서가 인증서 체인의 루트에서 분기됩니다. CA는 하나 이상의 중간 인증서를 발급하여 보호된 루트와 서버 인증서 간의 중간 역할을 수행합니다. |
| 키 저장소 | 키 저장소는 해당 공개 키 및 인증서와 함께 개인 키가 들어 있는 호스트 관리 시스템의 리포지토리입니다. 이러한 키와 인증서는 컨트롤러와 같은 사용자 고유의 엔터티를 식별합니다. |
| 루트 인증서입니다 | 루트 인증서는 인증서 체인의 계층 구조 맨 위에 있으며 다른 인증서에 서명하는 데 사용되는 개인 키를 포함합니다. 루트는 특정 CA 조직을 식별합니다. 모든 네트워크 장치에 동일한 CA를 사용하는 경우 하나의 루트 인증서만 있으면 됩니다. |
| 서명된 인증서 | CA(인증 기관)에서 유효성을 검사하는 인증서입니다. 이 데이터 파일에는 개인 키가 포함되어 있으며 HTTPS 연결을 통해 서버와 클라이언트 간에 암호화된 형식으로 데이터가 전송됩니다. 또한 서명된 인증서에는 개체 소유자(일반적으로 서버 또는 웹 사이트)에 대한 세부 정보와 문자와 숫자로 구성된 디지털 서명이 포함됩니다. 서명된 인증서는 신뢰 체인을 사용하므로 프로덕션 환경에서 가장 많이 사용됩니다. "CA 서명 인증서" 또는 "관리 인증서"라고도 합니다. |
| 자체 서명된 인증서 | 자체 서명된 인증서는 해당 엔터티의 소유자에 의해 유효성이 검사됩니다. 이 데이터 파일에는 개인 키가 포함되어 있으며 HTTPS 연결을 통해 서버와 클라이언트 간에 암호화된 형식으로 데이터가 전송됩니다. 문자와 숫자로 구성된 디지털 서명도 포함되어 있습니다. 자체 서명된 인증서는 CA 서명 인증서와 동일한 신뢰 체인을 사용하지 않으므로 테스트 환경에서 가장 많이 사용됩니다. "사전 설치된" 인증서라고도 합니다. |
| 서버 인증서 | 서버 인증서는 인증서 체인의 맨 아래에 있습니다. 웹 사이트 또는 기타 장치와 같은 특정 엔터티를 식별합니다. 스토리지 시스템의 각 컨트롤러에는 별도의 서버 인증서가 필요합니다. |

| 기간 | 설명 |
| --- | --- |
| 트러스토어 | Truststore는 CA와 같이 신뢰할 수 있는 타사의 인증서가 포함된 저장소입니다. |

# 관리 시스템에 CA 서명 인증서를 사용합니다

Unified Manager를 호스팅하는 관리 시스템에 안전하게 액세스하기 위해 CA 서명 인증서를 받아서 가져올 수 있습니다.

시작하기 전에

보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

이 작업에 대해

CA 서명 인증서를 사용하는 것은 3단계 절차입니다.

## 1단계: CSR 파일을 완료합니다

먼저 웹 서비스 프록시 및 Unified Manager가 설치된 조직 및 호스트 시스템을 식별하는 인증서 서명 요청(CSR) 파일을 생성해야 합니다.

또는 OpenSSL과 같은 도구를 사용하여 CSR 파일을 생성하고 로 건너뛸 수 있습니다 2단계: CSR 파일을 제출합니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 관리 탭에서 * CSR 완료 * 를 선택합니다.
3. 다음 정보를 입력하고 * 다음 * 을 클릭합니다.
   - * 조직 * — 회사 또는 조직의 전체 법적 이름. Inc. 또는 Corp.와 같은 접미사를 포함합니다
   - * 조직 단위(선택 사항) * — 인증서를 처리하는 조직의 사업부입니다.
   - * 시/군/구 * — 호스트 시스템이나 업무가 위치한 도시.
   - * 주/지역(선택 사항) * — 호스트 시스템 또는 비즈니스가 위치한 주 또는 지역입니다.
   - * 국가 ISO 코드 * — 미국 등 해당 국가의 2자리 ISO(International Organization for Standardization) 코드입니다.
4. 웹 서비스 프록시가 설치된 호스트 시스템에 대한 다음 정보를 입력합니다.
   - * 공통 이름 * — 웹 서비스 프록시가 설치된 호스트 시스템의 IP 주소 또는 DNS 이름입니다. 주소가 올바른지 확인합니다. 입력한 주소와 정확하게 일치해야 브라우저에서 Unified Manager에 액세스할 수 있습니다. http:// 또는 https://.를 포함하지 마십시오 DNS 이름은 와일드카드로 시작할 수 없습니다.
   - * 대체 IP 주소 * — 공통 이름이 IP 주소인 경우 호스트 시스템에 대한 추가 IP 주소 또는 별칭을 선택적으로 입력할 수 있습니다. 여러 항목의 경우 쉼표로 구분된 형식을 사용합니다.
   - * 대체 DNS 이름 * — 공통 이름이 DNS 이름이면 호스트 시스템에 대한 추가 DNS 이름을 입력합니다. 여러 항목의 경우 쉼표로 구분된 형식을 사용합니다. 대체 DNS 이름이 없지만 첫 번째 필드에 DNS 이름을 입력한 경우 여기에 해당 이름을 복사합니다. DNS 이름은 와일드카드로 시작할 수 없습니다.

5. 호스트 정보가 올바른지 확인합니다. 그렇지 않으면 CA에서 반환된 인증서를 가져오려고 할 때 실패합니다.
6. 마침 * 을 클릭합니다.
7. 로 이동합니다 2단계: CSR 파일을 제출합니다.

## 2단계: CSR 파일을 제출합니다

CSR(인증서 서명 요청) 파일을 생성한 후 CA(인증 기관)로 보내 Unified Manager 및 웹 서비스 프록시를 호스팅하는 시스템에 대한 서명된 관리 인증서를 받습니다.

E-Series 시스템에는 .pem, .crt, .cer 또는 .key 파일 형식을 포함하는 서명된 인증서에 대한 PEM 형식(Base64 ASCII 인코딩)이 필요합니다.

단계

1. 다운로드한 CSR 파일을 찾습니다.

   다운로드의 폴더 위치는 브라우저에 따라 다릅니다.

2. CSR 파일을 CA(예: VeriSign 또는 DigiCert)에 제출하고 서명된 인증서를 PEM 형식으로 요청합니다.

   - CSR 파일을 CA에 제출한 후 다른 CSR 파일을 다시 생성하지 마십시오. * CSR을 생성할 때마다 시스템에서 개인 및 공개 키 쌍을 생성합니다. 공개 키는 CSR의 일부이며 개인 키는 시스템의 키 저장소에 보관됩니다. 서명된 인증서를 받아서 가져오면 시스템에서 개인 키와 공개 키가 모두 원래 쌍이 되도록 합니다. 키가 일치하지 않으면 서명된 인증서가 작동하지 않으므로 CA에서 새 인증서를 요청해야 합니다.

3. CA가 서명된 인증서를 반환하면 로 이동합니다 3단계: 관리 인증서를 가져옵니다.

## 3단계: 관리 인증서를 가져옵니다

CA(인증 기관)에서 서명된 인증서를 받은 후 웹 서비스 프록시 및 Unified Manager 인터페이스가 설치된 호스트 시스템으로 인증서를 가져옵니다.

시작하기 전에

- CA로부터 서명된 인증서를 받았습니다. 이러한 파일에는 루트 인증서, 하나 이상의 중간 인증서 및 서버 인증서가 포함됩니다.
- CA가 체인 인증서 파일(예: .p7b 파일)을 제공한 경우, 루트 인증서, 하나 이상의 중간 인증서 및 서버 인증서 등 개별 파일에 체인 파일의 압축을 풀어야 합니다. Windows를 사용할 수 있습니다 `certmgr` 파일을 압축 풀기 위한 유틸리티(마우스 오른쪽 버튼을 클릭하고 메뉴 선택: 모든 작업 [내보내기]). base-64 인코딩이 권장됩니다. 내보내기가 완료되면 체인의 각 인증서 파일에 대해 CER 파일이 표시됩니다.
- 웹 서비스 프록시가 실행되고 있는 호스트 시스템에 인증서 파일을 복사했습니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 관리 탭에서 * 가져오기 * 를 선택합니다.

   인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

3. 찾아보기 * 를 클릭하여 먼저 루트 및 중간 인증서 파일을 선택한 다음 서버 인증서를 선택합니다. 외부 도구에서 CSR을 생성한 경우 CSR과 함께 생성된 개인 키 파일도 가져와야 합니다.

   대화 상자에 파일 이름이 표시됩니다.

4. 가져오기 * 를 클릭합니다.

결과

파일이 업로드되고 검증됩니다. 인증서 정보가 인증서 관리 페이지에 표시됩니다.

# 관리 인증서를 재설정합니다

## 관리 인증서를 공장 자체 서명된 원래 상태로 되돌릴 수 있습니다.

시작하기 전에

보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

이 작업에 대해

이 작업은 Web Services Proxy 및 Unified Manager가 설치된 호스트 시스템에서 현재 관리 인증서를 삭제합니다. 인증서가 재설정되면 호스트 시스템은 자체 서명된 인증서를 사용하여 되돌아갑니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 관리 탭에서 * 재설정 * 을 선택합니다.

   관리 인증서 재설정 확인 대화 상자가 열립니다.

3. 유형 `reset` 필드에서 * 재설정 * 을 클릭합니다.

   브라우저가 새로 고쳐지면 브라우저가 대상 사이트에 대한 액세스를 차단하고 사이트가 HTTP Strict Transport Security를 사용하고 있다고 보고할 수 있습니다. 이 조건은 자체 서명된 인증서로 다시 전환하면 발생합니다. 대상에 대한 액세스를 차단하는 조건을 지우려면 브라우저에서 탐색 데이터를 지워야 합니다.

결과

시스템에서 서버에서 자체 서명된 인증서를 사용하도록 되돌립니다. 따라서 사용자가 세션에 대해 자체 서명된 인증서를 수동으로 수락하라는 메시지가 표시됩니다.

# 스토리지 인증서를 사용합니다

## 스토리지에 대한 인증서를 가져옵니다

## 필요한 경우 Unified Manager를 호스팅하는 시스템에서 인증할 수 있도록 스토리지 어레이에 대한 인증서를 가져올 수 있습니다. 인증서는 CA(인증 기관)에서 서명할 수도 있고 자체 서명할 수도 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

- 신뢰할 수 있는 인증서를 가져오는 경우 System Manager를 사용하여 스토리지 배열 컨트롤러에 대한 인증서를 가져와야 합니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 신뢰할 수 있는 * 탭을 선택합니다.

   이 페이지에는 스토리지 배열에 대해 보고된 모든 인증서가 표시됩니다.

3. [인증서] 가져오기 메뉴를 선택하여 CA 인증서를 가져오거나 메뉴: 자체 서명된 [스토리지 배열 인증서] 가져오기 를 선택하여 자체 서명된 인증서를 가져옵니다.

   보기를 제한하려면 * Show certificates that are… * filtering 필드를 사용하거나 열 머리글 중 하나를 클릭하여 인증서 행을 정렬할 수 있습니다.

4. 대화 상자에서 인증서를 선택한 다음 * 가져오기 * 를 클릭합니다.

   인증서가 업로드 및 검증됩니다.

## 신뢰할 수 있는 인증서를 삭제합니다

만료된 인증서와 같이 더 이상 필요하지 않은 인증서를 하나 이상 삭제할 수 있습니다.

시작하기 전에

기존 인증서를 삭제하기 전에 새 인증서를 가져옵니다.

> 루트 또는 중간 인증서를 삭제하면 여러 스토리지 시스템이 동일한 인증서 파일을 공유할 수 있으므로 여러 스토리지 시스템에 영향을 줄 수 있습니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 신뢰할 수 있는 * 탭을 선택합니다.
3. 테이블에서 하나 이상의 인증서를 선택한 다음 * 삭제 * 를 클릭합니다.

   > 사전 설치된 인증서에는 * 삭제 * 기능을 사용할 수 없습니다.

   신뢰할 수 있는 인증서 삭제 확인 대화 상자가 열립니다.

4. 삭제를 확인한 다음 * 삭제 * 를 클릭합니다.

   인증서가 테이블에서 제거됩니다.

## 신뢰할 수 없는 인증서를 확인합니다

신뢰할 수 없는 인증서는 스토리지 어레이에서 Unified Manager에 대한 보안 연결을 설정하려고 시도하지만 연결이 보안으로 확인하지 못할 때 발생합니다.

인증서 페이지에서는 스토리지 배열에서 자체 서명된 인증서를 가져오거나 신뢰할 수 있는 타사에서 발급한 CA(인증 기관) 인증서를 가져와 신뢰할 수 없는 인증서를 확인할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다.
- CA 서명 인증서를 가져올 계획인 경우:
  - 스토리지 배열의 각 컨트롤러에 대한 인증서 서명 요청(.csr 파일)을 생성하여 CA로 보냈습니다.
  - CA가 신뢰할 수 있는 인증서 파일을 반환했습니다.
  - 인증서 파일은 로컬 시스템에서 사용할 수 있습니다.

이 작업에 대해

다음 중 하나라도 해당되는 경우 신뢰할 수 있는 CA 인증서를 추가로 설치해야 할 수 있습니다.

- 최근에 스토리지 배열을 추가했습니다.
- 하나 이상의 인증서가 만료되었습니다.
- 하나 이상의 인증서가 해지되었습니다.
- 하나 이상의 인증서에 루트 또는 중간 인증서가 없습니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 신뢰할 수 있는 * 탭을 선택합니다.

   이 페이지에는 스토리지 배열에 대해 보고된 모든 인증서가 표시됩니다.

3. [인증서] 가져오기 메뉴를 선택하여 CA 인증서를 가져오거나 메뉴: 자체 서명된 [스토리지 배열 인증서] 가져오기 를 선택하여 자체 서명된 인증서를 가져옵니다.

   보기를 제한하려면 * Show certificates that are… * filtering 필드를 사용하거나 열 머리글 중 하나를 클릭하여 인증서 행을 정렬할 수 있습니다.

4. 대화 상자에서 인증서를 선택한 다음 * 가져오기 * 를 클릭합니다.

   인증서가 업로드 및 검증됩니다.

# 인증서를 관리합니다

## 인증서를 봅니다

## 인증서를 사용하는 조직, 인증서를 발급한 기관, 유효 기간 및 지문(고유 식별자)을 포함하는 인증서의 요약 정보를 볼 수 있습니다.

시작하기 전에

보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 다음 탭 중 하나를 선택합니다.
   - * 관리 * — 웹 서비스 프록시를 호스팅하는 시스템의 인증서를 표시합니다. 관리 인증서는 CA(인증 기관)에서 자체 서명하거나 승인할 수 있습니다. Unified Manager에 안전하게 액세스할 수 있습니다.
   - * 신뢰 * — Unified Manager가 스토리지 시스템 및 LDAP 서버와 같은 기타 원격 서버에 액세스할 수 있는 인증서를 표시합니다. 인증서는 CA(인증 기관)에서 발급하거나 자체 서명할 수 있습니다.
3. 인증서에 대한 자세한 내용을 보려면 해당 행을 선택하고 행 끝에 있는 줄임표를 선택한 다음 * 보기 * 또는 * 내보내기 * 를 클릭합니다.

## 인증서를 내보냅니다

## 인증서를 내보내 전체 세부 정보를 볼 수 있습니다.

시작하기 전에

내보낸 파일을 열려면 인증서 뷰어 응용 프로그램이 있어야 합니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 다음 탭 중 하나를 선택합니다.
   - * 관리 * — 웹 서비스 프록시를 호스팅하는 시스템의 인증서를 표시합니다. 관리 인증서는 CA(인증 기관)에서 자체 서명하거나 승인할 수 있습니다. Unified Manager에 안전하게 액세스할 수 있습니다.
   - * 신뢰 * — Unified Manager가 스토리지 시스템 및 LDAP 서버와 같은 기타 원격 서버에 액세스할 수 있는 인증서를 표시합니다. 인증서는 CA(인증 기관)에서 발급하거나 자체 서명할 수 있습니다.
3. 페이지에서 인증서를 선택한 다음 행 끝에 있는 줄임표를 클릭합니다.
4. 내보내기 * 를 클릭한 다음 인증서 파일을 저장합니다.
5. 인증서 뷰어 응용 프로그램에서 파일을 엽니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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