보안 인증서 관리

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/active-iq-unified-manager-918/config/task_view_https_security_certificate_ocf.html on November 13, 2026. Always check docs.netapp.com for the latest.

목차

보안 인증서 관리 . . . 1
- Active IQ Unified Manager에서 HTTPS 보안 인증서 보기 . . . 1
- Active IQ Unified Manager에서 HTTPS 인증서 서명 요청 다운로드 . . . 1
- Active IQ Unified Manager에 CA 서명 HTTPS 인증서를 설치합니다 . . . 1
  - 인증서 체인 예시 . . . 2
- Active IQ Unified Manager에서 외부 툴을 사용하여 생성된 HTTPS 인증서에 대해 알아보세요. . . . 2
  - EC 키 쌍을 사용하여 인증서를 로드하기 위한 형식 . . . 3
  - RSA 키 쌍을 사용하여 인증서를 로드하기 위한 형식 . . . 3
  - 외부에서 생성된 인증서를 업로드할 때의 검사 . . . 4
- 인증서 관리 페이지 설명 . . . 5
  - Active IQ Unified Manager의 HTTPS 인증서 페이지에 대해 알아보기 . . . 5
  - Active IQ Unified Manager에서 HTTPS 인증서 재생성 대화 상자 . . . 5

보안 인증서 관리

Active IQ Unified Manager에서 HTTPS 보안 인증서 보기

브라우저에서 가져온 인증서와 HTTPS 인증서 세부 정보를 비교하여 브라우저와 Unified Manager 간의 암호화된 연결이 가로채지지 않는지 확인할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

인증서를 보면 재생성된 인증서의 내용을 확인하거나 Unified Manager에 액세스할 수 있는 주체 대체 이름(SAN)을 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 일반 > *HTTPS 인증서*를 클릭합니다.

   HTTPS 인증서가 페이지 상단에 표시됩니다

HTTPS 인증서 페이지에 표시된 정보보다 보안 인증서에 대한 더 자세한 정보를 보려면 브라우저에서 연결 인증서를 확인할 수 있습니다.

Active IQ Unified Manager에서 HTTPS 인증서 서명 요청 다운로드

현재 HTTPS 보안 인증서에 대한 인증서 서명 요청을 다운로드하여 해당 파일을 인증 기관에 제공하여 서명받을 수 있습니다. CA에서 서명한 인증서는 중간자 공격을 방지하는 데 도움이 되며 자체 서명된 인증서보다 더 나은 보안 보호를 제공합니다.

시작하기 전에

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *HTTPS 인증서*를 클릭합니다.
2. *HTTPS 인증서 서명 요청 다운로드*를 클릭하세요.
3. `<hostname>.csr` 파일을 저장하십시오.

인증 기관에 파일을 제공하여 서명을 받은 다음, 서명된 인증서를 설치할 수 있습니다.

Active IQ Unified Manager에 CA 서명 HTTPS 인증서를 설치합니다

인증기관(CA)에서 서명 후 발급한 보안 인증서를 업로드하고 설치할 수 있습니다. 업로드 및 설치하려는 파일은 기존 자체 서명 인증서의 서명된 버전이어야 합니다. CA 서명 인증서는 중간자 공격을 방지하고 자체 서명 인증서보다 더 나은 보안을 제공합니다.

*무엇 .시작하기 전에

다음 작업을 완료해야 합니다:

- 인증서 서명 요청 파일을 다운로드하고 인증 기관에서 서명을 받았습니다
- 인증서 체인을 PEM 형식으로 저장했습니다
- Unified Manager 서버 인증서부터 루트 서명 인증서까지, 중간 인증서를 포함하여 인증서 체인에 있는 모든 인증서를 포함했습니다.

애플리케이션 관리자 역할이 있어야 합니다.

CSR이 생성된 인증서의 유효 기간이 397일을 초과하는 경우, CA는 인증서에 서명하고 반환하기 전에 유효 기간을 397일로 단축합니다.

단계

1. 왼쪽 탐색 창에서 일반 > *HTTPS 인증서*를 클릭합니다.
2. *HTTPS 인증서 설치*를 클릭하세요.
3. 표시되는 대화 상자에서 *파일 선택...*을 클릭하여 업로드할 파일을 찾으십시오.
4. 파일을 선택한 다음 *설치*를 클릭하여 파일을 설치하십시오.

   자세한 내용은 "외부 툴을 사용하여 생성된 HTTPS 인증서 설치"을 참조하십시오.

인증서 체인 예시

다음 예시는 인증서 체인 파일의 형태를 보여줍니다:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Active IQ Unified Manager에서 외부 툴을 사용하여 생성된 HTTPS 인증서에 대해 알아보세요.

OpenSSL, BoringSSL, LetsEncrypt 등과 같은 외부 툴을 사용하여 생성된 자체 서명 또는 CA 서명 인증서를 설치할 수 있습니다.

이 인증서는 외부에서 생성된 공개-개인 키 쌍이므로 인증서 체인과 함께 개인 키를 로드해야 합니다. 허용되는 키 쌍 알고리즘은 “RSA” 및 "`EC`"입니다. **HTTPS** 인증서 설치 옵션은 일반 섹션의 HTTPS 인증서 페이지에서 사용할 수 있습니다. 업로드하는 파일은 다음 입력 형식이어야 합니다.

1. Active IQ Unified Manager 호스트에 속하는 서버의 개인 키
2. 개인 키와 일치하는 서버 인증서
3. 위 인증서에 서명하는 데 사용되는 루트까지 역순으로 된 CA 인증서

EC 키 쌍을 사용하여 인증서를 로드하기 위한 형식

허용되는 곡선은 "`prime256v1`"과 "`secp384r1`"입니다. 외부에서 생성된 EC 쌍이 포함된 인증서 샘플:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

RSA 키 쌍을 사용하여 인증서를 로드하기 위한 형식

호스트 인증서에 속하는 RSA 키 쌍에 허용되는 키 크기는 2048, 3072 및 4096입니다. 외부에서 생성된 *RSA 키 쌍*이 있는 인증서:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

인증서가 업로드된 후 변경 사항을 적용하려면 Active IQ Unified Manager 인스턴스를 다시 시작해야 합니다.

외부에서 생성된 인증서를 업로드할 때의 검사

시스템은 외부 툴을 사용하여 생성된 인증서를 업로드하는 동안 검사를 수행합니다. 검사 중 하나라도 실패하면 인증서가 거부됩니다. 또한 제품 내의 CSR에서 생성된 인증서와 외부 툴을 사용하여 생성된 인증서에 대한 유효성 검사도 포함되어 있습니다.

- 입력된 개인 키는 입력된 호스트 인증서와 비교하여 유효성을 검사합니다.
- 호스트 인증서의 일반 이름(CN)은 호스트의 FQDN과 비교하여 검사됩니다.
- 호스트 인증서의 일반 이름(CN)은 비어 있거나 공백이어서는 안 되며, localhost로 설정되어서도 안 됩니다.
- 인증서의 유효 시작일은 미래일 수 없으며, 유효 만료일도 과거일 수 없습니다.
- 중간 CA 또는 CA가 존재하는 경우 인증서의 유효 시작일은 미래여서는 안 되며 유효 만료일은 과거여서는 안 됩니다.



입력에 포함된 개인 키는 암호화되어 있으면 안 됩니다. 암호화된 개인 키가 있는 경우 시스템에서 이를 거부합니다.

예시 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

예시 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

예제 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
```

```
-----END EC PRIVATE KEY-----
```

인증서 설치에 실패하면 기술 자료(KB) 문서를 참조하십시오: "ActiveIQ Unified Manager에서 외부에서 생성된 인증서를 설치하는 데 실패했습니다."

인증서 관리 페이지 설명

Active IQ Unified Manager의 HTTPS 인증서 페이지에 대해 알아보기

HTTPS 인증서 페이지에서는 현재 보안 인증서를 확인하고, 인증서 서명 요청을 다운로드하고, 새 자체 서명 HTTPS 인증서를 생성하거나, 새 HTTPS 인증서를 설치할 수 있습니다.

새로운 자체 서명 HTTPS 인증서를 생성하지 않은 경우 이 페이지에 표시되는 인증서는 설치 중에 생성된 인증서입니다.

명령 버튼

명령 버튼을 사용하면 다음과 같은 작업을 수행할 수 있습니다:

- **HTTPS** 인증서 서명 요청 다운로드

  현재 설치된 HTTPS 인증서에 대한 인증 요청을 다운로드합니다. 브라우저에서 <hostname>.csr 파일을 저장하라는 메시지가 표시되므로, 이 파일을 인증 기관에 제공하여 서명을 받을 수 있습니다.

- **HTTPS** 인증서 설치

  인증 기관에서 서명 후 발급한 보안 인증서를 업로드하고 설치할 수 있습니다. 새 인증서는 관리 서버를 재시작하면 적용됩니다.

- **HTTPS** 인증서 재생성

  이 기능을 사용하면 현재 보안 인증서를 대체하는 새 자체 서명 HTTPS 인증서를 생성할 수 있습니다. 새 인증서는 Unified Manager를 다시 시작한 후에 적용됩니다.

Active IQ Unified Manager에서 HTTPS 인증서 재생성 대화 상자

HTTPS 인증서 재생성 대화 상자를 사용하면 보안 정보를 사용자 지정한 다음 해당 정보를 사용하여 새 HTTPS 인증서를 생성할 수 있습니다.

현재 인증서 정보가 이 페이지에 표시됩니다.

"\`현재 인증서 속성을 사용하여 재생성\`" 및 "\`현재 인증서 속성 업데이트\`" 옵션을 사용하면 현재 정보로 인증서를 재생성하거나 새 정보로 인증서를 생성할 수 있습니다.

- 일반 이름

  필수 항목입니다. 보안을 설정하려는 정규화된 도메인 이름(FQDN)입니다.

  Unified Manager 고가용성 구성에서는 가상 IP 주소를 사용하십시오.

- 이메일

  선택 사항입니다. 소속 기관에 연락할 수 있는 이메일 주소이며, 일반적으로 인증서 관리자 또는 IT 부서의 이메일 주소입니다.

- 회사

  선택 사항입니다. 일반적으로 회사 법인명입니다.

- 부서

  선택 사항. 회사 내 부서명.

- 도시

  선택 사항. 회사 소재 도시.

- 상태

  (선택 사항) 회사 소재지(주 또는 도)를 약어 없이 기재해 주십시오.

- 국가

  선택 사항. 회사의 소재 국가입니다. 일반적으로 해당 국가의 두 글자 ISO 코드입니다.

- 다른 이름

  필수 항목입니다. 기존 localhost 또는 기타 네트워크 주소 외에 이 서버에 액세스하는 데 사용할 수 있는 추가적인 비기본 도메인 이름입니다. 각 대체 이름은 쉼표로 구분하십시오.

  인증서의 대체 이름 필드에서 로컬 식별 정보를 제거하려면 “Exclude local identifying information (e.g. localhost)” 확인란을 선택합니다. 이 확인란을 선택하면 필드에 입력한 내용만 대체 이름 필드에 사용됩니다. 비워 두면 결과 인증서에 대체 이름 필드가 전혀 포함되지 않습니다.

- 키 크기 **(**키 알고리즘**: RSA)**

  키 알고리즘은 RSA로 설정되어 있습니다. 키 크기는 2048, 3072 또는 4096비트 중에서 선택할 수 있습니다. 기본 키 크기는 2048비트로 설정되어 있습니다.

- 유효기간

  기본 유효 기간은 397일입니다. 이전 버전에서 업그레이드한 경우 이전 인증서의 유효 기간이 변경되지 않은 상태로 표시될 수 있습니다.

자세한 내용은 "HTTPS 인증서 생성"를 참조하십시오.

저작권 정보

Copyright © 2026 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.