Sicherheitszertifikate verwalten

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/de-de/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.

Inhalt

Sicherheitszertifikate verwalten . . . 1
- Das HTTPS-Sicherheitszertifikat in Active IQ Unified Manager anzeigen . . . 1
- Herunterladen einer HTTPS-Zertifikatsignierungsanforderung in Active IQ Unified Manager . . . 1
- Installation eines von einer Zertifizierungsstelle signierten HTTPS-Zertifikats in Active IQ Unified Manager . . . 2
  - Beispiel einer Zertifikatskette . . . 2
- Informationen zu HTTPS-Zertifikaten, die mit externen Tools in Active IQ Unified Manager Unified Manager generiert wurden . . . 3
  - Format zum Laden eines Zertifikats mit einem EC Schlüsselpaar . . . 3
  - Format zum Laden eines Zertifikats mit einem RSA-Schlüsselpaar . . . 4
  - Prüfungen beim Hochladen extern generierter Zertifikate . . . 4
- Seitenbeschreibungen für die Zertifikatsverwaltung . . . 5
  - Informationen zur HTTPS-Zertifikatsseite in Active IQ Unified Manager . . . 5
  - Dialogfeld „HTTPS-Zertifikat in Active IQ Unified Manager neu generieren“ . . . 6

Sicherheitszertifikate verwalten

Das HTTPS-Sicherheitszertifikat in Active IQ Unified Manager anzeigen

Sie können die Details des HTTPS-Zertifikats mit dem abgerufenen Zertifikat in Ihrem Browser vergleichen, um sicherzustellen, dass die verschlüsselte Verbindung Ihres Browsers zu Unified Manager nicht abgefangen wird.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Die Anzeige des Zertifikats ermöglicht die Überprüfung des Inhalts eines neu generierten Zertifikats oder die Anzeige von Subject Alt Names (SAN), über die auf Unified Manager zugegriffen werden kann.

Schritt

1. Im linken Navigationsbereich auf **General** > **HTTPS Certificate** klicken.

   Das HTTPS-Zertifikat wird oben auf der Seite angezeigt

Falls Sie detailliertere Informationen zum Sicherheitszertifikat benötigen, als auf der Seite HTTPS Certificate angezeigt werden, können Sie das Verbindungszertifikat in Ihrem Browser anzeigen.

Herunterladen einer HTTPS-Zertifikatsignierungsanforderung in Active IQ Unified Manager

Sie können eine Zertifikatssignierungsanforderung für das aktuelle HTTPS-Sicherheitszertifikat herunterladen, um die Datei einer Zertifizierungsstelle zur Signierung vorzulegen. Ein von einer Zertifizierungsstelle signiertes Zertifikat hilft, Man-in-the-Middle-Angriffe zu verhindern, und bietet besseren Schutz als ein selbstsigniertes Zertifikat.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich auf **General** > **HTTPS Certificate** klicken.
2. Sie können auf **Download HTTPS Certificate Signing Request** klicken.
3. Die `<hostname>.csr` Datei speichern.

Sie können die Datei einer Zertifizierungsstelle zum Signieren vorlegen und anschließend das signierte Zertifikat installieren.

Installation eines von einer Zertifizierungsstelle signierten HTTPS-Zertifikats in Active IQ Unified Manager

Sie können ein Sicherheitszertifikat hochladen und installieren, nachdem es von einer Certificate Authority signiert und zurückgegeben wurde. Die Datei, die Sie hochladen und installieren, muss eine signierte Version des vorhandenen selbstsignierten Zertifikats sein. Ein CA-signiertes Zertifikat hilft, Man-in-the-Middle-Angriffe zu verhindern, und bietet besseren Schutz als ein selbstsigniertes Zertifikat.

*Was Sie vor Beginn beachten sollten

Sie müssen die folgenden Aktionen abgeschlossen haben:

- Die Datei mit der Zertifikatsignierungsanforderung wurde heruntergeladen und durch eine Zertifizierungsstelle signiert.
- Zertifikatskette im PEM-Format gespeichert
- Die Kette umfasste alle Zertifikate, vom Unified Manager Serverzertifikat bis zum Stamm-Signaturzertifikat, einschließlich aller vorhandenen Zwischenzertifikate.

Sie benötigen die Rolle des Anwendungsadministrators.

Beträgt die Gültigkeitsdauer des Zertifikats, für das ein CSR erstellt wurde, mehr als 397 Tage, wird sie von der CA vor der Unterzeichnung und Rücksendung des Zertifikats auf 397 Tage verkürzt.

Schritte

1. Im linken Navigationsbereich auf **General** > **HTTPS Certificate** klicken.
2. Anschließend wählen Sie **HTTPS-Zertifikat installieren** aus.
3. In dem angezeigten Dialogfeld kann über **Datei auswählen…** die hochzuladende Datei gesucht werden.
4. Nach dem Auswählen der Datei installiert ein Klick auf **Install** die Datei.

   Informationen finden sich unter "Installation eines mit externen Tools generierten HTTPS-Zertifikats".

Beispiel einer Zertifikatskette

Das folgende Beispiel zeigt, wie die Zertifikatskettendatei aussehen könnte:

```
-----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-----
```

Informationen zu HTTPS-Zertifikaten, die mit externen Tools in Active IQ Unified Manager Unified Manager generiert wurden

Sie können selbstsignierte oder CA-signierte Zertifikate installieren, die mit einem externen Tool wie OpenSSL, BoringSSL oder LetsEncrypt generiert wurden.

Sie sollten den privaten Schlüssel zusammen mit der Zertifikatskette hochladen, da diese Zertifikate extern generierte Paare aus öffentlichem und privatem Schlüssel sind. Die zulässigen Schlüsselpaaralgorithmen sind „`RSA`“ und „`EC`“. Die Option „Install HTTPS Certificate“ ist auf der Seite „HTTPS Certificates“ im Abschnitt „General“ verfügbar. Die hochgeladene Datei sollte das folgende Eingabeformat aufweisen.

1. Privater Schlüssel des Servers, der zum Active IQ Unified Manager Host gehört
2. Zertifikat des Servers, das zum privaten Schlüssel passt
3. Zertifikate der Zertifizierungsstellen in umgekehrter Reihenfolge bis zur Root-CA, die zum Signieren des obigen Zertifikats verwendet werden

Format zum Laden eines Zertifikats mit einem EC Schlüsselpaar

Zulässige Kurven sind „`prime256v1`“ und „`secp384r1`“. Beispiel eines Zertifikats mit einem extern generierten EC-Paar:

```
 -----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-----
```

Format zum Laden eines Zertifikats mit einem RSA-Schlüsselpaar

Die zulässigen Schlüssellängen für das zum Host-Zertifikat gehörende RSA-Schlüsselpaar sind 2048, 3072 und 4096. Zertifikat mit einem extern generierten **RSA-Schlüsselpaar**:

```
-----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-----
```

Nach dem Hochladen des Zertifikats sollte die Active IQ Unified Manager Instanz neu gestartet werden, damit die Änderungen wirksam werden.

Prüfungen beim Hochladen extern generierter Zertifikate

Das System führt beim Hochladen eines mit externen Tools erstellten Zertifikats Prüfungen durch. Wenn eine dieser Prüfungen fehlschlägt, lehnt das System das Zertifikat ab. Die Validierung umfasst auch Zertifikate, die innerhalb des Produkts aus dem CSR generiert werden, sowie Zertifikate, die mit externen Tools erstellt werden.

- Der private Schlüssel in den Eingabedaten wird mit dem Host-Zertifikat in den Eingabedaten validiert.
- Der Common Name (CN) im Hostzertifikat wird mit dem FQDN des Hosts verglichen.
- Der Common Name (CN) des Hostzertifikats darf nicht leer sein oder nur Leerzeichen enthalten und darf nicht auf localhost gesetzt sein.
- Das Gültigkeitsbeginndatum sollte nicht in der Zukunft liegen, und das Gültigkeitsablaufdatum des Zertifikats sollte nicht in der Vergangenheit liegen.
- Falls Intermediate CA oder CA vorhanden ist, sollte das Gültigkeitsbeginn-Datum des Zertifikats nicht in der Zukunft liegen und das Gültigkeitsablaufdatum nicht in der Vergangenheit liegen.

Der private Schlüssel in den Eingabedaten darf nicht verschlüsselt sein. Falls private Schlüssel verschlüsselt sind, lehnt das System sie ab.

Beispiel 1

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

```
-----END ENCRYPTED PRIVATE KEY-----
```

Beispiel 2

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

Beispiel 3

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

Falls die Zertifikatsinstallation fehlschlägt, finden Sie weitere Informationen im Wissensdatenbank-Artikel (KB): "ActiveIQ Unified Manager kann ein extern generiertes Zertifikat nicht installieren"

Seitenbeschreibungen für die Zertifikatsverwaltung

Informationen zur HTTPS-Zertifikatsseite in Active IQ Unified Manager

Die Seite „HTTPS-Zertifikat“ ermöglicht das Anzeigen des aktuellen Sicherheitszertifikats, das Herunterladen einer Anforderung zur Zertifikatsignierung, das Generieren eines neuen selbstsignierten HTTPS-Zertifikats oder das Installieren eines neuen HTTPS-Zertifikats.

Wenn Sie kein neues selbstsigniertes HTTPS-Zertifikat erstellt haben, wird auf dieser Seite das Zertifikat angezeigt, das während der Installation generiert wurde.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie die folgenden Vorgänge durchführen:

- **HTTPS-Zertifikatsignierungsanforderung herunterladen**

  Lädt eine Zertifikatanforderung für das derzeit installierte HTTPS-Zertifikat herunter. Ihr Browser fordert Sie auf, die <hostname>.csr-Datei zu speichern, damit Sie die Datei einer Zertifizierungsstelle zum Signieren bereitstellen können.

- **Installation des HTTPS-Zertifikats**

  Ermöglicht das Hochladen und Installieren eines Sicherheitszertifikats, nachdem dieses von einer Zertifizierungsstelle signiert und zurückgesendet wurde. Das neue Zertifikat ist nach einem Neustart des Verwaltungsservers wirksam.

- **HTTPS-Zertifikat neu generieren**

  Ermöglicht die Generierung eines neuen selbstsignierten HTTPS-Zertifikats, das das aktuelle Sicherheitszertifikat ersetzt. Das neue Zertifikat ist nach einem Neustart des Unified Manager gültig.

Dialogfeld „HTTPS-Zertifikat in Active IQ Unified Manager neu generieren“

Im Dialogfeld „HTTPS-Zertifikat neu generieren“ können Sie die Sicherheitsinformationen anpassen und anschließend ein neues HTTPS-Zertifikat mit diesen Informationen generieren.

Auf dieser Seite erscheinen die aktuellen Zertifikatsinformationen.

Die Auswahlmöglichkeiten “Regenerate Using Current Certificate Attributes” und “Update the Current Certificate Attributes” ermöglichen es Ihnen, das Zertifikat mit den aktuellen Informationen neu zu generieren oder ein Zertifikat mit neuen Informationen zu erstellen.

- **Allgemeiner Name**

  Erforderlich. Der vollqualifizierte Domain-Name (FQDN), den Sie sichern möchten.

  In Hochverfügbarkeitskonfigurationen von Unified Manager kommt die virtuelle IP-Adresse zum Einsatz.

- **E-Mail**

  Optional. Eine E-Mail-Adresse zur Kontaktaufnahme mit Ihrem Unternehmen; in der Regel die E-Mail-Adresse des Zertifikatsadministrators oder der IT-Abteilung.

- **Unternehmen**

  Optional. In der Regel der eingetragene Name Ihres Unternehmens.

- **Abteilung**

  Optional. Der Name der Abteilung in Ihrem Unternehmen.

- **Stadt**

  Optional. Der Ort Ihres Unternehmens.

- **Zustand**

  Optional. Das Bundesland oder die Provinz Ihres Unternehmens, nicht abgekürzt.

- **Land**

  Optional. Der Länderstandort Ihres Unternehmens. Dies ist normalerweise ein zweistelliger ISO-Code des Landes.

- **Alternative Bezeichnungen**

  Erforderlich. Zusätzliche, nicht primäre Domänennamen, die zusätzlich zu localhost oder anderen Netzwerkadressen für den Zugriff auf diesen Server verwendet werden können. Als Trennzeichen zwischen den einzelnen alternativen Namen dienen Kommas.

Das Kontrollkästchen „`Lokale Identifikationsinformationen ausschließen (z. B. localhost)`“ wird ausgewählt, wenn die lokalen Identifikationsinformationen aus dem Feld „Alternative Namen“ im Zertifikat entfernt werden sollen. Wenn dieses Kontrollkästchen aktiviert ist, werden im Feld „Alternative Namen“ nur die Daten verwendet, die in das Feld eingegeben werden. Wenn das Feld leer bleibt, enthält das resultierende Zertifikat überhaupt kein Feld „Alternative Namen“.

- **SCHLÜSSELLÄNGE (SCHLÜSSELALGORITHMUS: RSA)**

  Der Schlüsselalgorithmus ist auf RSA eingestellt. Sie können zwischen den Schlüssellängen 2048, 3072 oder 4096 Bit wählen. Die Standardschlüssellänge beträgt 2048 Bit.

- **GÜLTIGKEITSDAUER**

  Die Standardgültigkeitsdauer beträgt 397 Tage. Wenn Sie ein Upgrade von einer früheren Version durchgeführt haben, bleibt die Gültigkeit des vorherigen Zertifikats möglicherweise unverändert.

Weitere Informationen sind unter "Generierung von HTTPS-Zertifikaten" verfügbar.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.