Gestisci i certificati di sicurezza

Active IQ Unified Manager

NetApp
November 13, 2026

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

Sommario

Gestisci i certificati di sicurezza . . . 1
- Visualizza il certificato di sicurezza HTTPS in Active IQ Unified Manager . . . 1
- Scarica una richiesta di firma del certificato HTTPS in Active IQ Unified Manager . . . 1
- Installa un certificato HTTPS firmato da una CA in Active IQ Unified Manager . . . 1
  - Esempio di catena di certificati . . . 2
- Scopri i certificati HTTPS generati utilizzando strumenti esterni in Active IQ Unified Manager Unified Manager . . . 3
  - Formato per il caricamento di un certificato con una coppia di chiavi EC . . . 3
  - Formato per caricare un certificato con una coppia di chiavi RSA . . . 3
  - Verifiche durante il caricamento di certificati generati esternamente . . . 4
- Descrizioni delle pagine per la gestione dei certificati . . . 5
  - Scopri la pagina relativa al certificato HTTPS in Active IQ Unified Manager . . . 5
  - Finestra di dialogo Rigenera certificato HTTPS in Active IQ Unified Manager . . . 5

Gestisci i certificati di sicurezza

Visualizza il certificato di sicurezza HTTPS in Active IQ Unified Manager

Puoi confrontare i dettagli del certificato HTTPS con il certificato recuperato nel browser per assicurarti che la connessione crittografata del browser a Unified Manager non venga intercettata.

Prima di iniziare

Devi disporre del ruolo di Operatore, Amministratore di applicazioni o Amministratore di archiviazione.

Visualizzando il certificato, puoi verificare il contenuto di un certificato rigenerato oppure visualizzare i nomi alternativi del soggetto (SAN) tramite i quali puoi accedere a Unified Manager.

Passaggio

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Certificato HTTPS**.

   Il certificato HTTPS viene visualizzato in alto nella pagina

Se hai bisogno di visualizzare informazioni più dettagliate sul certificato di sicurezza rispetto a quelle mostrate nella pagina HTTPS Certificate, puoi visualizzare il certificato di connessione nel tuo browser.

Scarica una richiesta di firma del certificato HTTPS in Active IQ Unified Manager

Puoi scaricare una richiesta di firma del certificato per il certificato di sicurezza HTTPS corrente, così da poter fornire il file a una Certificate Authority (CA) per la firma. Un certificato firmato da una CA contribuisce a prevenire gli attacchi man-in-the-middle e offre una protezione di sicurezza migliore rispetto a un certificato autofirmato.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Certificato HTTPS**.
2. Fai clic su **Scarica la richiesta di firma del certificato HTTPS**.
3. Salva il `<hostname>.csr` file.

Puoi fornire il file a un'autorità di certificazione per la firma e quindi installare il certificato firmato.

Installa un certificato HTTPS firmato da una CA in Active IQ Unified Manager

Puoi caricare e installare un certificato di sicurezza dopo che un'Autorità di certificazione lo ha firmato e restituito. Il file che carichi e installi deve essere una versione firmata del

certificato autofirmato esistente. Un certificato firmato da un'Autorità di certificazione contribuisce a prevenire gli attacchi man-in-the-middle e offre una protezione di sicurezza migliore rispetto a un certificato autofirmato.

*Cosa fare prima di iniziare

Devi aver completato le seguenti azioni:

- Hai scaricato il file di richiesta di firma del certificato e lo hai fatto firmare da un'autorità di certificazione
- Catena di certificati salvata in formato PEM
- Sono inclusi tutti i certificati nella catena, dal certificato del server Unified Manager al certificato di firma radice, compresi eventuali certificati intermedi presenti

Devi avere il ruolo di Amministratore dell'applicazione.

Se la validità del certificato per il quale è stato creato un CSR è superiore a 397 giorni, l'autorità di certificazione (CA) la ridurrà a 397 giorni prima di firmare e restituire il certificato

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Certificato HTTPS**.
2. Fai clic su **Installa certificato HTTPS**.
3. Nella finestra di dialogo visualizzata, fai clic su **Scegli file…** per individuare il file da caricare.
4. Seleziona il file, quindi fai clic su **Installa** per installarlo.

   Per informazioni, vedi "Installazione di un certificato HTTPS generato utilizzando strumenti esterni".

Esempio di catena di certificati

L'esempio seguente mostra come potrebbe apparire il file della catena di certificati:

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

Scopri i certificati HTTPS generati utilizzando strumenti esterni in Active IQ Unified Manager Unified Manager

Puoi installare certificati autofirmati o firmati da una CA e generati utilizzando uno strumento esterno come OpenSSL, BoringSSL, LetsEncrypt.

Devi caricare la chiave privata insieme alla catena di certificati, perché questi certificati sono coppie di chiavi pubblica-privata generate esternamente. Gli algoritmi consentiti per la coppia di chiavi sono “RSA” ed “EC”. L’opzione **Install HTTPS Certificate** è disponibile nella pagina HTTPS Certificates, nella sezione General. Il file che carichi deve essere nel seguente formato di input.

1. Chiave privata del server che appartiene all’host Active IQ Unified Manager
2. Certificato del server corrispondente alla chiave privata
3. Certificato delle CA in ordine inverso fino alla radice, utilizzate per firmare il certificato precedente

Formato per il caricamento di un certificato con una coppia di chiavi EC

Le curve consentite sono “prime256v1” e “secp384r1”. Esempio di certificato con una coppia EC generata esternamente:

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

Formato per caricare un certificato con una coppia di chiavi RSA

Le dimensioni consentite per la coppia di chiavi RSA appartenente al certificato host sono 2048, 3072 e 4096. certificato con una **coppia di chiavi RSA** generata esternamente:

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

Dopo aver caricato il certificato, dovresti riavviare l'istanza di Active IQ Unified Manager affinché le modifiche abbiano effetto.

Verifiche durante il caricamento di certificati generati esternamente

Il sistema esegue controlli durante il caricamento di un certificato generato utilizzando strumenti esterni. Se uno qualsiasi dei controlli fallisce, il certificato viene rifiutato. Sono inoltre incluse convalide per i certificati generati dal CSR (Certificate Signing Request) all'interno del prodotto e per i certificati generati utilizzando strumenti esterni.

- La chiave privata nell'input viene convalidata rispetto al certificato host nell'input.
- Il nome comune (CN) nel certificato dell'host viene confrontato con il FQDN dell'host.
- Il nome comune (CN) del certificato dell'host non deve essere vuoto o composto solo da spazi e non deve essere impostato su localhost.
- La data di inizio validità non deve essere futura e la data di scadenza della validità del certificato non deve essere passata.
- Se esiste un Intermediate CA o un CA, la data di inizio della validità del certificato non deve essere nel futuro e la data di scadenza della validità non deve essere nel passato.



La chiave privata inserita non deve essere crittografata. Se sono presenti chiavi private crittografate, il sistema le rifiuta.

Esempio 1

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

Esempio 2

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

```
-----END RSA PRIVATE KEY-----
```

Esempio 3

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

Se l'installazione del certificato non riesce, consulta l'articolo della knowledge base (KB): "ActiveIQ Unified Manager non riesce a installare un certificato generato esternamente"

Descrizioni delle pagine per la gestione dei certificati

Scopri la pagina relativa al certificato HTTPS in Active IQ Unified Manager

La pagina Certificato HTTPS consente di visualizzare il certificato di sicurezza corrente, scaricare una richiesta di firma del certificato, generare un nuovo certificato HTTPS autofirmato o installare un nuovo certificato HTTPS.

Se non hai generato un nuovo certificato HTTPS autofirmato, il certificato visualizzato in questa pagina è quello generato durante l'installazione.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Scarica la richiesta di firma del certificato HTTPS**

  Scarica una richiesta di certificazione per il certificato HTTPS attualmente installato. Il browser ti chiederà di salvare il file <hostname>.csr in modo da poterlo fornire a un'autorità di certificazione per la firma.

- **Installa il certificato HTTPS**

  Ti consente di caricare e installare un certificato di sicurezza dopo che un'Autorità di Certificazione lo ha firmato e restituito. Il nuovo certificato entra in vigore dopo che riavvii il server di gestione.

- **Rigenera il certificato HTTPS**

  Ti consente di generare un nuovo certificato HTTPS autofirmato che sostituisce il certificato di sicurezza corrente. Il nuovo certificato sarà attivo dopo aver riavviato Unified Manager.

Finestra di dialogo Rigenera certificato HTTPS in Active IQ Unified Manager

La finestra di dialogo Rigenera certificato HTTPS consente di personalizzare le informazioni di sicurezza e quindi di generare un nuovo certificato HTTPS con tali informazioni.

Le informazioni correnti sul certificato sono visualizzate in questa pagina.

Le opzioni “Regenerate Using Current Certificate Attributes” e “Update the Current Certificate Attributes” ti consentono di rigenerare il certificato con le informazioni correnti oppure di generarne uno con nuove informazioni.

- **Nome comune**

  Obbligatorio. Il fully qualified domain name (FQDN) che desideri proteggere.

  Nelle configurazioni ad alta disponibilità di Unified Manager, usa l’indirizzo IP virtuale.

- **E-mail**

  Facoltativo. Un indirizzo e-mail per contattare la tua organizzazione; in genere l’indirizzo e-mail dell’amministratore dei certificati o del reparto IT.

- **Azienda**

  Facoltativo. In genere corrisponde alla ragione sociale della tua azienda.

- **Dipartimento**

  Facoltativo. Il nome del reparto nella tua azienda.

- **Città**

  Facoltativo. La città in cui si trova la tua azienda.

- **Stato**

  Facoltativo. Lo stato o la provincia in cui si trova la tua azienda, senza abbreviazioni.

- **Paese**

  Facoltativo. Il paese in cui ha sede la tua azienda. In genere si tratta di un codice ISO di due lettere che identifica il paese.

- **Nomi alternativi**

  Obbligatorio. domain name aggiuntivi, non primari, che puoi usare per accedere a questo server oltre a localhost o ad altri indirizzi di rete esistenti. Separa ciascun nome alternativo con una virgola.

  Seleziona la casella di controllo “Escludi informazioni di identificazione locali (ad es. localhost)” se vuoi rimuovere le informazioni di identificazione locali dal campo Nomi alternativi del certificato. Quando selezioni questa casella di controllo, nel campo Nomi alternativi viene usato solo quello che inserisci nel campo. Se lo lasci vuoto, il certificato risultante non avrà alcun campo Nomi alternativi.

- **DIMENSIONE DELLA CHIAVE (ALGORITMO DELLA CHIAVE: RSA)**

  L’algoritmo della chiave è impostato su RSA. Puoi selezionare una delle seguenti dimensioni della chiave: 2048, 3072 o 4096 bit. La dimensione predefinita della chiave è impostata su 2048 bit.

- **PERIODO DI VALIDITÀ**

  Il periodo di validità predefinito è di 397 giorni. Se hai eseguito l’aggiornamento da una versione precedente, la validità del certificato precedente potrebbe non essere cambiata.

Per ulteriori informazioni, consulta "Generazione di certificati HTTPS".

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.