



Gestire i certificati di sicurezza

Active IQ Unified Manager

NetApp

October 15, 2025

This PDF was generated from https://docs.netapp.com/it-it/active-iq-unified-manager-916/config/task_view_https_security_certificate_ocf.html on October 15, 2025. Always check docs.netapp.com for the latest.

Sommario

- Gestire i certificati di sicurezza 1
 - Visualizza il certificato di sicurezza HTTPS 1
 - Scarica una richiesta di firma del certificato HTTPS 1
 - Installa un certificato HTTPS firmato e restituito da una CA 1
 - Esempio di catena di certificati 2
 - Installa un certificato HTTPS generato utilizzando strumenti esterni 3
 - Formato per il caricamento di un certificato con una coppia di chiavi EC 3
 - Formato per il caricamento di un certificato con una coppia di chiavi RSA 3
 - Controlli durante il caricamento di certificati generati esternamente 4
- Descrizioni delle pagine per la gestione dei certificati 5
 - Pagina del certificato HTTPS 5
 - Finestra di dialogo Rigenera certificato HTTPS 6

Gestire i certificati di sicurezza

È possibile configurare HTTPS nel server Unified Manager per monitorare e gestire i cluster tramite una connessione sicura.

Visualizza il certificato di sicurezza HTTPS

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

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

La visualizzazione del certificato consente di verificare il contenuto di un certificato rigenerato o di visualizzare i nomi alternativi del soggetto (SAN) da cui è possibile accedere a Unified Manager.

Fare un passo

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

Il certificato HTTPS viene visualizzato nella parte superiore della pagina

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

Scarica una richiesta di firma del certificato HTTPS

È possibile scaricare una richiesta di firma della certificazione per l'attuale certificato di sicurezza HTTPS, in modo da poter fornire il file a un'autorità di certificazione per la firma. Un certificato firmato da una CA aiuta a prevenire gli attacchi man-in-the-middle e offre una migliore protezione di sicurezza rispetto a un certificato autofirmato.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Passi

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

È possibile fornire il file a un'autorità di certificazione affinché lo firmi e quindi installare il certificato firmato.

Installa un certificato HTTPS firmato e restituito da una CA

È possibile 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 una CA aiuta a prevenire gli attacchi man-in-the-middle e fornisce una migliore protezione di sicurezza rispetto a un certificato autofirmato.

*Cosa. Prima di iniziare

Devi aver completato le seguenti azioni:

- Ho scaricato il file di richiesta di firma del certificato e l'ho fatto firmare da un'autorità di certificazione
- Salvata la catena di certificati in formato PEM
- Inclusi tutti i certificati nella catena, dal certificato del server Unified Manager al certificato di firma radice, inclusi tutti i certificati intermedi presenti

È necessario disporre del ruolo di amministratore dell'applicazione.



Se la validità del certificato per il quale è stato creato un CSR è superiore a 397 giorni, la validità verrà ridotta a 397 giorni dalla CA prima di firmare e restituire il certificato

Passi

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

Per informazioni, vedere ["Installazione di un certificato HTTPS generato tramite 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-----
```

Installa un certificato HTTPS generato utilizzando strumenti esterni

È possibile installare certificati autofirmati o firmati da una CA e generati tramite uno strumento esterno come OpenSSL, BoringSSL, LetsEncrypt.

È necessario caricare la chiave privata insieme alla catena di certificati, poiché questi certificati sono coppie di chiavi pubblica-privata generate esternamente. Gli algoritmi di coppia di chiavi consentiti sono “RSA” e “EC”. L'opzione **Installa certificato HTTPS** è disponibile nella pagina Certificati HTTPS nella sezione Generale. Il file caricato deve essere nel seguente formato di input.

1. Chiave privata del server che appartiene all'host Active IQ Unified Manager
2. Certificato del server che corrisponde alla chiave privata
3. Certificato delle CA inverso fino alla radice, che vengono utilizzati per firmare il certificato di cui sopra

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 il caricamento di un certificato con una coppia di chiavi RSA

Le dimensioni delle chiavi 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, è necessario riavviare l'istanza di Active IQ Unified Manager affinché le modifiche abbiano effetto.

Controlli durante il caricamento di certificati generati esternamente

Il sistema esegue controlli durante il caricamento di un certificato generato tramite strumenti esterni. Se uno qualsiasi dei controlli fallisce, il certificato viene rifiutato. Sono incluse anche le convalide per i certificati generati dal CSR all'interno del prodotto e per i certificati generati tramite strumenti esterni.

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



La chiave privata nell'input non deve essere crittografata. Se sono presenti chiavi private crittografate, queste vengono rifiutate dal sistema.

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, consultare l'articolo della Knowledge Base (KB):https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager non riesce a installare un certificato generato esternamente"]

Descrizioni delle pagine per la gestione dei certificati

È possibile utilizzare la pagina Certificato HTTPS per visualizzare i certificati di sicurezza correnti e per generare nuovi certificati HTTPS.

Pagina del certificato HTTPS

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 chiede di salvare il file <hostname>.csr in modo da poterlo fornire a un'autorità di certificazione per la firma.

- **Installa il certificato HTTPS**

Consente di caricare e installare un certificato di sicurezza dopo che un'autorità di certificazione lo ha firmato e restituito. Il nuovo certificato sarà effettivo dopo il riavvio del server di gestione.

- **Rigenera il certificato HTTPS**

Consente di generare un nuovo certificato HTTPS autofirmato, che sostituisce l'attuale certificato di sicurezza. Il nuovo certificato sarà effettivo dopo il riavvio di Unified Manager.

Finestra di dialogo Rigenera certificato HTTPS

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 attuali sul certificato vengono visualizzate in questa pagina.

Le selezioni "Rigenera utilizzando gli attributi del certificato corrente" e "Aggiorna gli attributi del certificato corrente" consentono di rigenerare il certificato con le informazioni correnti o di generare un certificato con nuove informazioni.

- **Nome comune**

Necessario. Il nome di dominio completamente qualificato (FQDN) che desideri proteggere.

Nelle configurazioni ad alta disponibilità di Unified Manager, utilizzare l'indirizzo IP virtuale.

- **E-mail**

Opzionale. Un indirizzo email per contattare la tua organizzazione; in genere l'indirizzo email dell'amministratore del certificato o del reparto IT.

- **Azienda**

Opzionale. Solitamente è il nome della società.

- **Dipartimento**

Opzionale. Il nome del reparto della tua azienda.

- **Città**

Opzionale. La sede della tua azienda in città.

- **Stato**

Opzionale. La sede della tua azienda, non in forma abbreviata, nello stato o nella provincia.

- **Paese**

Opzionale. Il paese in cui ha sede la tua azienda. In genere si tratta di un codice ISO di due lettere del Paese.

- **Nomi alternativi**

Necessario. Nomi di dominio aggiuntivi, non primari, che possono essere utilizzati per accedere a questo server oltre all'indirizzo localhost o ad altri indirizzi di rete esistenti. Separare ogni nome alternativo con una virgola.

Selezionare la casella di controllo "Escludi informazioni di identificazione locali (ad esempio localhost)" se si desidera rimuovere le informazioni di identificazione locali dal campo Nomi alternativi nel certificato. Quando questa casella di controllo è selezionata, nel campo Nomi alternativi verrà utilizzato solo ciò che inserisci nel campo. Se lasciato vuoto, il certificato risultante non avrà alcun campo Nomi alternativi.

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

L'algoritmo chiave è impostato su RSA. È possibile 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 397 giorni. Se hai effettuato l'aggiornamento da una versione precedente, potresti notare che la validità del certificato precedente è rimasta invariata.

Per maggiori informazioni, vedere ["Generazione di certificati HTTPS"](#).

Informazioni sul copyright

Copyright © 2025 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.