Gestisci le impostazioni di autenticazione SAML

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/concept_manage_saml_authentication_settings_um.html on November 13, 2026. Always check docs.netapp.com for the latest.

Sommario

Gestisci le impostazioni di autenticazione SAML . . . 1
- Abilita l'autenticazione SAML in Active IQ Unified Manager . . . 1
- Usa un provider di identità in Active IQ Unified Manager . . . 1
  - Standard di crittografia supportati . . . 1
  - Fornitori di identità validati . . . 1
  - Requisiti di configurazione di ADFS . . . 1
  - Altri requisiti di configurazione . . . 2
- Abilita l'autenticazione SAML in Active IQ Unified Manager . . . 2
- Cambia il provider di identità per l'autenticazione SAML in Active IQ Unified Manager . . . 3
- Aggiorna le impostazioni di autenticazione SAML dopo una modifica del certificato di sicurezza di Active IQ Unified Manager . . . 4
- Disabilita l'autenticazione SAML in Active IQ Unified Manager . . . 5
- Disabilita l'autenticazione SAML dalla console di manutenzione di Active IQ Unified Manager . . . 6
- Usa la pagina di autenticazione SAML in Active IQ Unified Manager . . . 6

Gestisci le impostazioni di autenticazione SAML

Abilita l'autenticazione SAML in Active IQ Unified Manager

Dopo aver configurato le impostazioni di autenticazione remota, puoi abilitare l'autenticazione SAML (Security Assertion Markup Language) in modo che gli utenti remoti siano autenticati da un provider di identità (IdP) sicuro prima di poter accedere all'interfaccia utente web di Unified Manager.

Tieni presente che, dopo aver abilitato l'autenticazione SAML, solo gli utenti remoti avranno accesso all'interfaccia utente grafica di Unified Manager. Gli utenti locali e gli utenti Maintenance non potranno accedere alla UI. Questa configurazione non ha alcun impatto sugli utenti che accedono alla console di manutenzione.

Usa un provider di identità in Active IQ Unified Manager

Quando configuri Unified Manager per utilizzare un provider di identità (IdP) per eseguire l'autenticazione SAML per tutti gli utenti remoti, devi tenere presenti alcune impostazioni di configurazione obbligatorie affinché la connessione a Unified Manager abbia esito positivo.

Devi inserire l'URI e i metadati di Unified Manager nel server IdP. Puoi copiare queste informazioni dalla pagina di autenticazione SAML di Unified Manager. Unified Manager è considerato il service provider (SP) nello standard Security Assertion Markup Language (SAML).

Standard di crittografia supportati

- Advanced Encryption Standard (AES): AES-128 e AES-256
- Algoritmo di hash sicuro (SHA): SHA-1 e SHA-256

Fornitori di identità validati

- Shibboleth
- Active Directory Federation Services (ADFS)

Requisiti di configurazione di ADFS

- Devi definire tre regole di attestazione nel seguente ordine, necessarie affinché Unified Manager possa analizzare le risposte SAML di ADFS per questa voce di trust della relying party.

Regola attestazioni	Valore
SAM-account-name	ID nome
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Gruppi di token — Nome non qualificato	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Devi impostare il metodo di autenticazione su "Forms Authentication", altrimenti gli utenti potrebbero ricevere un errore quando escono da Unified Manager. Segui questi passaggi:

a. Apri la console di gestione ADFS.

b. Fai clic sulla cartella Criteri di autenticazione nella visualizzazione ad albero a sinistra.

c. In Azioni sulla destra, fai clic su Modifica criterio di autenticazione primaria globale.

d. Imposta il metodo di autenticazione Intranet su “Forms Authentication” invece dell’impostazione predefinita “Windows Authentication”.

- In alcuni casi l’accesso tramite l’IdP viene rifiutato quando il certificato di sicurezza di Unified Manager è firmato da una CA. Esistono due soluzioni alternative per risolvere questo problema:
  - Segui le istruzioni indicate nel link per disabilitare il controllo di revoca sul server ADFS per la relying party associata al certificato CA nella catena:

    "Disabilita il controllo della revoca per Relying Party Trust"

  - Assicurati che il server CA risieda all’interno del server ADFS per firmare la richiesta di certificato del server Unified Manager.

Altri requisiti di configurazione

- Lo scostamento dell’orologio di Unified Manager è impostato su 5 minuti, quindi la differenza di orario tra il server IdP e il server Unified Manager non può essere superiore a 5 minuti, altrimenti l’autenticazione non riuscirà.

Abilita l’autenticazione SAML in Active IQ Unified Manager

Puoi abilitare l’autenticazione SAML (Security Assertion Markup Language) in modo che gli utenti remoti vengano autenticati da un provider di identità (IdP) sicuro prima di poter accedere all’interfaccia utente web di Unified Manager.

Prima di iniziare

- Devi aver configurato l’autenticazione remota e aver verificato che sia andata a buon fine.
- Devi aver creato almeno un Remote User o un Remote Group con il ruolo di Application Administrator.
- Il provider di identità (IdP) deve essere supportato da Unified Manager e deve essere configurato.
- Devi disporre dell’URL dell’IdP e dei metadati.
- Devi avere accesso al server IdP.

Dopo aver abilitato l’autenticazione SAML da Unified Manager, gli utenti non possono accedere all’interfaccia utente grafica finché l’IdP non è stato configurato con le informazioni host del server Unified Manager. Quindi devi essere pronto a completare entrambe le parti della connessione prima di avviare il processo di configurazione. L’IdP può essere configurato prima o dopo aver configurato Unified Manager.

Solo gli utenti remoti avranno accesso all’interfaccia utente grafica di Unified Manager dopo che avrai abilitato l’autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all’interfaccia utente. Questa configurazione non influisce sugli utenti che accedono alla console di manutenzione, ai comandi di Unified Manager o alle ZAPI.

Unified Manager si riavvia automaticamente al termine della configurazione SAML su questa pagina.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione SAML**.
2. Seleziona la casella di controllo **Abilita autenticazione SAML**.

   Vedi i campi necessari per configurare la connessione IdP.

3. Inserisci l'URI dell'IdP e i metadati dell'IdP necessari per connettere il server Unified Manager al server IdP.

   Se il server IdP è accessibile direttamente dal server Unified Manager, dopo aver inserito l'URI dell'IdP, puoi fare clic sul pulsante **Recupera metadati IdP** per compilare automaticamente il campo Metadati IdP.

4. Copia l'URI dei metadati dell'host di Unified Manager oppure salva i metadati dell'host in un file di testo XML.

   Puoi configurare il server IdP con queste informazioni in questo momento.

5. Fare clic su **Save**.

   Viene visualizzata una finestra di messaggio per confermare che vuoi completare la configurazione e riavviare Unified Manager.

6. Fai clic su **Confirm and Logout** e Unified Manager si riavvia.

La prossima volta che gli utenti remoti autorizzati tenteranno di accedere all'interfaccia grafica di Unified Manager, dovranno inserire le proprie credenziali nella pagina di accesso dell'IdP anziché nella pagina di accesso di Unified Manager.

Se non l'hai già fatto, accedi al tuo IdP e inserisci l'URI del server Unified Manager e i metadati per completare la configurazione.

> Quando usi ADFS come provider di identità, la GUI di Unified Manager non rispetta il timeout di ADFS e continua a funzionare finché non viene raggiunto il timeout della sessione di Unified Manager. Puoi modificare il timeout della sessione della GUI facendo clic su **Generale** > **Impostazioni funzionalità** > **Timeout di inattività**.

Cambia il provider di identità per l'autenticazione SAML in Active IQ Unified Manager

Puoi modificare il provider di identità (IdP) che Unified Manager utilizza per autenticare gli utenti remoti.

Prima di iniziare

- Devi disporre dell'URL dell'IdP e dei metadati.
- Devi avere accesso all'IdP.

Il nuovo IdP può essere configurato prima o dopo la configurazione di Unified Manager.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione SAML**.
2. Inserisci il nuovo URI dell'IdP e i metadati dell'IdP necessari per connettere il server Unified Manager all'IdP.

Se l'IdP è accessibile direttamente dal server Unified Manager, dopo aver inserito l'URL dell'IdP, puoi fare clic sul pulsante **Recupera metadati IdP** per compilare automaticamente il campo Metadati IdP.

3. Copia l'URI dei metadati di Unified Manager oppure salva i metadati in un file di testo XML.
4. Fai clic su **Salva configurazione**.

   Viene visualizzata una finestra di messaggio per confermare che vuoi modificare la configurazione.

5. Fare clic su **OK**.

Accedi al nuovo IdP e inserisci l'URI del server Unified Manager e i metadati per completare la configurazione.

La prossima volta che gli utenti remoti autorizzati tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella nuova pagina di accesso di IdP anziché nella vecchia pagina di accesso di IdP.

Aggiorna le impostazioni di autenticazione SAML dopo una modifica del certificato di sicurezza di Active IQ Unified Manager

Qualsiasi modifica al certificato di sicurezza HTTPS installato sul server Unified Manager richiede che tu aggiorni le impostazioni di configurazione dell'autenticazione SAML. Il certificato viene aggiornato se rinomini il sistema host, assegni un nuovo indirizzo IP al sistema host o modifichi manualmente il certificato di sicurezza del sistema.

Dopo la modifica del certificato di sicurezza e il riavvio del server Unified Manager, l'autenticazione SAML non funzionerà e gli utenti non potranno accedere all'interfaccia grafica di Unified Manager. Devi aggiornare le impostazioni di autenticazione SAML sia sul server IdP sia sul server Unified Manager per riattivare l'accesso all'interfaccia utente.

Passaggi

1. Accedi alla console di manutenzione.
2. Nel **Menu principale**, inserisci il numero corrispondente all'opzione **Disabilita autenticazione SAML**.

   Viene visualizzato un messaggio per confermare che vuoi disabilitare l'autenticazione SAML e riavviare Unified Manager.

3. Avvia l'interfaccia utente di Unified Manager utilizzando il FQDN o l'indirizzo IP aggiornato, accetta il certificato del server aggiornato nel browser ed effettua l'accesso utilizzando le credenziali dell'utente di manutenzione.
4. Nella pagina **Configurazione/Autenticazione**, seleziona la scheda **Autenticazione SAML** e configura la connessione IdP.
5. Copia l'URI dei metadati dell'host di Unified Manager oppure salva i metadati dell'host in un file di testo XML.
6. Fare clic su **Save**.

   Viene visualizzata una finestra di messaggio per confermare che vuoi completare la configurazione e riavviare Unified Manager.

7. Fai clic su **Confirm and Logout** e Unified Manager si riavvia.

8. Accedi al tuo server IdP e inserisci l'URI del server Unified Manager e i metadati per completare la configurazione.

Fornitore di identità	Passaggi di configurazione
ADFS	a. Elimina la voce esistente di relying party trust nella GUI di gestione di ADFS. b. Aggiungi una nuova voce di attendibilità della relying party utilizzando il `saml_sp_metadata.xml` dal server Unified Manager aggiornato. c. Definisci le tre regole di attestazione necessarie affinché Unified Manager possa analizzare le risposte SAML di ADFS per questa voce di trust della relying party. d. Riavvia il servizio Windows ADFS.
Shibboleth	a. Aggiorna il nuovo FQDN del server Unified Manager nei file `attribute-filter.xml` e `relying-party.xml`. b. Riavvia il server web Apache Tomcat e attendi che la porta 8005 torni online.

9. Accedi a Unified Manager e verifica che l'autenticazione SAML funzioni correttamente tramite il tuo IdP.

Disabilita l'autenticazione SAML in Active IQ Unified Manager

Puoi disabilitare l'autenticazione SAML quando vuoi interrompere l'autenticazione degli utenti remoti tramite un provider di identità sicuro (IdP) prima che possano accedere all'interfaccia utente web di Unified Manager. Quando l'autenticazione SAML è disabilitata, i provider di servizi directory configurati, come Active Directory o LDAP, eseguono l'autenticazione di accesso.

Dopo aver disabilitato l'autenticazione SAML, oltre agli utenti remoti configurati, anche gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia utente grafica.

Puoi anche disabilitare l'autenticazione SAML usando la console di manutenzione di Unified Manager se non hai accesso all'interfaccia utente grafica.

Unified Manager si riavvia automaticamente dopo la disattivazione dell'autenticazione SAML.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione SAML**.
2. Deseleziona la casella di controllo **Abilita l'autenticazione SAML**.
3. Fare clic su **Save**.

   Viene visualizzata una finestra di messaggio per confermare che vuoi completare la configurazione e riavviare Unified Manager.

4. Fai clic su **Confirm and Logout** e Unified Manager si riavvia.

La prossima volta che gli utenti remoti tenteranno di accedere all'interfaccia grafica di Unified Manager, dovranno inserire le proprie credenziali nella pagina di accesso di Unified Manager anziché nella pagina di accesso dell'IdP.

Accedi al tuo IdP ed elimina l'URI del server Unified Manager e i metadati.

Disabilita l'autenticazione SAML dalla console di manutenzione di Active IQ Unified Manager

Potresti dover disabilitare l'autenticazione SAML dalla console di manutenzione quando non hai accesso alla GUI di Unified Manager. Ciò potrebbe verificarsi in caso di configurazione errata o se l'IdP non è accessibile.

Prima di iniziare

Devi avere accesso alla console di manutenzione come utente di manutenzione.

Quando l'autenticazione SAML è disabilitata, i provider di servizi di directory configurati, come Active Directory o LDAP, eseguono l'autenticazione di accesso. Oltre agli utenti remoti configurati, anche gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia utente grafica.

Puoi anche disabilitare l'autenticazione SAML dalla pagina Setup/Authentication nella UI.

Unified Manager si riavvia automaticamente dopo la disattivazione dell'autenticazione SAML.

Passaggi

1. Accedi alla console di manutenzione.
2. Nel **Menu principale**, inserisci il numero corrispondente all'opzione **Disabilita autenticazione SAML**.

   Viene visualizzato un messaggio per confermare che vuoi disabilitare l'autenticazione SAML e riavviare Unified Manager.

3. Digita **y**, quindi premi Invio e Unified Manager si riavvia.

La prossima volta che gli utenti remoti tenteranno di accedere all'interfaccia grafica di Unified Manager, dovranno inserire le proprie credenziali nella pagina di accesso di Unified Manager anziché nella pagina di accesso dell'IdP.

Se necessario, accedi al tuo IdP ed elimina l'URL del server Unified Manager e i metadati.

Usa la pagina di autenticazione SAML in Active IQ Unified Manager

Puoi usare la pagina Autenticazione SAML per configurare Unified Manager in modo che autentichi gli utenti remoti tramite SAML attraverso un provider di identità (IdP) sicuro prima che possano accedere all'interfaccia utente web di Unified Manager.

- Per creare o modificare la configurazione SAML, devi disporre del ruolo Application Administrator.

- Devi aver configurato l'autenticazione remota.
- Devi aver configurato almeno un utente remoto o un gruppo remoto.

Dopo aver configurato l'autenticazione remota e gli utenti remoti, puoi selezionare la casella di controllo Abilita autenticazione SAML per abilitare l'autenticazione tramite un provider di identità sicuro.

- **URI IdP**

  L'URI per accedere all'IdP dal server Unified Manager. Di seguito sono elencati alcuni esempi di URI.

  Esempio di URI ADFS:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Esempio di URI Shibboleth:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Metadati dell'IdP**

  I metadati IdP in formato XML.

  Se l'URL dell'IdP è accessibile dal server Unified Manager, puoi fare clic sul pulsante **Recupera metadati IdP** per compilare questo campo.

- **Sistema host (FQDN)**

  Il FQDN del sistema host Unified Manager come definito durante l'installazione. Puoi modificare questo valore se necessario.

- **URI dell'host**

  L'URI per accedere al sistema host di Unified Manager dall'IdP.

- **Metadati dell'host**

  I metadati del sistema host in formato XML.

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.