Gestisci l'accesso degli utenti

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

Sommario

Gestisci l’accesso degli utenti . . . 1
- Aggiungi utenti . . . 1
  - Aggiungi utenti in Active IQ Unified Manager . . . 1
  - Crea un utente database in Active IQ Unified Manager . . . 1
- Modifica le impostazioni utente in Active IQ Unified Manager . . . 2
- Visualizza gli utenti in Active IQ Unified Manager . . . 2
- Elimina utenti o gruppi in Active IQ Unified Manager . . . 3
- Scopri il controllo degli accessi in base al ruolo in Active IQ Unified Manager . . . 3
- Scopri le tipologie di utente in Active IQ Unified Manager . . . 3
- Scopri i ruoli utente in Active IQ Unified Manager . . . 4
- Scopri i ruoli e le funzionalità degli utenti in Active IQ Unified Manager . . . 5

Gestisci l’accesso degli utenti

Aggiungi utenti

Aggiungi utenti in Active IQ Unified Manager

Puoi aggiungere utenti locali o utenti del database utilizzando la pagina Utenti. Puoi anche aggiungere utenti remoti o gruppi che appartengono a un server di autenticazione. Puoi assegnare ruoli a questi utenti e, in base ai privilegi dei ruoli, gli utenti possono gestire gli oggetti di storage e i dati con Unified Manager oppure visualizzare i dati in un database.

Prima di iniziare

- Devi avere il ruolo di Amministratore dell’applicazione.
- Per aggiungere un utente o un gruppo remoto, devi aver abilitato l’autenticazione remota e configurato il server di autenticazione.
- Se intendi configurare l’autenticazione SAML in modo che un provider di identità (IdP) autentichi gli utenti che accedono all’interfaccia grafica, assicurati che questi utenti siano definiti come utenti “remote”.

  L’accesso all’interfaccia utente non è consentito agli utenti di tipo “local” o “maintenance” quando l’autenticazione SAML è abilitata.

Se aggiungi un gruppo da Windows Active Directory, tutti i membri diretti e i sottogruppi nidificati possono autenticarsi a Unified Manager, a meno che i sottogruppi nidificati non siano disabilitati. Se aggiungi un gruppo da OpenLDAP o da altri servizi di autenticazione, solo i membri diretti di quel gruppo possono autenticarsi a Unified Manager.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Utenti**.
2. Nella pagina Utenti, fai clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi utente, seleziona il tipo di utente che desideri aggiungere e inserisci le informazioni richieste.

   Quando inserisci le informazioni utente richieste, devi specificare un indirizzo email univoco per quell’utente. Devi evitare di specificare indirizzi email condivisi da più utenti.

4. Fai clic su **Add**.

Crea un utente database in Active IQ Unified Manager

Per supportare una connessione tra Workflow Automation e Unified Manager, o per accedere alle viste del database, devi prima creare un utente del database con il ruolo Integration Schema o Report Schema nell’interfaccia web di Unified Manager.

Prima di iniziare

Devi avere il ruolo di Amministratore dell’applicazione.

Gli utenti del database consentono l’integrazione con Workflow Automation e l’accesso alle viste del database

specifiche per i report. Gli utenti del database non hanno accesso all'interfaccia utente web di Unified Manager né alla console di manutenzione e non possono eseguire chiamate API.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Utenti**.
2. Nella pagina Utenti, fai clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi utente, seleziona **Utente database** nell'elenco a discesa **Tipo**.
4. Inserisci un nome e una password per l'utente del database.
5. Nel menu a discesa **Ruolo**, seleziona il ruolo appropriato.

Se sei…	Scegli questo ruolo
Collegamento di Unified Manager con Workflow Automation	Schema di integrazione
Accesso ai report e ad altre viste del database	Schema di report

6. Fai clic su **Add**.

Modifica le impostazioni utente in Active IQ Unified Manager

Puoi modificare le impostazioni utente, come l'indirizzo e-mail e il ruolo, specificate per ciascun utente. Ad esempio, potresti voler modificare il ruolo di un utente che è un operatore dello storage e assegnargli i privilegi di amministratore dello storage.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Quando modifichi il ruolo assegnato a un utente, le modifiche vengono applicate quando si verifica una delle seguenti azioni:

- Esci e accedi nuovamente a Unified Manager.
- Hai raggiunto il timeout della sessione di 24 ore.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Utenti**.
2. Nella pagina Utenti, seleziona l'utente per il quale vuoi modificare le impostazioni e fai clic su **Modifica**.
3. Nella finestra di dialogo Modifica utente, modifica le impostazioni appropriate specificate per l'utente.
4. Fare clic su **Save**.

Visualizza gli utenti in Active IQ Unified Manager

Puoi usare la pagina Utenti per visualizzare l'elenco degli utenti che gestiscono oggetti di storage e dati usando Unified Manager. Puoi visualizzare i dettagli degli utenti, come il nome utente, il tipo di utente, l'indirizzo e-mail e il ruolo assegnato agli utenti.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Passaggio

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

Elimina utenti o gruppi in Active IQ Unified Manager

Puoi eliminare uno o più utenti dal database del server di gestione per impedire a utenti specifici di accedere a Unified Manager. Puoi anche eliminare i gruppi in modo che tutti gli utenti del gruppo non possano più accedere al server di gestione.

Prima di iniziare

- Quando elimini i gruppi remoti, devi aver riassegnato gli eventi assegnati agli utenti di tali gruppi.

  Se elimini utenti locali o utenti remoti, gli eventi assegnati a questi utenti vengono automaticamente disassegnati.

- Devi avere il ruolo di Amministratore dell'applicazione.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Utenti**.
2. Nella pagina Utenti, seleziona gli utenti o i gruppi che desideri eliminare, quindi fai clic su **Elimina**.
3. Fai clic su **Sì** per confermare l'eliminazione.

Scopri il controllo degli accessi in base al ruolo in Active IQ Unified Manager

RBAC (in base al ruolo, role-based access control) offre la possibilità di controllare chi ha accesso a varie funzionalità e risorse nel server Active IQ Unified Manager. RBAC permette agli amministratori di gestire gruppi di utenti definendo i ruoli. Se hai bisogno di limitare l'accesso a specifiche funzionalità per determinati amministratori, devi creare account amministratore per loro. Se vuoi limitare le informazioni che gli amministratori possono visualizzare e le operazioni che possono eseguire, devi applicare ruoli agli account amministratore che crei.

Il server di gestione utilizza il controllo degli accessi basato sui ruoli (RBAC) per l'accesso utente e le autorizzazioni del ruolo. Se non hai modificato le impostazioni predefinite del server di gestione per l'accesso dell'utente amministrativo, non devi accedere per visualizzarle.

Quando avvii un'operazione che richiede privilegi specifici, il server di gestione ti chiede di accedere. Ad esempio, per creare account amministratore, devi accedere con un account con accesso Application Administrator.

Scopri le tipologie di utente in Active IQ Unified Manager

Un tipo di utente specifica il tipo di account dell'utente e include utenti remoti, gruppi remoti, utenti locali, utenti del database e utenti della manutenzione. Ognuno di questi tipi ha un proprio ruolo, che viene assegnato da un utente con il ruolo di Administrator.

Le tipologie di utente di Unified Manager sono le seguenti:

- **Utente di manutenzione**

  Creato durante la configurazione iniziale di Unified Manager. L'utente addetto alla manutenzione crea quindi altri utenti e assegna loro i ruoli. L'utente addetto alla manutenzione è anche l'unico utente con accesso alla console di manutenzione. Quando Unified Manager viene installato su un sistema Red Hat Enterprise Linux, all'utente addetto alla manutenzione viene assegnato il nome utente "umadmin."

- **Utente locale**

  Accede all'interfaccia utente di Unified Manager ed esegue le funzioni in base al ruolo assegnato dall'utente addetto alla manutenzione o da un utente con il ruolo di amministratore dell'applicazione.

- **Gruppo remoto**

  Un gruppo di utenti che accedono all'interfaccia utente di Unified Manager utilizzando le credenziali memorizzate sul server di autenticazione. Il nome di questo account deve corrispondere al nome di un gruppo memorizzato sul server di autenticazione. A tutti gli utenti all'interno del gruppo remoto viene concesso l'accesso all'interfaccia utente di Unified Manager utilizzando le proprie credenziali individuali. I gruppi remoti possono svolgere funzioni in base ai ruoli loro assegnati.

- **Utente remoto**

  Accede all'interfaccia utente di Unified Manager utilizzando le credenziali memorizzate sul server di autenticazione. Un utente remoto esegue le funzioni in base al ruolo assegnato dall'utente di manutenzione o da un utente con il ruolo di Application Administrator.

- **Utente del database**

  Ha accesso in sola lettura ai dati nel database di Unified Manager, non ha accesso all'interfaccia web di Unified Manager né alla console di manutenzione e non può eseguire chiamate API.

Scopri i ruoli utente in Active IQ Unified Manager

L'utente di manutenzione o l'Application Administrator assegna un ruolo a ogni utente. Ogni ruolo contiene determinati privilegi. L'ambito delle attività che puoi svolgere in Unified Manager dipende dal ruolo che ti è stato assegnato e dai privilegi che tale ruolo contiene.

Unified Manager include i seguenti ruoli utente predefiniti:

- **Operatore**

  Visualizza le informazioni del sistema storage e altri dati raccolti da Unified Manager, inclusi lo storico e l'andamento della capacità. Questo ruolo consente all'operatore storage di visualizzare, assegnare, confermare, risolvere e aggiungere note agli eventi.

- **Amministratore dello storage**

  Configura le operazioni di gestione dello storage all'interno di Unified Manager. Questo ruolo consente all'amministratore dello storage di configurare le soglie e di creare avvisi e altre opzioni e policy specifiche per la gestione dello storage.

- **Amministratore dell'applicazione**

Configura impostazioni non correlate alla gestione dello storage. Questo ruolo consente la gestione di utenti, certificati di sicurezza, accesso al database e opzioni amministrative, tra cui autenticazione, SMTP, rete e AutoSupport.

Quando Unified Manager viene installato su sistemi Linux, all'utente iniziale con il ruolo di Amministratore dell'applicazione viene assegnato automaticamente il nome "umadmin".

- **Schema di integrazione**

  Questo ruolo consente l'accesso in sola lettura alle viste del database di Unified Manager per integrare Unified Manager con OnCommand Workflow Automation (WFA).

- **Schema del report**

  Questo ruolo ti consente l'accesso in sola lettura ai report e ad altre viste del database direttamente dal database di Unified Manager. I database che puoi visualizzare includono:

  - netapp_model_view
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - scalemonitor

Scopri i ruoli e le funzionalità degli utenti in Active IQ Unified Manager

In base al ruolo utente assegnato, puoi determinare quali operazioni puoi eseguire in Unified Manager.

La tabella seguente mostra le funzioni che ciascun ruolo utente può svolgere:

Funzione	Operatore	Amministratore dello storage	Amministratore dell'applicazione	Schema di integrazione	Schema di report
Visualizza le informazioni del sistema storage	•	•	•	•	•
Visualizza altri dati, come cronologie e andamenti della capacità	•	•	•	•	•
Visualizza, assegna e risolvi gli eventi	•	•	•		

Funzione	Operatore	Amministratore dello storage	Amministratore dell'applicazione	Schema di integrazione	Schema di report
Visualizza gli oggetti del servizio storage, come le associazioni SVM e i pool di risorse	•	•	•		
Visualizza le politiche relative alle soglie	•	•	•		
Gestisci gli oggetti del servizio storage, come le associazioni SVM e i pool di risorse		•	•		
Definisci gli avvisi		•	•		
Gestisci le opzioni di gestione dello storage		•	•		
Gestisci le policy di gestione dello storage		•	•		
Gestisci utenti			•		
Gestisci le opzioni amministrative			•		
Definire le politiche di soglia			•		
Gestisci l'accesso al database			•		
Gestisci l'integrazione con WFA e fornisci l'accesso alle viste del database				•	
Pianifica e salva i report		•	•		

Funzione	Operatore	Amministratore dello storage	Amministratore dell'applicazione	Schema di integrazione	Schema di report
Esegui le operazioni "Fix It" da Management Actions		•	•		
Fornisci accesso in sola lettura alle viste del database					•

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.