



# Controlla l'accesso a StorageGRID

## StorageGRID software

NetApp  
December 03, 2025

# Sommario

Controlla l'accesso a StorageGRID . . . . .	1
Controllo dell'accesso a StorageGRID . . . . .	1
Controlla l'accesso al Grid Manager . . . . .	1
Abilita l'accesso singolo . . . . .	1
Cambia la passphrase di provisioning . . . . .	1
Cambiare le password della console del nodo . . . . .	1
Cambia la passphrase di provisioning . . . . .	2
Cambiare le password della console del nodo . . . . .	2
Accedi alla procedura guidata . . . . .	3
Inserisci la passphrase di provisioning . . . . .	3
Scarica il pacchetto di ripristino corrente . . . . .	3
Cambiare le password della console del nodo . . . . .	4
Modificare le password di accesso SSH per i nodi amministrativi . . . . .	5
Accedi alla procedura guidata . . . . .	5
Scarica il pacchetto di ripristino corrente . . . . .	5
Cambia le chiavi di accesso SSH . . . . .	6
Utilizzare la federazione delle identità . . . . .	7
Configurare la federazione delle identità per Grid Manager . . . . .	7
Forza la sincronizzazione con la fonte dell'identità . . . . .	11
Disabilitare la federazione delle identità . . . . .	11
Linee guida per la configurazione di un server OpenLDAP . . . . .	11
Gestisci gruppi di amministratori . . . . .	12
Crea un gruppo di amministratori . . . . .	12
Visualizza e modifica i gruppi di amministrazione . . . . .	14
Duplica un gruppo . . . . .	14
Elimina un gruppo . . . . .	15
Autorizzazioni del gruppo amministratore . . . . .	15
Interazione tra permessi e modalità di accesso . . . . .	15
Accesso root . . . . .	15
Cambia la password di root del tenant . . . . .	16
Configurazione della pagina della topologia della griglia . . . . .	16
ILM . . . . .	16
Manutenzione . . . . .	16
Gestisci gli avvisi . . . . .	17
Query sulle metriche . . . . .	17
Ricerca metadati oggetto . . . . .	17
Altra configurazione della griglia . . . . .	17
Amministratore dell'appliance di archiviazione . . . . .	18
Conti degli inquilini . . . . .	18
Gestisci utenti . . . . .	18
Crea un utente locale . . . . .	18
Visualizza e modifica gli utenti locali . . . . .	19
Duplica un utente . . . . .	21

Elimina un utente . . . . .	21
Utilizzare l'accesso singolo (SSO) . . . . .	21
Configurare l'accesso singolo . . . . .	21
Requisiti e considerazioni per l'accesso singolo . . . . .	25
Conferma che gli utenti federati possono accedere . . . . .	26
Utilizza la modalità sandbox . . . . .	28
Creare trust di relying party in AD FS . . . . .	36
Crea applicazioni aziendali in Azure AD . . . . .	41
Crea connessioni al fornitore di servizi (SP) in PingFederate . . . . .	43
Disabilitare l'accesso singolo . . . . .	47
Disattivare e riattivare temporaneamente l'accesso singolo per un nodo di amministrazione . . . . .	48

# Controlla l'accesso a StorageGRID

## Controllo dell'accesso a StorageGRID

È possibile controllare chi può accedere a StorageGRID e quali attività gli utenti possono eseguire creando o importando gruppi e utenti e assegnando autorizzazioni a ciascun gruppo. Facoltativamente, è possibile abilitare l'accesso singolo (SSO), creare certificati client e modificare le password della griglia.

### Controlla l'accesso al Grid Manager

È possibile determinare chi può accedere a Grid Manager e all'API Grid Management importando gruppi e utenti da un servizio di federazione delle identità o impostando gruppi e utenti locali.

Utilizzando "[federazione di identità](#)" rende l'impostazione "[gruppi](#)" E "[utenti](#)" più veloce e consente agli utenti di accedere a StorageGRID utilizzando credenziali familiari. È possibile configurare la federazione delle identità se si utilizza Active Directory, OpenLDAP o Oracle Directory Server.



Se si desidera utilizzare un altro servizio LDAP v3, contattare l'assistenza tecnica.

Si determinano le attività che ciascun utente può svolgere assegnando diverse "[permessi](#)" a ciascun gruppo. Ad esempio, potresti voler consentire agli utenti di un gruppo di gestire le regole ILM e agli utenti di un altro gruppo di eseguire attività di manutenzione. Per accedere al sistema, un utente deve appartenere ad almeno un gruppo.

Facoltativamente, è possibile configurare un gruppo in sola lettura. Gli utenti di un gruppo di sola lettura possono visualizzare solo impostazioni e funzionalità. Non possono apportare modifiche o eseguire operazioni in Grid Manager o nell'API Grid Management.

### Abilita l'accesso singolo

Il sistema StorageGRID supporta l'accesso Single Sign-On (SSO) utilizzando lo standard Security Assertion Markup Language 2.0 (SAML 2.0). Dopo di te ["configurare e abilitare SSO"](#), tutti gli utenti devono essere autenticati da un provider di identità esterno prima di poter accedere a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API. Gli utenti locali non possono accedere a StorageGRID.

### Cambia la passphrase di provisioning

La passphrase di provisioning è necessaria per numerose procedure di installazione e manutenzione e per scaricare il pacchetto di ripristino StorageGRID . La passphrase è necessaria anche per scaricare i backup delle informazioni sulla topologia della griglia e le chiavi di crittografia per il sistema StorageGRID . Puoi ["cambiare la passphrase"](#) come richiesto.

### Cambiare le password della console del nodo

Ogni nodo nella griglia ha una password univoca per la console del nodo, che è necessaria per accedere al nodo come "admin" tramite SSH oppure come utente root su una connessione alla console fisica/VM. Se necessario, puoi ["cambiare la password della console del nodo"](#) per ogni nodo.

# Cambia la passphrase di provisioning

Utilizzare questa procedura per modificare la passphrase di provisioning StorageGRID . La passphrase è necessaria per le procedure di recupero, espansione e manutenzione. La passphrase è necessaria anche per scaricare i backup del pacchetto di ripristino che includono le informazioni sulla topologia della griglia, le password della console del nodo della griglia e le chiavi di crittografia per il sistema StorageGRID .

## Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai i permessi di accesso di Manutenzione o Root.
- Hai la passphrase di provisioning corrente.

## Informazioni su questo compito

La passphrase di provisioning è richiesta per molte procedure di installazione e manutenzione e per "[scaricando il pacchetto di ripristino](#)" . La passphrase di provisioning non è elencata in `Passwords.txt` file. Assicuratevi di documentare la passphrase di provisioning e di conservarla in un luogo sicuro e protetto.

## Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Password griglia**.
2. In **Modifica passphrase di provisioning**, seleziona **Apporta una modifica**
3. Inserisci la tua passphrase di provisioning attuale.
4. Inserisci la nuova passphrase. La passphrase deve contenere almeno 8 e non più di 32 caratteri. Le passphrase sono sensibili alle maiuscole e alle minuscole.
5. Conservare la nuova passphrase di provisioning in un luogo sicuro. È necessario per le procedure di installazione, ampliamento e manutenzione.
6. Reinserisci la nuova passphrase e seleziona **Salva**.

Una volta completata la modifica della passphrase di provisioning, il sistema visualizza un banner verde di successo.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

7. Selezionare **Pacchetto di ripristino**.

8. Immettere la nuova passphrase di provisioning per scaricare il nuovo pacchetto di ripristino.



Dopo aver modificato la passphrase di provisioning, è necessario scaricare immediatamente un nuovo pacchetto di ripristino. Il file Recovery Package consente di ripristinare il sistema in caso di errore.

# Cambiare le password della console del nodo

Ogni nodo della griglia ha una password univoca per la console del nodo, necessaria per accedere al nodo. Segui questi passaggi per modificare ogni password univoca della console del nodo per ogni nodo nella tua griglia.

## Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Autorizzazione di accesso alla manutenzione o alla root](#)" .
- Hai la passphrase di provisioning corrente.

## Informazioni su questo compito

Utilizzare la password della console del nodo per accedere a un nodo come "admin" tramite SSH oppure come utente root su una connessione VM/console fisica. Il processo di modifica della password della console del nodo crea nuove password per ogni nodo nella griglia e memorizza le password in un file aggiornato `Passwords.txt` nel pacchetto di ripristino. Le password sono elencate nella colonna Password del file `Passwords.txt`.



Esistono password di accesso SSH separate per le chiavi SSH utilizzate per la comunicazione tra i nodi. Questa procedura non modifica le password di accesso SSH.

## Accedi alla procedura guidata

### Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Password griglia**.
2. In **Modifica password console nodo**, seleziona **Apporta una modifica**.

## Inserisci la passphrase di provisioning

### Passi

1. Inserisci la passphrase di provisioning per la tua griglia.
2. Selezionare **Continua**.

## Scarica il pacchetto di ripristino corrente

Prima di modificare le password della console del nodo, scaricare il pacchetto di ripristino corrente. È possibile utilizzare le password contenute in questo file se il processo di modifica della password non riesce per un nodo.

### Passi

1. Seleziona **Scarica pacchetto di ripristino**.
2. Copia il file del pacchetto di ripristino( `.zip` ) in due luoghi sicuri, protetti e separati.
3. Selezionare **Continua**.
4. Quando viene visualizzata la finestra di dialogo di conferma, seleziona **Sì** se sei pronto a iniziare a modificare le password della console del nodo.

Non è possibile annullare questo processo una volta avviato.



Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID .

## Cambiare le password della console del nodo

Quando si avvia il processo di inserimento della password della console del nodo, viene generato un nuovo pacchetto di ripristino che include le nuove password. Quindi, le password vengono aggiornate su ciascun nodo.

### Passi

1. Attendi che venga generato il nuovo pacchetto di ripristino, operazione che potrebbe richiedere alcuni minuti.
2. Seleziona **Scarica nuovo pacchetto di ripristino**.
3. Al termine del download:
  - a. Apri il **.zip** file.
  - b. Conferma di poter accedere ai contenuti, incluso il **Passwords.txt** file, che contiene le nuove password della console del nodo.
  - c. Copia il nuovo file del pacchetto di ripristino(**.zip**) in due luoghi sicuri, protetti e separati.



Non sovrascrivere il vecchio Recovery Package.

Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID .

4. Seleziona la casella di controllo per indicare che hai scaricato il nuovo pacchetto di ripristino e ne hai verificato il contenuto.
5. Selezionare **Modifica password console nodo** e attendere che tutti i nodi vengano aggiornati con le nuove password. Potrebbero volerci alcuni minuti.

Se le password vengono modificate per tutti i nodi, viene visualizzato un banner verde di operazione riuscita. Vai al passaggio successivo.

Se si verifica un errore durante il processo di aggiornamento, un messaggio banner elenca il numero di nodi le cui password non sono state modificate. Il sistema riproverà automaticamente il processo su qualsiasi nodo la cui password non è riuscita a cambiare. Se il processo termina con alcuni nodi che non hanno ancora modificato la password, viene visualizzato il pulsante **Riprova**.

Se l'aggiornamento della password non è riuscito per uno o più nodi:

- a. Esaminare i messaggi di errore elencati nella tabella.
- b. Risolvere i problemi.
- c. Seleziona **Riprova**.



Il nuovo tentativo modifica solo le password della console dei nodi che non sono riusciti nei precedenti tentativi di modifica della password.

6. Dopo aver modificato le password della console del nodo per tutti i nodi, eliminare il [primo pacchetto di ripristino scaricato](#).
7. Facoltativamente, utilizzare il collegamento **Pacchetto di ripristino** per scaricare una copia aggiuntiva del nuovo Pacchetto di ripristino.

# Modificare le password di accesso SSH per i nodi amministrativi

La modifica delle password di accesso SSH per i nodi amministrativi aggiorna anche i set univoci di chiavi SSH interne per ciascun nodo nella griglia. Il nodo di amministrazione primario utilizza queste chiavi SSH per accedere ai nodi tramite autenticazione sicura e senza password.

Utilizzare una chiave SSH per accedere a un nodo come `admin` o all'utente `root` su una macchina virtuale o su una connessione alla console fisica.

## Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Autorizzazione di accesso alla manutenzione o alla root](#)" .
- Hai la passphrase di provisioning corrente.

## Informazioni su questo compito

Le nuove password di accesso per i nodi di amministrazione e le nuove chiavi interne per ciascun nodo sono memorizzate nel `Passwords.txt` file nel pacchetto di ripristino. Le chiavi sono elencate nella colonna Password di quel file.

Esistono password di accesso SSH separate per le chiavi SSH utilizzate per la comunicazione tra i nodi. Questa procedura non li modifica.

## Accedi alla procedura guidata

### Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Password griglia**.
2. In **Modifica chiavi SSH**, seleziona **Apporta una modifica**.

## Scarica il pacchetto di ripristino corrente

Prima di modificare le chiavi di accesso SSH, scaricare il pacchetto di ripristino corrente. È possibile utilizzare le chiavi contenute in questo file se il processo di modifica delle chiavi non riesce per un nodo.

### Passi

1. Inserisci la passphrase di provisioning per la tua griglia.
2. Seleziona **Scarica pacchetto di ripristino**.
3. Copia il file del pacchetto di ripristino( `.zip` ) in due luoghi sicuri, protetti e separati.



Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID .

4. Selezionare **Continua**.
5. Quando viene visualizzata la finestra di dialogo di conferma, seleziona **Sì** se sei pronto a iniziare a modificare le chiavi di accesso SSH.



Non è possibile annullare questo processo una volta avviato.

## Cambia le chiavi di accesso SSH

Quando viene avviato il processo di modifica delle chiavi di accesso SSH, viene generato un nuovo pacchetto di ripristino che include le nuove chiavi. Quindi, le chiavi vengono aggiornate su ciascun nodo.

### Passi

1. Attendi che venga generato il nuovo pacchetto di ripristino, operazione che potrebbe richiedere alcuni minuti.
2. Quando il pulsante Scarica nuovo pacchetto di ripristino è abilitato, seleziona **Scarica nuovo pacchetto di ripristino** e salva il nuovo file del pacchetto di ripristino( .zip ) in due luoghi sicuri, protetti e separati.
3. Al termine del download:
  - a. Apri il .zip file.
  - b. Conferma di poter accedere ai contenuti, incluso il Passwords.txt file, che contiene le nuove chiavi di accesso SSH.
  - c. Copia il nuovo file del pacchetto di ripristino( .zip ) in due luoghi sicuri, protetti e separati.



Non sovrascrivere il vecchio Recovery Package.

Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID .

4. Attendi che le chiavi vengano aggiornate su ciascun nodo, operazione che potrebbe richiedere alcuni minuti.

Se le chiavi vengono modificate per tutti i nodi, viene visualizzato un banner verde di successo.

Se si verifica un errore durante il processo di aggiornamento, un messaggio banner elenca il numero di nodi le cui chiavi non sono state modificate. Il sistema riproverà automaticamente il processo su qualsiasi nodo la cui chiave non è riuscita a cambiare. Se il processo termina con alcuni nodi che non hanno ancora una chiave modificata, viene visualizzato il pulsante **Riprova**.

Se l'aggiornamento della chiave non è riuscito per uno o più nodi:

- a. Esaminare i messaggi di errore elencati nella tabella.
- b. Risolvere i problemi.
- c. Seleziona **Riprova**.

Il nuovo tentativo modifica solo le chiavi di accesso SSH sui nodi che non sono riusciti durante i precedenti tentativi di modifica delle chiavi.

5. Dopo aver modificato le chiavi di accesso SSH per tutti i nodi, eliminare [primo pacchetto di ripristino scaricato](#) .
6. Facoltativamente, selezionare **MANUTENZIONE > Sistema > Pacchetto di ripristino** per scaricare una copia aggiuntiva del nuovo Pacchetto di ripristino.

# Utilizzare la federazione delle identità

L'utilizzo della federazione delle identità velocizza la configurazione di gruppi e utenti e consente agli utenti di accedere a StorageGRID utilizzando credenziali familiari.

## Configurare la federazione delle identità per Grid Manager

È possibile configurare la federazione delle identità in Grid Manager se si desidera che i gruppi di amministratori e gli utenti vengano gestiti in un altro sistema, ad esempio Active Directory, Azure Active Directory (Azure AD), OpenLDAP o Oracle Directory Server.

### Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .
- Stai utilizzando Active Directory, Azure AD, OpenLDAP o Oracle Directory Server come provider di identità.



Se si desidera utilizzare un servizio LDAP v3 non presente nell'elenco, contattare l'assistenza tecnica.

- Se si prevede di utilizzare OpenLDAP, è necessario configurare il server OpenLDAP. Vedere [Linee guida per la configurazione di un server OpenLDAP](#) .
- Se si prevede di abilitare l'accesso singolo (SSO), è necessario aver esaminato il "[requisiti e considerazioni per l'accesso unico](#)" .
- Se si prevede di utilizzare Transport Layer Security (TLS) per le comunicazioni con il server LDAP, il provider di identità utilizza TLS 1.2 o 1.3. Vedere "[Cifrature supportate per le connessioni TLS in uscita](#)" .

### Informazioni su questo compito

È possibile configurare un'origine identità per Grid Manager se si desidera importare gruppi da un altro sistema, ad esempio Active Directory, Azure AD, OpenLDAP o Oracle Directory Server. È possibile importare i seguenti tipi di gruppi:

- Gruppi di amministrazione. Gli utenti nei gruppi di amministrazione possono accedere a Grid Manager ed eseguire attività in base alle autorizzazioni di gestione assegnate al gruppo.
- Gruppi di utenti tenant per tenant che non utilizzano una propria fonte di identità. Gli utenti nei gruppi di tenant possono accedere a Tenant Manager ed eseguire attività in base alle autorizzazioni assegnate al gruppo in Tenant Manager. Vedere "[Crea un account inquilino](#)" E "[Utilizzare un account tenant](#)" per i dettagli.

## Inserisci la configurazione

### Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Federazione identità**.
2. Selezionare **Abilita federazione delle identità**.
3. Nella sezione **Tipo di servizio LDAP**, seleziona il tipo di servizio LDAP che desideri configurare.

## LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

Azure

OpenLDAP

Other

Selezionare **Altro** per configurare i valori per un server LDAP che utilizza Oracle Directory Server.

4. Se hai selezionato **Altro**, compila i campi nella sezione Attributi LDAP. procedere al passaggio successivo.

- **Nome univoco utente:** il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a `sAMAccountName` per Active Directory e `uid` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `uid`.
- **UUID utente:** il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a `objectGUID` per Active Directory e `entryUUID` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun utente per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.
- **Nome univoco del gruppo:** il nome dell'attributo che contiene l'identificatore univoco di un gruppo LDAP. Questo attributo è equivalente a `sAMAccountName` per Active Directory e `cn` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `cn`.
- **UUID gruppo:** il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a `objectGUID` per Active Directory e `entryUUID` per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale di 32 cifre in formato stringa o a 16 byte, in cui i trattini vengono ignorati.

5. Per tutti i tipi di servizio LDAP, immettere le informazioni richieste sul server LDAP e sulla connessione di rete nella sezione Configura server LDAP.

- **Nome host:** nome di dominio completo (FQDN) o indirizzo IP del server LDAP.
- **Porta:** la porta utilizzata per connettersi al server LDAP.



La porta predefinita per STARTTLS è 389, mentre la porta predefinita per LDAPS è 636. Tuttavia, puoi utilizzare qualsiasi porta, a patto che il firewall sia configurato correttamente.

- **Nome utente:** percorso completo del nome distinto (DN) dell'utente che si conserverà al server LDAP.

Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome dell'entità utente.

L'utente specificato deve avere l'autorizzazione per elencare gruppi e utenti e per accedere ai seguenti attributi:

- `sAMAccountName` `O` `uid`
- `objectGUID`, `entryUUID` , O `nsuniqueid`
- `cn`

- memberOf`O `isMemberOf
  - **Directory attiva:** objectSid , primaryGroupID , userAccountControl , E userPrincipalName
  - **Azzurro:** accountEnabled E userPrincipalName
  - **Password:** la password associata al nome utente.
-  Se in futuro dovessi cambiare la password, dovrà aggiornarla in questa pagina.
- **DN base gruppo:** percorso completo del nome distinto (DN) per un sottoalbero LDAP in cui si desidera cercare i gruppi. Nell'esempio di Active Directory (sotto), tutti i gruppi il cui nome distinto è relativo al DN di base (DC=storagegrid,DC=example,DC=com) possono essere utilizzati come gruppi federati.
-  I valori **Nome univoco del gruppo** devono essere univoci all'interno del **DN di base del gruppo** a cui appartengono.
- **DN base utente:** percorso completo del nome distinto (DN) di un sottoalbero LDAP in cui si desidera cercare gli utenti.



I valori **Nome univoco utente** devono essere univoci all'interno del **Nome base utente** a cui appartengono.

- **Formato nome utente associato** (facoltativo): il modello di nome utente predefinito che StorageGRID dovrebbe utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il **formato nome utente di associazione** perché può consentire agli utenti di accedere se StorageGRID non è in grado di assocarsi all'account di servizio.

Inserisci uno di questi modelli:

- **Modello UserPrincipalName (Active Directory e Azure):** [USERNAME]@example.com
- **Modello di nome di accesso di livello inferiore (Active Directory e Azure):**  
example\ [USERNAME]
- **Modello di nome distinto:** CN=[USERNAME] , CN=Users, DC=example, DC=com

Includi **[USERNAME]** esattamente come scritto.

## 6. Nella sezione Transport Layer Security (TLS), seleziona un'impostazione di sicurezza.

- **Usa STARTTLS:** usa STARTTLS per proteggere le comunicazioni con il server LDAP. Questa è l'opzione consigliata per Active Directory, OpenLDAP o Altro, ma non è supportata per Azure.
- **Usa LDAPS:** l'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. È necessario selezionare questa opzione per Azure.
- **Non utilizzare TLS:** il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Azure.



L'utilizzo dell'opzione **Non utilizzare TLS** non è supportato se il server Active Directory impone la firma LDAP. È necessario utilizzare STARTTLS o LDAPS.

## 7. Se hai selezionato STARTTLS o LDAPS, scegli il certificato utilizzato per proteggere la connessione.

- **Utilizza il certificato CA del sistema operativo:** utilizza il certificato Grid CA predefinito installato sul sistema operativo per proteggere le connessioni.
- **Utilizza certificato CA personalizzato:** utilizza un certificato di sicurezza personalizzato.

Se selezioni questa impostazione, copia e incolla il certificato di sicurezza personalizzato nella casella di testo Certificato CA.

## Testare la connessione e salvare la configurazione

Dopo aver immesso tutti i valori, è necessario testare la connessione prima di poter salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente associato, se ne è stato fornito uno.

### Passi

1. Selezionare **Test connessione**.
2. Se non hai fornito un formato di nome utente di associazione:
  - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test di connessione riuscito". Selezionare **Salva** per salvare la configurazione.
  - Se le impostazioni di connessione non sono valide, viene visualizzato il messaggio "Impossibile stabilire la connessione di prova". Selezionare **Chiudi**. Quindi, risovi eventuali problemi e verifica nuovamente la connessione.
3. Se hai fornito un formato di nome utente vincolato, inserisci il nome utente e la password di un utente federato valido.

Ad esempio, inserisci il tuo nome utente e la tua password. Non includere caratteri speciali nel nome utente, come @ o /.

The screenshot shows a 'Test Connection' dialog box. At the top, it says 'Test Connection' and has a close button. Below that, there's a message: 'To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.' There are two input fields: 'Test username' containing 'myusername' and 'Test password' containing redacted text. Below the password field is a visibility toggle icon. At the bottom left is a 'Cancel' button, and at the bottom right is a blue 'Test Connection' button.

- Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test di connessione riuscito". Selezionare **Salva** per salvare la configurazione.
- Se le impostazioni di connessione, il formato del nome utente associato o il nome utente e la password di prova non sono validi, viene visualizzato un messaggio di errore. Risovi eventuali problemi e verifica nuovamente la connessione.

## Forza la sincronizzazione con la fonte dell'identità

Il sistema StorageGRID sincronizza periodicamente i gruppi federati e gli utenti dalla fonte di identità. È possibile forzare l'avvio della sincronizzazione se si desidera abilitare o limitare le autorizzazioni utente il più rapidamente possibile.

### Passi

1. Vai alla pagina Federazione delle identità.
2. Seleziona **Sincronizza server** nella parte superiore della pagina.

Il processo di sincronizzazione potrebbe richiedere del tempo, a seconda dell'ambiente.



L'avviso **Errore di sincronizzazione della federazione delle identità** viene attivato se si verifica un problema durante la sincronizzazione di gruppi e utenti federati dall'origine dell'identità.

## Disabilitare la federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione delle identità per gruppi e utenti. Quando la federazione delle identità è disabilitata, non c'è comunicazione tra StorageGRID e l'origine dell'identità. Tuttavia, tutte le impostazioni configurate vengono mantenute, consentendoti di riattivare facilmente la federazione delle identità in futuro.

### Informazioni su questo compito

Prima di disattivare la federazione delle identità, è necessario tenere presente quanto segue:

- Gli utenti federati non potranno effettuare l'accesso.
- Gli utenti federati attualmente connessi manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno effettuare l'accesso dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non verrà eseguita e non verranno generati avvisi per gli account che non sono stati sincronizzati.
- La casella di controllo **Abilita federazione delle identità** è disabilitata se l'accesso Single Sign-On (SSO) è impostato su **Abilitato** o **Modalità Sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedere "[Disabilitare l'accesso singolo](#)".

### Passi

1. Vai alla pagina Federazione delle identità.
2. Deseleziona la casella di controllo **Abilita federazione delle identità**.

## Linee guida per la configurazione di un server OpenLDAP

Se si desidera utilizzare un server OpenLDAP per la federazione delle identità, è necessario configurare impostazioni specifiche sul server OpenLDAP.



Per le origini identità diverse da ActiveDirectory o Azure, StorageGRID non bloccherà automaticamente l'accesso S3 agli utenti disabilitati esternamente. Per bloccare l'accesso S3, eliminare tutte le chiavi S3 dell'utente o rimuovere l'utente da tutti i gruppi.

## Sovraposizioni di membri e raffinazione

Le sovrapposizioni memberof e refint dovrebbero essere abilitate. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo in <http://www.openldap.org/doc/admin24/index.html>["Documentazione OpenLDAP: Guida dell'amministratore versione 2.4"] .

## Indicizzazione

È necessario configurare i seguenti attributi OpenLDAP con le parole chiave di indice specificate:

- olcDbIndex: objectClass eq
- olcDbIndex: uid eq,pres,sub
- olcDbIndex: cn eq,pres,sub
- olcDbIndex: entryUUID eq

Inoltre, assicurati che i campi menzionati nella guida per Nome utente siano indicizzati per prestazioni ottimali.

Consultare le informazioni sul mantenimento dell'appartenenza al gruppo inverso in <http://www.openldap.org/doc/admin24/index.html>["Documentazione OpenLDAP: Guida dell'amministratore versione 2.4"] .

## Gestisci gruppi di amministratori

È possibile creare gruppi di amministratori per gestire le autorizzazioni di sicurezza per uno o più utenti amministratori. Per poter accedere al sistema StorageGRID , gli utenti devono appartenere a un gruppo.

### Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .
- Se si prevede di importare un gruppo federato, è necessario aver configurato la federazione delle identità e il gruppo federato esiste già nell'origine identità configurata.

## Crea un gruppo di amministratori

I gruppi di amministratori consentono di stabilire quali utenti possono accedere a quali funzionalità e operazioni in Grid Manager e nell'API Grid Management.

### Accedi alla procedura guidata

#### Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Gruppi amministratori**.
2. Seleziona **Crea gruppo**.

### Scegli un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federato.

- Crea un gruppo locale se vuoi assegnare autorizzazioni agli utenti locali.
- Crea un gruppo federato per importare gli utenti dall'origine dell'identità.

## Gruppo locale

### Passi

1. Seleziona **Gruppo locale**.
2. Inserisci un nome visualizzato per il gruppo, che potrai aggiornare in seguito se necessario. Ad esempio, "Utenti addetti alla manutenzione" o "Amministratori ILM".
3. Inserisci un nome univoco per il gruppo, che non potrai aggiornare in seguito.
4. Selezionare **Continua**.

## Gruppo federato

### Passi

1. Seleziona **Gruppo federato**.
2. Inserisci il nome del gruppo che desideri importare, esattamente come appare nell'origine identità configurata.
  - Per Active Directory e Azure, utilizzare sAMAccountName.
  - Per OpenLDAP, utilizzare il CN (nome comune).
  - Per un altro LDAP, utilizzare il nome univoco appropriato per il server LDAP.
3. Selezionare **Continua**.

## Gestisci i permessi del gruppo

### Passi

1. Per la **Modalità di accesso**, seleziona se gli utenti del gruppo possono modificare le impostazioni ed eseguire operazioni in Grid Manager e nell'API di gestione della griglia oppure se possono solo visualizzare impostazioni e funzionalità.
  - **Lettura-scrittura** (predefinito): gli utenti possono modificare le impostazioni ed eseguire le operazioni consentite dalle loro autorizzazioni di gestione.
  - **Sola lettura**: gli utenti possono solo visualizzare impostazioni e funzionalità. Non possono apportare modifiche o eseguire operazioni in Grid Manager o nell'API Grid Management. Gli utenti locali con privilegi di sola lettura possono modificare le proprie password.



Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su **Sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

2. Seleziona uno o più "autorizzazioni del gruppo amministratore" .

È necessario assegnare almeno un'autorizzazione a ciascun gruppo; in caso contrario, gli utenti appartenenti al gruppo non potranno accedere a StorageGRID.

3. Se stai creando un gruppo locale, seleziona **Continua**. Se stai creando un gruppo federato, seleziona **Crea gruppo e Fine**.

## Aggiungi utenti (solo gruppi locali)

### Passi

1. Facoltativamente, seleziona uno o più utenti locali per questo gruppo.

Se non hai ancora creato utenti locali, puoi salvare il gruppo senza aggiungere utenti. Puoi aggiungere questo gruppo all'utente nella pagina Utenti. Vedere "[Gestisci utenti](#)" per i dettagli.

2. Seleziona **Crea gruppo e Fine**.

## Visualizza e modifica i gruppi di amministrazione

È possibile visualizzare i dettagli dei gruppi esistenti, modificare un gruppo o duplicare un gruppo.

- Per visualizzare le informazioni di base per tutti i gruppi, consultare la tabella nella pagina Gruppi.
- Per visualizzare tutti i dettagli di un gruppo specifico o per modificare un gruppo, utilizzare il menu **Azioni** o la pagina dei dettagli.

Compito	Menu Azioni	Pagina dei dettagli
Visualizza i dettagli del gruppo	a. Selezionare la casella di controllo per il gruppo. b. Seleziona <b>Azioni &gt; Visualizza dettagli gruppo</b> .	Selezionare il nome del gruppo nella tabella.
Modifica il nome visualizzato (solo gruppi locali)	a. Selezionare la casella di controllo per il gruppo. b. Seleziona <b>Azioni &gt; Modifica nome gruppo</b> . c. Inserisci il nuovo nome. d. Seleziona <b>Salva modifiche</b> .	a. Selezionare il nome del gruppo per visualizzarne i dettagli. b. Seleziona l'icona di modifica  . c. Inserisci il nuovo nome. d. Seleziona <b>Salva modifiche</b> .
Modifica la modalità di accesso o le autorizzazioni	a. Selezionare la casella di controllo per il gruppo. b. Seleziona <b>Azioni &gt; Visualizza dettagli gruppo</b> . c. Facoltativamente, modifica la modalità di accesso del gruppo. d. Facoltativamente, seleziona o deselectiona "autorizzazioni del gruppo amministratore". e. Seleziona <b>Salva modifiche</b> .	a. Selezionare il nome del gruppo per visualizzarne i dettagli. b. Facoltativamente, modifica la modalità di accesso del gruppo. c. Facoltativamente, seleziona o deselectiona "autorizzazioni del gruppo amministratore". d. Seleziona <b>Salva modifiche</b> .

## Duplica un gruppo

### Passi

1. Selezionare la casella di controllo per il gruppo.

2. Selezionare **Azioni > Duplica gruppo**.
3. Completa la procedura guidata Duplica gruppo.

## Elimina un gruppo

È possibile eliminare un gruppo di amministratori quando si desidera rimuovere il gruppo dal sistema e rimuovere tutte le autorizzazioni ad esso associate. L'eliminazione di un gruppo di amministratori rimuove tutti gli utenti dal gruppo, ma non elimina gli utenti stessi.

### Passi

1. Nella pagina Gruppi, seleziona la casella di controllo per ogni gruppo che desideri rimuovere.
2. Selezionare **Azioni > Elimina gruppo**.
3. Seleziona **Elimina gruppi**.

## Autorizzazioni del gruppo amministratore

Quando si creano gruppi di utenti amministratori, si selezionano una o più autorizzazioni per controllare l'accesso a funzionalità specifiche di Grid Manager. È quindi possibile assegnare ciascun utente a uno o più di questi gruppi di amministratori per determinare quali attività può eseguire quell'utente.

È necessario assegnare almeno un'autorizzazione a ciascun gruppo; in caso contrario, gli utenti appartenenti a quel gruppo non potranno accedere a Grid Manager o all'API Grid Management.

Per impostazione predefinita, qualsiasi utente appartenente a un gruppo che dispone di almeno un'autorizzazione può eseguire le seguenti attività:

- Sign in a Grid Manager
- Visualizza la dashboard
- Visualizza le pagine dei nodi
- Visualizza gli avvisi correnti e risolti
- Cambiare la propria password (solo utenti locali)
- Visualizzare alcune informazioni fornite nelle pagine Configurazione e Manutenzione

## Interazione tra permessi e modalità di accesso

Per tutte le autorizzazioni, l'impostazione **Modalità di accesso** del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni oppure se possono solo visualizzare le impostazioni e le funzionalità correlate. Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su **Sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

Nelle sezioni seguenti vengono descritte le autorizzazioni che è possibile assegnare durante la creazione o la modifica di un gruppo di amministratori. Per qualsiasi funzionalità non esplicitamente menzionata è necessario il permesso di **accesso root**.

### Accesso root

Questa autorizzazione fornisce l'accesso a tutte le funzionalità di amministrazione della griglia.

## Cambia la password di root del tenant

Questa autorizzazione fornisce l'accesso all'opzione **Cambia password di root** nella pagina Tenant, consentendo di controllare chi può modificare la password per l'utente root locale del tenant. Questa autorizzazione viene utilizzata anche per la migrazione delle chiavi S3 quando è abilitata la funzionalità di importazione delle chiavi S3. Gli utenti che non dispongono di questa autorizzazione non possono visualizzare l'opzione **Cambia password di root**.



Per concedere l'accesso alla pagina Tenant, che contiene l'opzione **Cambia password di root**, assegnare anche l'autorizzazione **Account tenant**.

## Configurazione della pagina della topologia della griglia

Questa autorizzazione consente di accedere alle schede Configurazione nella pagina **SUPPORTO > Strumenti > Topologia griglia**.



La pagina Topologia griglia è stata deprecata e verrà rimossa in una versione futura.

## ILM

Questa autorizzazione fornisce l'accesso alle seguenti opzioni del menu **ILM**:

- Regole
- Politiche
- Tag di policy
- Pool di stoccaggio
- Gradi di stoccaggio
- Regioni
- Ricerca metadati oggetto



Per gestire i gradi di archiviazione, gli utenti devono disporre delle autorizzazioni **Altra configurazione della griglia** e **Configurazione della pagina della topologia della griglia**.

## Manutenzione

Per utilizzare queste opzioni, gli utenti devono disporre dell'autorizzazione di manutenzione:

- **CONFIGURAZIONE > Controllo accessi:**
  - Password di griglia
- **CONFIGURAZIONE > Rete:**
  - Nomi di dominio endpoint S3
- **MANUTENZIONE > Attività:**
  - Dismissione
  - Espansione
  - Controllo dell'esistenza dell'oggetto

- Recupero

- **MANUTENZIONE > Sistema:**

- Pacchetto di recupero
- Aggiornamento software

- **SUPPORTO > Strumenti:**

- Registri

Gli utenti che non dispongono dell'autorizzazione di manutenzione possono visualizzare, ma non modificare, queste pagine:

- **MANUTENZIONE > Rete:**

- server DNS
- Rete a griglia
- server NTP

- **MANUTENZIONE > Sistema:**

- Licenza

- **CONFIGURAZIONE > Rete:**

- Nomi di dominio endpoint S3

- **CONFIGURAZIONE > Sicurezza:**

- Certificati

- **CONFIGURAZIONE > Monitoraggio:**

- Server di audit e syslog

## Gestisci gli avvisi

Questa autorizzazione fornisce l'accesso alle opzioni per la gestione degli avvisi. Gli utenti devono disporre di questa autorizzazione per gestire silenzi, notifiche di avviso e regole di avviso.

## Query sulle metriche

Questa autorizzazione fornisce l'accesso a:

- Pagina **SUPPORTO > Strumenti > Metriche**
- Query personalizzate sulle metriche Prometheus utilizzando la sezione **Metriche** dell'API di gestione della griglia
- Schede della dashboard di Grid Manager che contengono metriche

## Ricerca metadati oggetto

Questa autorizzazione fornisce l'accesso alla pagina **ILM > Ricerca metadati oggetto**.

## Altra configurazione della griglia

Questa autorizzazione fornisce l'accesso ad ulteriori opzioni di configurazione della griglia.



Per visualizzare queste opzioni aggiuntive, gli utenti devono disporre anche dell'autorizzazione **Configurazione della pagina topologia griglia**.

- **ILM:**

- Gradi di stoccaggio

- **CONFIGURAZIONE > Sistema:**

- **SUPPORTO > Altro:**

- Costo del collegamento

## Amministratore dell'appliance di archiviazione

Questa autorizzazione prevede:

- Accesso a E-Series SANtricity System Manager su dispositivi di storage tramite Grid Manager.
- Possibilità di eseguire attività di risoluzione dei problemi e manutenzione nella scheda Gestisci unità per gli apparecchi che supportano queste operazioni.

## Conti degli inquilini

Questa autorizzazione fornisce la possibilità di:

- Accedi alla pagina Inquilini, dove puoi creare, modificare e rimuovere gli account degli inquilini
- Visualizza le policy di classificazione del traffico esistenti
- Visualizza le schede della dashboard di Grid Manager che contengono i dettagli del tenant

## Gestisci utenti

È possibile visualizzare gli utenti locali e federati. È anche possibile creare utenti locali e assegnarli a gruppi di amministratori locali per determinare a quali funzionalità di Grid Manager possono accedere questi utenti.

### Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .

### Crea un utente locale

È possibile creare uno o più utenti locali e assegnare ciascun utente a uno o più gruppi locali. Le autorizzazioni del gruppo controllano a quali funzionalità di Grid Manager e Grid Management API l'utente può accedere.

È possibile creare solo utenti locali. Utilizzare la fonte di identità esterna per gestire utenti e gruppi federati.

Grid Manager include un utente locale predefinito, denominato "root". Non è possibile rimuovere l'utente root.



Se è abilitato l'accesso Single Sign-On (SSO), gli utenti locali non possono accedere a StorageGRID.

## Accedi alla procedura guidata

### Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Utenti amministratori.**
2. Seleziona **Crea utente.**

## Inserisci le credenziali utente

### Passi

1. Inserisci il nome completo dell'utente, un nome utente univoco e una password.
2. Facoltativamente, seleziona **Sì** se questo utente non deve avere accesso a Grid Manager o all'API Grid Management.
3. Selezionare **Continua.**

## Assegna ai gruppi

### Passi

1. Facoltativamente, assegnare l'utente a uno o più gruppi per determinare le autorizzazioni dell'utente.

Se non hai ancora creato gruppi, puoi salvare l'utente senza selezionare i gruppi. Puoi aggiungere questo utente a un gruppo nella pagina Gruppi.

Se un utente appartiene a più gruppi, le autorizzazioni sono cumulative. Vedere "[Gestisci gruppi di amministratori](#)" per i dettagli.

2. Selezionare **Crea utente** e poi **Fine.**

## Visualizza e modifica gli utenti locali

È possibile visualizzare i dettagli degli utenti locali e federati esistenti. È possibile modificare un utente locale per cambiarne il nome completo, la password o l'appartenenza al gruppo. È anche possibile impedire temporaneamente a un utente di accedere a Grid Manager e all'API Grid Management.

È possibile modificare solo gli utenti locali. Utilizzare la fonte di identità esterna per gestire gli utenti federati.

- Per visualizzare le informazioni di base per tutti gli utenti locali e federati, consultare la tabella nella pagina Utenti.
- Per visualizzare tutti i dettagli di un utente specifico, modificare un utente locale o cambiare la password di un utente locale, utilizzare il menu **Azioni** o la pagina dei dettagli.

Tutte le modifiche verranno applicate la volta successiva che l'utente si disconnette e accede nuovamente a Grid Manager.



Gli utenti locali possono modificare le proprie password utilizzando l'opzione **Cambia password** nel banner di Grid Manager.

Compito	Menu Azioni	Pagina dei dettagli
Visualizza i dettagli dell'utente	<ul style="list-style-type: none"> <li>a. Selezionare la casella di controllo per l'utente.</li> <li>b. Seleziona <b>Azioni &gt; Visualizza dettagli utente</b>.</li> </ul>	Selezionare il nome dell'utente nella tabella.
Modifica il nome completo (solo utenti locali)	<ul style="list-style-type: none"> <li>a. Selezionare la casella di controllo per l'utente.</li> <li>b. Seleziona <b>Azioni &gt; Modifica nome completo</b>.</li> <li>c. Inserisci il nuovo nome.</li> <li>d. Seleziona <b>Salva modifiche</b>.</li> </ul>	<ul style="list-style-type: none"> <li>a. Selezionare il nome dell'utente per visualizzarne i dettagli.</li> <li>b. Seleziona l'icona di modifica .</li> <li>c. Inserisci il nuovo nome.</li> <li>d. Seleziona <b>Salva modifiche</b>.</li> </ul>
Nega o consenti l'accesso a StorageGRID	<ul style="list-style-type: none"> <li>a. Selezionare la casella di controllo per l'utente.</li> <li>b. Seleziona <b>Azioni &gt; Visualizza dettagli utente</b>.</li> <li>c. Selezionare la scheda Accesso.</li> <li>d. Selezionare <b>Sì</b> per impedire all'utente di accedere a Grid Manager o all'API di gestione della griglia, oppure selezionare <b>No</b> per consentire all'utente di accedere.</li> <li>e. Seleziona <b>Salva modifiche</b>.</li> </ul>	<ul style="list-style-type: none"> <li>a. Selezionare il nome dell'utente per visualizzarne i dettagli.</li> <li>b. Selezionare la scheda Accesso.</li> <li>c. Selezionare <b>Sì</b> per impedire all'utente di accedere a Grid Manager o all'API di gestione della griglia, oppure selezionare <b>No</b> per consentire all'utente di accedere.</li> <li>d. Seleziona <b>Salva modifiche</b>.</li> </ul>
Cambia password (solo utenti locali)	<ul style="list-style-type: none"> <li>a. Selezionare la casella di controllo per l'utente.</li> <li>b. Seleziona <b>Azioni &gt; Visualizza dettagli utente</b>.</li> <li>c. Selezionare la scheda Password.</li> <li>d. Inserisci una nuova password.</li> <li>e. Seleziona <b>Cambia password</b>.</li> </ul>	<ul style="list-style-type: none"> <li>a. Selezionare il nome dell'utente per visualizzarne i dettagli.</li> <li>b. Selezionare la scheda Password.</li> <li>c. Inserisci una nuova password.</li> <li>d. Seleziona <b>Cambia password</b>.</li> </ul>

Compito	Menu Azioni	Pagina dei dettagli
Cambia gruppi (solo utenti locali)	<ul style="list-style-type: none"> <li>a. Selezionare la casella di controllo per l'utente.</li> <li>b. Seleziona <b>Azioni &gt; Visualizza dettagli utente</b>.</li> <li>c. Selezionare la scheda Gruppi.</li> <li>d. Facoltativamente, seleziona il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser.</li> <li>e. Selezionare <b>Modifica gruppi</b> per selezionare gruppi diversi.</li> <li>f. Seleziona <b>Salva modifiche</b>.</li> </ul>	<ul style="list-style-type: none"> <li>a. Selezionare il nome dell'utente per visualizzarne i dettagli.</li> <li>b. Selezionare la scheda Gruppi.</li> <li>c. Facoltativamente, seleziona il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser.</li> <li>d. Selezionare <b>Modifica gruppi</b> per selezionare gruppi diversi.</li> <li>e. Seleziona <b>Salva modifiche</b>.</li> </ul>

## Duplica un utente

È possibile duplicare un utente esistente per crearne uno nuovo con le stesse autorizzazioni.

### Passi

1. Selezionare la casella di controllo per l'utente.
2. Selezionare **Azioni > Duplica utente**.
3. Completa la procedura guidata Duplica utente.

## Elimina un utente

È possibile eliminare un utente locale per rimuoverlo definitivamente dal sistema.



Non è possibile eliminare l'utente root.

### Passi

1. Nella pagina Utenti, seleziona la casella di controllo per ogni utente che desideri rimuovere.
2. Selezionare **Azioni > Elimina utente**.
3. Seleziona **Elimina utente**.

## Utilizzare l'accesso singolo (SSO)

### Configurare l'accesso singolo

Quando è abilitato l'accesso Single Sign-On (SSO), gli utenti possono accedere a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API solo se le loro credenziali sono autorizzate tramite il processo di accesso SSO implementato dalla tua organizzazione. Gli utenti locali non possono accedere a StorageGRID.

## Come funziona l'accesso singolo

Il sistema StorageGRID supporta l'accesso Single Sign-On (SSO) utilizzando lo standard Security Assertion Markup Language 2.0 (SAML 2.0).

Prima di abilitare l'accesso Single Sign-On (SSO), esaminare in che modo i processi di accesso e disconnessione StorageGRID vengono influenzati dall'abilitazione dell'SSO.

### Sign in quando SSO è abilitato

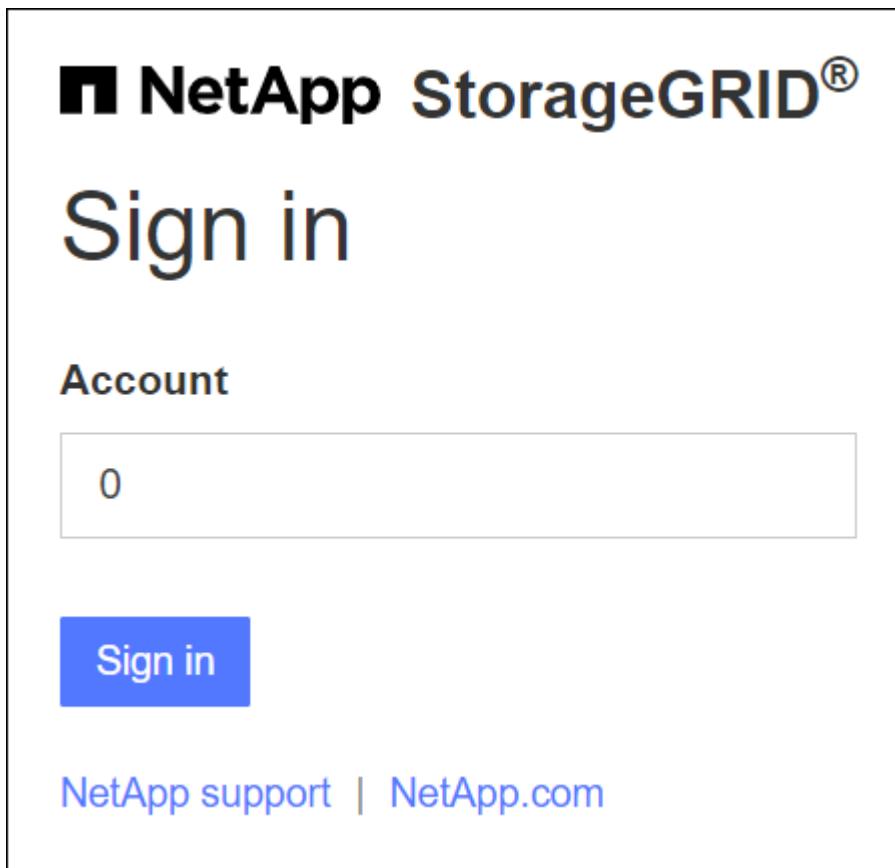
Quando l'SSO è abilitato e accedi a StorageGRID, verrai reindirizzato alla pagina SSO della tua organizzazione per convalidare le tue credenziali.

### Passi

1. Immettere il nome di dominio completo o l'indirizzo IP di qualsiasi nodo di amministrazione StorageGRID in un browser Web.

Viene visualizzata la pagina Sign in a StorageGRID .

- Se è la prima volta che accedi all'URL su questo browser, ti verrà richiesto un ID account:



- Se hai già effettuato l'accesso a Grid Manager o Tenant Manager, ti verrà chiesto di selezionare un account recente o di immettere un ID account:



# Tenant Manager

## Recent

S3 tenant

## Account

62984032838045582045

**Sign in**

NetApp support | NetApp.com



La pagina Sign in StorageGRID non viene visualizzata quando si immette l'URL completo per un account tenant (ovvero un nome di dominio completo o un indirizzo IP seguito da `?accountId=20-digit-account-id`). Invece, verrai immediatamente reindirizzato alla pagina di accesso SSO della tua organizzazione, dove potrai [accedi con le tue credenziali SSO](#).

2. Indica se desideri accedere al Grid Manager o al Tenant Manager:

- Per accedere a Grid Manager, lasciare vuoto il campo **ID account**, immettere **0** come ID account oppure selezionare **Grid Manager** se compare nell'elenco degli account recenti.
- Per accedere a Tenant Manager, immettere l'ID account del tenant a 20 cifre oppure selezionare un tenant per nome se compare nell'elenco degli account recenti.

3. Seleziona \* Sign in\*

StorageGRID ti reindirizza alla pagina di accesso SSO della tua organizzazione. Per esempio:

Sign in with your organizational account

someone@example.com

Password

**Sign in**

4. Sign in con le tue credenziali SSO.

Se le tue credenziali SSO sono corrette:

- a. Il provider di identità (IdP) fornisce una risposta di autenticazione a StorageGRID.
- b. StorageGRID convalida la risposta di autenticazione.
- c. Se la risposta è valida e si appartiene a un gruppo federato con autorizzazioni di accesso StorageGRID , si accede a Grid Manager o Tenant Manager, a seconda dell'account selezionato.



Se l'account di servizio non è accessibile, puoi comunque effettuare l'accesso, a patto che tu sia un utente esistente appartenente a un gruppo federato con autorizzazioni di accesso StorageGRID .

5. Facoltativamente, accedi ad altri nodi amministrativi oppure a Grid Manager o Tenant Manager, se disponi delle autorizzazioni adeguate.

Non è necessario reinserire le credenziali SSO.

#### Disconnettersi quando SSO è abilitato

Quando SSO è abilitato per StorageGRID, ciò che accade quando ci si disconnette dipende dall'account a cui si è effettuato l'accesso e da dove ci si disconnette.

#### Passi

1. Individua il link **Esci** nell'angolo in alto a destra dell'interfaccia utente.
2. Seleziona **Esci**.

Viene visualizzata la pagina Sign in a StorageGRID . Il menu a discesa **Account recenti** è stato aggiornato per includere **Grid Manager** o il nome del tenant, in modo da poter accedere più rapidamente a queste interfacce utente in futuro.

Se hai effettuato l'accesso a...	E ti disconnetti da...	Hai effettuato la disconnessione da...
Grid Manager su uno o più nodi amministrativi	Grid Manager su qualsiasi nodo di amministrazione	Grid Manager su tutti i nodi amministrativi  <b>Nota:</b> se si utilizza Azure per SSO, potrebbero essere necessari alcuni minuti per uscire da tutti i nodi amministrativi.
Tenant Manager su uno o più nodi amministrativi	Tenant Manager su qualsiasi nodo amministrativo	Tenant Manager su tutti i nodi amministrativi
Sia Grid Manager che Tenant Manager	Responsabile della griglia	Solo il Grid Manager. Per uscire dall'SSO è necessario anche disconnettersi da Tenant Manager.



La tabella riassume cosa succede quando ci si disconnette se si utilizza una singola sessione del browser. Se hai effettuato l'accesso a StorageGRID in più sessioni del browser, devi disconnetterti da tutte le sessioni del browser separatamente.

## Requisiti e considerazioni per l'accesso singolo

Prima di abilitare l'accesso Single Sign-On (SSO) per un sistema StorageGRID , esaminare i requisiti e le considerazioni.

### Requisiti del fornitore di identità

StorageGRID supporta i seguenti provider di identità SSO (IdP):

- Servizio federativo di Active Directory (AD FS)
- Azure Active Directory (Azure AD)
- PingFederate

È necessario configurare la federazione delle identità per il sistema StorageGRID prima di poter configurare un provider di identità SSO. Il tipo di servizio LDAP utilizzato per la federazione delle identità determina il tipo di SSO che è possibile implementare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Directory attiva	<ul style="list-style-type: none"><li>• Directory attiva</li><li>• Azzurro</li><li>• PingFederate</li></ul>
Azzurro	Azzurro

### Requisiti AD FS

È possibile utilizzare una qualsiasi delle seguenti versioni di AD FS:

- Windows Server 2022 ADFS
- Windows Server 2019 ADFS
- Windows Server 2016 ADFS



Windows Server 2016 dovrebbe utilizzare "[Aggiornamento KB3201845](#)" , o superiore.

### Requisiti aggiuntivi

- Sicurezza del livello di trasporto (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versione 3.5.1 o successiva

### Considerazioni per Azure

Se si utilizza Azure come tipo di SSO e gli utenti hanno nomi di entità utente che non utilizzano sAMAccountName come prefisso, potrebbero verificarsi problemi di accesso se StorageGRID perde la

connessione con il server LDAP. Per consentire agli utenti di accedere, è necessario ripristinare la connessione al server LDAP.

### Requisiti del certificato del server

Per impostazione predefinita, StorageGRID utilizza un certificato di interfaccia di gestione su ciascun nodo di amministrazione per proteggere l'accesso a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API. Quando si configurano trust di relying party (AD FS), applicazioni aziendali (Azure) o connessioni del provider di servizi (PingFederate) per StorageGRID, si utilizza il certificato del server come certificato di firma per le richieste StorageGRID .

Se non l'hai già fatto "[configurato un certificato personalizzato per l'interfaccia di gestione](#)" , dovresti farlo ora. Quando si installa un certificato server personalizzato, questo viene utilizzato per tutti i nodi amministrativi e può essere utilizzato in tutti i trust relying party StorageGRID , nelle applicazioni aziendali o nelle connessioni SP .

 Non è consigliabile utilizzare il certificato server predefinito di un nodo di amministrazione in un trust di relying party, in un'applicazione aziendale o in una connessione SP . Se il nodo fallisce e lo si ripristina, viene generato un nuovo certificato server predefinito. Prima di poter accedere al nodo recuperato, è necessario aggiornare il trust della relying party, l'applicazione aziendale o la connessione SP con il nuovo certificato.

È possibile accedere al certificato del server di un nodo di amministrazione effettuando l'accesso alla shell dei comandi del nodo e andando su `/var/local/mgmt-api` elenco. Un certificato server personalizzato è denominato `custom-server.crt` . Il certificato del server predefinito del nodo è denominato `server.crt` .

### Requisiti portuali

L'accesso Single Sign-On (SSO) non è disponibile sulle porte riservate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione tramite Single Sign-On, è necessario utilizzare la porta HTTPS predefinita (443). Vedere "[Controllare l'accesso al firewall esterno](#)" .

### Conferma che gli utenti federati possono accedere

Prima di abilitare l'accesso Single Sign-On (SSO), è necessario confermare che almeno un utente federato possa accedere a Grid Manager e a Tenant Manager per tutti gli account tenant esistenti.

#### Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .
- Hai già configurato la federazione delle identità.

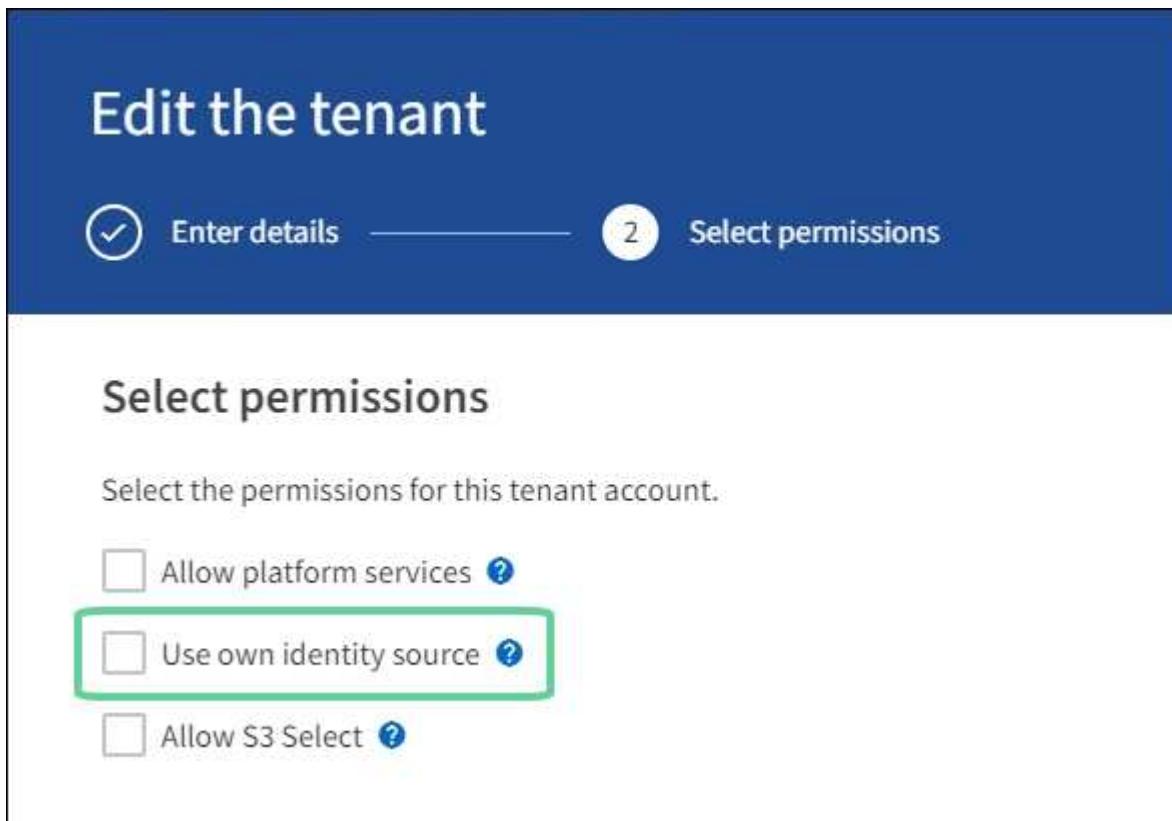
#### Passi

1. Se sono già presenti account tenant, verificare che nessuno dei tenant utilizzi la propria fonte di identità.



Quando si abilita SSO, un'origine identità configurata in Tenant Manager viene sostituita dall'origine identità configurata in Grid Manager. Gli utenti appartenenti all'origine identità del tenant non potranno più effettuare l'accesso a meno che non dispongano di un account con l'origine identità di Grid Manager.

- a. Sign in al Tenant Manager per ogni account tenant.
  - b. Selezionare **GESTIONE ACCESSI > Federazione identità**.
  - c. Verificare che la casella di controllo **Abilita federazione delle identità** non sia selezionata.
  - d. In tal caso, verificare che tutti i gruppi federati eventualmente utilizzati per questo account tenant non siano più necessari, deselectare la casella di controllo e selezionare **Salva**.
2. Verificare che un utente federato possa accedere a Grid Manager:
- a. Da Grid Manager, seleziona **CONFIGURAZIONE > Controllo accessi > Gruppi amministratori**.
  - b. Assicurarsi che almeno un gruppo federato sia stato importato dall'origine identità di Active Directory e che gli sia stata assegnata l'autorizzazione di accesso Root.
  - c. Disconnessione.
  - d. Conferma di poter accedere nuovamente a Grid Manager come utente del gruppo federato.
3. Se sono presenti account tenant, verificare che un utente federato con autorizzazione di accesso Root possa accedere:
- a. Da Grid Manager, seleziona **TENANTS**.
  - b. Selezionare l'account tenant e selezionare **Azioni > Modifica**.
  - c. Nella scheda Inserisci dettagli, seleziona **Continua**.
  - d. Se è selezionata la casella di controllo **Usa la propria fonte di identità**, deselectarla e selezionare **Salva**.



Viene visualizzata la pagina Inquilino.

- a. Selezionare l'account tenant, selezionare \* Sign in\* e accedere all'account tenant come utente root locale.

- b. Da Tenant Manager, seleziona **GESTIONE ACCESSI > Gruppi**.
- c. Assicurarsi che almeno a un gruppo federato di Grid Manager sia stata assegnata l'autorizzazione di accesso Root per questo tenant.
- d. Disconnessione.
- e. Conferma di poter accedere nuovamente al tenant come utente nel gruppo federato.

#### Informazioni correlate

- "[Requisiti e considerazioni per l'accesso singolo](#)"
- "[Gestisci gruppi di amministratori](#)"
- "[Utilizzare un account tenant](#)"

## Utilizza la modalità sandbox

È possibile utilizzare la modalità sandbox per configurare e testare l'accesso singolo (SSO) prima di abilitarlo per tutti gli utenti StorageGRID . Dopo aver abilitato l'SSO, puoi tornare alla modalità sandbox ogni volta che hai bisogno di modificare o testare nuovamente la configurazione.

#### Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Tu hai il "[Permesso di accesso root](#)" .
- Hai configurato la federazione delle identità per il tuo sistema StorageGRID .
- Per il tipo di servizio LDAP di federazione delle identità, hai selezionato Active Directory o Azure, in base al provider di identità SSO che intendi utilizzare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Directory attiva	<ul style="list-style-type: none"> <li>• Directory attiva</li> <li>• Azzurro</li> <li>• PingFederate</li> </ul>
Azzurro	Azzurro

#### Informazioni su questo compito

Quando l'SSO è abilitato e un utente tenta di accedere a un nodo di amministrazione, StorageGRID invia una richiesta di autenticazione al provider di identità SSO. A sua volta, il provider di identità SSO invia una risposta di autenticazione a StorageGRID, indicando se la richiesta di autenticazione è andata a buon fine. Per richieste andate a buon fine:

- La risposta da Active Directory o PingFederate include un identificatore univoco universale (UUID) per l'utente.
- La risposta di Azure include un nome dell'entità utente (UPN).

Per consentire a StorageGRID (il fornitore del servizio) e al provider di identità SSO di comunicare in modo sicuro sulle richieste di autenticazione degli utenti, è necessario configurare determinate impostazioni in StorageGRID. Successivamente, è necessario utilizzare il software del provider di identità SSO per creare un

trust della relying party (AD FS), un'applicazione aziendale (Azure) o un provider di servizi (PingFederate) per ciascun nodo di amministrazione. Infine, è necessario tornare a StorageGRID per abilitare SSO.

La modalità sandbox semplifica l'esecuzione di questa configurazione avanti e indietro e il test di tutte le impostazioni prima di abilitare l'SSO. Quando si utilizza la modalità sandbox, gli utenti non possono accedere tramite SSO.

## Accedi alla modalità sandbox

### Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.

Viene visualizzata la pagina Single Sign-on, con l'opzione **Disabilitato** selezionata.

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO status  Disabled  Sandbox Mode  Enabled

**Save**



Se le opzioni di stato SSO non vengono visualizzate, verificare di aver configurato il provider di identità come origine dell'identità federata. Vedere "[Requisiti e considerazioni per l'accesso singolo](#)".

2. Selezionare **Modalità Sandbox**.

Viene visualizzata la sezione Provider di identità.

## Inserisci i dettagli del provider di identità

### Passi

1. Selezionare il **tipo SSO** dall'elenco a discesa.
2. Compila i campi nella sezione Identity Provider in base al tipo di SSO selezionato.

## Directory attiva

- a. Immettere il **Nome del servizio federativo** per il provider di identità, esattamente come appare in Active Directory Federation Service (AD FS).



Per individuare il nome del servizio federativo, accedere a Windows Server Manager. Selezionare **Strumenti > Gestione AD FS**. Dal menu Azione, seleziona **Modifica proprietà del servizio federativo**. Nel secondo campo viene visualizzato il nome del servizio federativo.

- b. Specificare quale certificato TLS verrà utilizzato per proteggere la connessione quando il provider di identità invia informazioni di configurazione SSO in risposta alle richieste StorageGRID .

- **Utilizza il certificato CA del sistema operativo:** utilizza il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
- **Utilizza certificato CA personalizzato:** utilizza un certificato CA personalizzato per proteggere la connessione.

Se selezioni questa impostazione, copia il testo del certificato personalizzato e incollalo nella casella di testo **Certificato CA**.

- **Non utilizzare TLS:** non utilizzare un certificato TLS per proteggere la connessione.



Se si modifica il certificato CA, immediatamente "[riavviare il servizio mgmt-api sui nodi amministrativi](#)" e testare un SSO riuscito nel Grid Manager.

- c. Nella sezione Relying Party, specificare l'**identificatore del relying party** per StorageGRID. Questo valore controlla il nome utilizzato per ogni trust della relying party in AD FS.

- Ad esempio, se la tua griglia ha un solo nodo amministrativo e non prevedi di aggiungerne altri in futuro, inserisci SG O StorageGRID .
- Se la griglia include più di un nodo di amministrazione, includi la stringa [HOSTNAME] nell'identificatore. Ad esempio, SG- [HOSTNAME] . Viene generata una tabella che mostra l'identificatore della parte affidabile per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.



È necessario creare un trust della relying party per ciascun nodo amministrativo nel sistema StorageGRID . La presenza di un trust di parte affidabile per ogni nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- d. Seleziona **Salva**.

Per alcuni secondi sul pulsante **Salva** apparirà un segno di spunta verde.

**Save ✓**

## Azzurro

- a. Specificare quale certificato TLS verrà utilizzato per proteggere la connessione quando il provider di identità invia informazioni di configurazione SSO in risposta alle richieste StorageGRID .

- **Utilizza il certificato CA del sistema operativo:** utilizza il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
- **Utilizza certificato CA personalizzato:** utilizza un certificato CA personalizzato per proteggere la connessione.

Se selezioni questa impostazione, copia il testo del certificato personalizzato e incollalo nella casella di testo **Certificato CA**.

- **Non utilizzare TLS:** non utilizzare un certificato TLS per proteggere la connessione.



Se si modifica il certificato CA, immediatamente "[riavviare il servizio mgmt-api sui nodi amministrativi](#)" e testare un SSO riuscito nel Grid Manager.

- Nella sezione Applicazione aziendale, specificare il **Nome dell'applicazione aziendale** per StorageGRID. Questo valore controlla il nome utilizzato per ogni applicazione aziendale in Azure AD.

- Ad esempio, se la tua griglia ha un solo nodo amministrativo e non prevedi di aggiungerne altri in futuro, inserisci SG O StorageGRID .
- Se la griglia include più di un nodo di amministrazione, includi la stringa [HOSTNAME] nell'identificatore. Ad esempio, SG- [HOSTNAME] . Viene generata una tabella che mostra il nome dell'applicazione aziendale per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.



È necessario creare un'applicazione aziendale per ciascun nodo amministrativo nel sistema StorageGRID . Disporre di un'applicazione aziendale per ciascun nodo amministrativo garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo amministrativo.

- Segui i passaggi in "[Crea applicazioni aziendali in Azure AD](#)" per creare un'applicazione aziendale per ogni nodo amministrativo elencato nella tabella.
- Da Azure AD, copiare l'URL dei metadati della federazione per ogni applicazione aziendale. Quindi, incolla questo URL nel campo **URL metadati federazione** corrispondente in StorageGRID.
- Dopo aver copiato e incollato un URL dei metadati di federazione per tutti i nodi amministrativi, seleziona **Salva**.

Per alcuni secondi sul pulsante **Salva** apparirà un segno di spunta verde.

**Save ✓**

### PingFederate

- Specificare quale certificato TLS verrà utilizzato per proteggere la connessione quando il provider di identità invia informazioni di configurazione SSO in risposta alle richieste StorageGRID .
  - **Utilizza il certificato CA del sistema operativo:** utilizza il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
  - **Utilizza certificato CA personalizzato:** utilizza un certificato CA personalizzato per proteggere la connessione.

Se selezioni questa impostazione, copia il testo del certificato personalizzato e incollalo nella casella di testo **Certificato CA**.

- **Non utilizzare TLS:** non utilizzare un certificato TLS per proteggere la connessione.



Se si modifica il certificato CA, immediatamente "[riavviare il servizio mgmt-api sui nodi amministrativi](#)" e testare un SSO riuscito nel Grid Manager.

- Nella sezione Fornitore di servizi (SP), specificare l'ID di connessione SP per StorageGRID. Questo valore controlla il nome utilizzato per ogni connessione SP in PingFederate.

- Ad esempio, se la tua griglia ha un solo nodo amministrativo e non prevedi di aggiungerne altri in futuro, inserisci SG O StorageGRID .
- Se la griglia include più di un nodo di amministrazione, includi la stringa [HOSTNAME] nell'identificatore. Ad esempio, SG- [HOSTNAME] . Viene generata una tabella che mostra l'ID di connessione SP per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.



È necessario creare una connessione SP per ciascun nodo amministrativo nel sistema StorageGRID . Disporre di una connessione SP per ciascun nodo amministrativo garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo amministrativo.

- Specificare l'URL dei metadati della federazione per ciascun nodo di amministrazione nel campo **URL dei metadati della federazione**.

Utilizzare il seguente formato:

```
https://<Federation Service Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection ID>
```

- Selezione **Salva**.

Per alcuni secondi sul pulsante **Salva** apparirà un segno di spunta verde.

**Save** ✓

## Configurare trust di relying party, applicazioni aziendali o connessioni SP

Una volta salvata la configurazione, viene visualizzato l'avviso di conferma della modalità Sandbox. Questa nota conferma che la modalità sandbox è ora abilitata e fornisce istruzioni generali.

StorageGRID può rimanere in modalità sandbox per tutto il tempo necessario. Tuttavia, quando nella pagina Single Sign-on è selezionata la **Modalità Sandbox**, l'SSO è disabilitato per tutti gli utenti StorageGRID . Possono effettuare l'accesso solo gli utenti locali.

Seguire questi passaggi per configurare trust di relying party (Active Directory), completare applicazioni

aziendali (Azure) o configurare connessioni SP (PingFederate).

## Directory attiva

### Passi

1. Vai ad Active Directory Federation Services (AD FS).
2. Creare uno o più trust di relying party per StorageGRID, utilizzando ciascun identificatore di relying party mostrato nella tabella nella pagina Single Sign-on StorageGRID .

È necessario creare un trust per ogni nodo amministrativo mostrato nella tabella.

Per le istruzioni, vai a "[Creare trust di relying party in AD FS](#)" .

## Azzurro

### Passi

1. Dalla pagina Single Sign-On per il nodo di amministrazione a cui hai effettuato l'accesso, seleziona il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi amministrativi nella griglia, ripeti questi passaggi:
  - a. Sign in al nodo.
  - b. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
  - c. Scarica e salva i metadati SAML per quel nodo.
3. Vai al portale di Azure.
4. Segui i passaggi in "[Crea applicazioni aziendali in Azure AD](#)" per caricare il file di metadati SAML per ciascun nodo di amministrazione nella corrispondente applicazione aziendale di Azure.

## PingFederate

### Passi

1. Dalla pagina Single Sign-On per il nodo di amministrazione a cui hai effettuato l'accesso, seleziona il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi amministrativi nella griglia, ripeti questi passaggi:
  - a. Sign in al nodo.
  - b. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
  - c. Scarica e salva i metadati SAML per quel nodo.
3. Vai su PingFederate.
4. "[Creare una o più connessioni al fornitore di servizi \(SP\) per StorageGRID](#)" . Utilizzare l'ID di connessione SP per ciascun nodo amministrativo (mostrato nella tabella nella pagina StorageGRID Single Sign-on) e i metadati SAML scaricati per tale nodo amministrativo.

È necessario creare una connessione SP per ogni nodo amministrativo mostrato nella tabella.

## Test delle connessioni SSO

Prima di imporre l'uso dell'accesso singolo per l'intero sistema StorageGRID , è necessario verificare che l'accesso singolo e la disconnessione singola siano configurati correttamente per ciascun nodo di amministrazione.

## Directory attiva

### Passi

- Nella pagina StorageGRID Single Sign-on, individuare il collegamento nel messaggio della modalità Sandbox.

L'URL deriva dal valore immesso nel campo **Nome del servizio federativo**.

**Sandbox mode**

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

- Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
- Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
- From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

- Seleziona il collegamento oppure copia e incolla l'URL in un browser per accedere alla pagina di accesso del tuo provider di identità.
- Per confermare di poter utilizzare SSO per accedere a StorageGRID, seleziona \* Sign in a uno dei seguenti siti\*, seleziona l'identificativo della parte affidabile per il tuo nodo di amministrazione primario e seleziona \* Sign in\*.

You are not signed in.

Sign in to this site.  
 Sign in to one of the following sites:  
SG-DC1-ADM1

Sign in

- Inserisci il tuo nome utente e la tua password federati.

- Se le operazioni di accesso e disconnessione SSO vanno a buon fine, viene visualizzato un messaggio di conferma.

✓ Single sign-on authentication and logout test completed successfully.

- Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risovi il problema, cancella i cookie del browser e riprova.

- Ripetere questi passaggi per verificare la connessione SSO per ciascun nodo amministrativo nella

griglia.

## Azzurro

### Passi

1. Vai alla pagina Single Sign-On nel portale di Azure.
2. Seleziona **Prova questa applicazione**.
3. Inserisci le credenziali di un utente federato.
  - Se le operazioni di accesso e disconnessione SSO vanno a buon fine, viene visualizzato un messaggio di conferma.

 Single sign-on authentication and logout test completed successfully.

- Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risovi il problema, cancella i cookie del browser e riprova.
4. Ripetere questi passaggi per verificare la connessione SSO per ciascun nodo amministrativo nella griglia.

## PingFederate

### Passi

1. Dalla pagina StorageGRID Single Sign-on, selezionare il primo collegamento nel messaggio della modalità Sandbox.

Seleziona e testa un collegamento alla volta.

**Sandbox mode**

Sandbox mode is currently enabled. Use this mode to configure service provider (SP) connections and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
  - [https://\[REDACTED\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[REDACTED]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
  - [https://\[REDACTED\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[REDACTED]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

2. Inserisci le credenziali di un utente federato.

- Se le operazioni di accesso e disconnessione SSO vanno a buon fine, viene visualizzato un messaggio di conferma.

 Single sign-on authentication and logout test completed successfully.

- Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risovi il problema, cancella i cookie del browser e riprova.
3. Seleziona il collegamento successivo per verificare la connessione SSO per ciascun nodo di amministrazione nella tua griglia.

Se vedi un messaggio di pagina scaduta, seleziona il pulsante **Indietro** nel tuo browser e invia nuovamente le tue credenziali.

## Abilita l'accesso singolo

Dopo aver confermato di poter utilizzare SSO per accedere a ciascun nodo di amministrazione, puoi abilitare SSO per l'intero sistema StorageGRID .



Quando SSO è abilitato, tutti gli utenti devono utilizzare SSO per accedere a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API. Gli utenti locali non possono più accedere a StorageGRID.

### Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
2. Modificare lo stato SSO in **Abilitato**.
3. Seleziona **Salva**.
4. Rivedere il messaggio di avviso e selezionare **OK**.

Ora è abilitato l'accesso singolo.



Se si utilizza il portale di Azure e si accede a StorageGRID dallo stesso computer utilizzato per accedere ad Azure, assicurarsi che l'utente del portale di Azure sia anche un utente StorageGRID autorizzato (un utente in un gruppo federato importato in StorageGRID) oppure disconnettersi dal portale di Azure prima di tentare di accedere a StorageGRID.

## Creare trust di relying party in AD FS

È necessario utilizzare Active Directory Federation Services (AD FS) per creare un trust della relying party per ogni nodo amministrativo nel sistema. È possibile creare trust di relying party utilizzando i comandi di PowerShell, importando metadati SAML da StorageGRID o immettendo i dati manualmente.

### Prima di iniziare

- Hai configurato l'accesso Single Sign-On per StorageGRID e hai selezionato **AD FS** come tipo di SSO.
- La **modalità sandbox** è selezionata nella pagina Single sign-on in Grid Manager. Vedere "[Utilizza la modalità sandbox](#)" .
- Conosci il nome di dominio completo (o l'indirizzo IP) e l'identificativo della parte affidabile per ciascun nodo di amministrazione nel tuo sistema. È possibile trovare questi valori nella tabella dei dettagli dei nodi di amministrazione nella pagina StorageGRID Single Sign-on.



È necessario creare un trust della relying party per ciascun nodo amministrativo nel sistema StorageGRID . La presenza di un trust di parte affidabile per ogni nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Hai esperienza nella creazione di trust relying party in AD FS oppure hai accesso alla documentazione di Microsoft AD FS.

- Stai utilizzando lo snap-in Gestione AD FS e appartieni al gruppo Amministratori.
- Se si crea manualmente il trust della relying party, si dispone del certificato personalizzato caricato per l'interfaccia di gestione StorageGRID oppure si sa come accedere a un nodo di amministrazione dalla shell dei comandi.

## Informazioni su questo compito

Queste istruzioni si applicano a Windows Server 2016 AD FS. Se si utilizza una versione diversa di AD FS, si noteranno lievi differenze nella procedura. Per qualsiasi domanda, consultare la documentazione di Microsoft AD FS.

### Creare un trust della relying party utilizzando Windows PowerShell

È possibile utilizzare Windows PowerShell per creare rapidamente uno o più trust relying party.

#### Passi

1. Dal menu Start di Windows, seleziona con il pulsante destro del mouse l'icona di PowerShell e seleziona **Esegui come amministratore**.
2. Al prompt dei comandi di PowerShell, immettere il seguente comando:

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifier" -MetadataURL  
"https://Admin_Node_FQDN/api/saml-metadata"
```

- Per *Admin\_Node\_Identifier*, immettere l'identificatore della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on. Ad esempio, SG-DC1-ADM1 .
- Per *Admin\_Node\_FQDN*, immettere il nome di dominio completo per lo stesso nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

3. Da Windows Server Manager, selezionare **Strumenti > Gestione AD FS**.

Viene visualizzato lo strumento di gestione AD FS.

4. Selezionare **AD FS > Trust delle parti affidabili**.

Viene visualizzato l'elenco dei trust delle parti affidanti.

5. Aggiungere una policy di controllo degli accessi al trust della relying party appena creato:

- a. Individua il trust della parte affidabile che hai appena creato.
- b. Fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica criterio di controllo degli accessi**.
- c. Selezionare una politica di controllo degli accessi.
- d. Selezionare **Applica** e selezionare **OK**

6. Aggiungere una politica di emissione dei reclami al trust della parte affidabile appena creato:

- a. Individua il trust della parte affidabile che hai appena creato.
- b. Fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica policy di emissione reclami**.
- c. Seleziona **Aggiungi regola**.
- d. Nella pagina Selezione modello di regola, seleziona **Invia attributi LDAP come claim** dall'elenco e

seleziona **Avanti**.

- e. Nella pagina Configura regola, immettere un nome visualizzato per questa regola.

Ad esempio, **ObjectGUID in Name ID o UPN in Name ID**.

- f. Per l'Attribute Store, selezionare **Active Directory**.
- g. Nella colonna Attributo LDAP della tabella Mapping, digitare **objectGUID** oppure selezionare **User-Principal-Name**.
- h. Nella colonna Tipo di richiesta in uscita della tabella Mapping, selezionare **ID nome** dall'elenco a discesa.
- i. Selezionare **Fine** e quindi **OK**.

7. Verificare che i metadati siano stati importati correttamente.

- a. Fare clic con il pulsante destro del mouse sul trust della relying party per aprirne le proprietà.
- b. Verificare che i campi nelle schede **Endpoint**, **Identificatori** e **Firma** siano compilati.

Se i metadati sono mancanti, verificare che l'indirizzo dei metadati della Federazione sia corretto oppure immettere i valori manualmente.

8. Ripetere questi passaggi per configurare un trust della relying party per tutti i nodi amministrativi nel sistema StorageGRID .
9. Al termine, torna a StorageGRID e verifica tutti i trust delle relying party per confermare che siano configurati correttamente. Vedere "[Utilizzare la modalità Sandbox](#)" per istruzioni.

### **Creare un trust della parte affidabile importando i metadati della federazione**

È possibile importare i valori per ciascun trust della relying party accedendo ai metadati SAML per ciascun nodo di amministrazione.

#### **Passi**

1. In Windows Server Manager, seleziona **Strumenti**, quindi seleziona **Gestione AD FS**.
2. In Azioni, seleziona **Aggiungi trust della parte affidabile**.
3. Nella pagina di benvenuto, seleziona **Richiedi informazioni** e seleziona **Avvia**.
4. Selezionare **Importa dati sulla parte affidabile pubblicati online o su una rete locale**.
5. In **Indirizzo metadati federazione (nome host o URL)**, digitare la posizione dei metadati SAML per questo nodo di amministrazione:

`https://Admin_Node_FQDN/api/saml-metadata`

Per `Admin_Node_FQDN`, immettere il nome di dominio completo per lo stesso nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

6. Completare la procedura guidata Trust della parte affidabile, salvare il trust della parte affidabile e chiudere la procedura guidata.



Quando si immette il nome visualizzato, utilizzare l'identificatore della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, SG-DC1-ADM1 .

7. Aggiungi una regola di rivendicazione:
  - a. Fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica policy di emissione reclami**.
  - b. Seleziona **Aggiungi regola**:
  - c. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come claim** dall'elenco e seleziona **Avanti**.
  - d. Nella pagina Configura regola, immettere un nome visualizzato per questa regola.  
Ad esempio, **ObjectGUID in Name ID** o **UPN in Name ID**.
  - e. Per l'Attribute Store, selezionare **Active Directory**.
  - f. Nella colonna Attributo LDAP della tabella Mapping, digitare **objectGUID** oppure selezionare **User-Principal-Name**.
  - g. Nella colonna Tipo di richiesta in uscita della tabella Mapping, selezionare **ID nome** dall'elenco a discesa.
  - h. Selezionare **Fine** e quindi **OK**.
8. Verificare che i metadati siano stati importati correttamente.
  - a. Fare clic con il pulsante destro del mouse sul trust della relying party per aprirne le proprietà.
  - b. Verificare che i campi nelle schede **Endpoint**, **Identificatori** e **Firma** siano compilati.  
Se i metadati sono mancanti, verificare che l'indirizzo dei metadati della Federazione sia corretto oppure immettere i valori manualmente.
9. Ripetere questi passaggi per configurare un trust della relying party per tutti i nodi amministrativi nel sistema StorageGRID .
10. Al termine, torna a StorageGRID e verifica tutti i trust delle relying party per confermare che siano configurati correttamente. Vedere "[Utilizzare la modalità Sandbox](#)" per istruzioni.

### Creare manualmente un trust della parte affidabile

Se si sceglie di non importare i dati per i trust delle parti affidabili, è possibile immettere i valori manualmente.

#### Passi

1. In Windows Server Manager, seleziona **Strumenti**, quindi seleziona **Gestione AD FS**.
2. In Azioni, seleziona **Aggiungi trust della parte affidabile**.
3. Nella pagina di benvenuto, seleziona **Richiedi informazioni** e seleziona **Avvia**.
4. Selezionare **Inserisci manualmente i dati sulla parte affidabile** e selezionare **Avanti**.
5. Completare la procedura guidata Trust della parte affidabile:
  - a. Inserisci un nome visualizzato per questo nodo di amministrazione.

Per coerenza, utilizzare l'identificatore della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, SG-DC1-ADM1 .

- b. Salta il passaggio per configurare un certificato di crittografia token facoltativo.
- c. Nella pagina Configura URL, seleziona la casella di controllo **Abilita supporto per il protocollo SAML 2.0 WebSSO**.
- d. Digitare l'URL dell'endpoint del servizio SAML per il nodo di amministrazione:

`https://Admin_Node_FQDN/api/saml-response`

Per `Admin_Node_FQDN`, immettere il nome di dominio completo per il nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

- e. Nella pagina Configura identificatori, specificare l'identificatore della parte affidabile per lo stesso nodo di amministrazione:

`Admin_Node_Identifier`

Per `Admin_Node_Identifier`, immettere l'identificatore della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on. Ad esempio, SG-DC1-ADM1 .

- f. Rivedere le impostazioni, salvare il trust della relying party e chiudere la procedura guidata.

Venne visualizzata la finestra di dialogo Modifica policy di emissione reclami.



Se la finestra di dialogo non viene visualizzata, fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica policy di emissione reclami**.

6. Per avviare la procedura guidata Claim Rules, seleziona **Aggiungi regola**:
  - a. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come claim** dall'elenco e seleziona **Avanti**.
  - b. Nella pagina Configura regola, immettere un nome visualizzato per questa regola.  
Ad esempio, **ObjectGUID in Name ID o UPN in Name ID**.
  - c. Per l'Attribute Store, selezionare **Active Directory**.
  - d. Nella colonna Attributo LDAP della tabella Mapping, digitare **objectGUID** oppure selezionare **User-Principal-Name**.
  - e. Nella colonna Tipo di richiesta in uscita della tabella Mapping, selezionare **ID nome** dall'elenco a discesa.
  - f. Selezionare **Fine** e quindi **OK**.
7. Fare clic con il pulsante destro del mouse sul trust della relying party per aprirne le proprietà.
8. Nella scheda **Endpoint**, configurare l'endpoint per la disconnessione singola (SLO):
  - a. Selezionare **Aggiungi SAML**.
  - b. Selezionare **Tipo di endpoint > Disconnessione SAML**.
  - c. Selezionare **Associa > Reindirizza**.
  - d. Nel campo **URL attendibile**, immettere l'URL utilizzato per la disconnessione singola (SLO) da questo nodo di amministrazione:

[https://Admin\\_Node\\_FQDN/api/saml-logout](https://Admin_Node_FQDN/api/saml-logout)

Per *Admin\_Node\_FQDN*, immettere il nome di dominio completo del nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

a. Selezionare **OK**.

9. Nella scheda **Firma**, specificare il certificato di firma per questo trust della parte affidabile:

a. Aggiungi il certificato personalizzato:

- Se disponi del certificato di gestione personalizzato caricato su StorageGRID, seleziona tale certificato.
- Se non si dispone del certificato personalizzato, accedere al nodo di amministrazione, andare su /var/local/mgmt-api directory del nodo di amministrazione e aggiungere il custom-server.crt file del certificato.



Utilizzo del certificato predefinito del nodo di amministrazione(server.crt) non è raccomandato. Se il nodo di amministrazione non funziona, il certificato predefinito verrà rigenerato quando si ripristina il nodo e sarà necessario aggiornare il trust della parte affidabile.

b. Selezionare **Applica** e quindi **OK**.

Le proprietà del relying party vengono salvate e chiuse.

10. Ripetere questi passaggi per configurare un trust della relying party per tutti i nodi amministrativi nel sistema StorageGRID .

11. Al termine, torna a StorageGRID e verifica tutti i trust delle relying party per confermare che siano configurati correttamente. Vedere "[Utilizza la modalità sandbox](#)" per istruzioni.

## Crea applicazioni aziendali in Azure AD

Puoi utilizzare Azure AD per creare un'applicazione aziendale per ogni nodo di amministrazione del tuo sistema.

### Prima di iniziare

- Hai iniziato a configurare l'accesso Single Sign-On per StorageGRID e hai selezionato **Azure** come tipo di SSO.
- La **modalità sandbox** è selezionata nella pagina Single sign-on in Grid Manager. Vedere "[Utilizza la modalità sandbox](#)" .
- Per ogni nodo amministrativo del sistema è disponibile il **nome dell'applicazione aziendale**. È possibile copiare questi valori dalla tabella dei dettagli del nodo di amministrazione nella pagina Single Sign-on StorageGRID .



È necessario creare un'applicazione aziendale per ciascun nodo amministrativo nel sistema StorageGRID . Disporre di un'applicazione aziendale per ciascun nodo amministrativo garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo amministrativo.

- Hai esperienza nella creazione di applicazioni aziendali in Azure Active Directory.
- Hai un account Azure con una sottoscrizione attiva.
- Nell'account Azure ricopri uno dei seguenti ruoli: amministratore globale, amministratore dell'applicazione cloud, amministratore dell'applicazione o proprietario dell'entità servizio.

## Accedi ad Azure AD

### Passi

1. Accedi al "[Portale di Azure](#)" .
2. Vai a "[Azure Active Directory](#)" .
3. Selezionare "[Applicazioni aziendali](#)" .

## Crea applicazioni aziendali e salva la configurazione StorageGRID SSO

Per salvare la configurazione SSO per Azure in StorageGRID, è necessario utilizzare Azure per creare un'applicazione aziendale per ciascun nodo di amministrazione. Copiare gli URL dei metadati della federazione da Azure e incollarli nei campi **URL metadati della federazione** corrispondenti nella pagina Single Sign-on di StorageGRID .

### Passi

1. Ripetere i seguenti passaggi per ciascun nodo di amministrazione.
  - a. Nel riquadro Applicazioni aziendali di Azure, seleziona **Nuova applicazione**.
  - b. Seleziona **Crea la tua applicazione**.
  - c. Per il nome, immettere il **Nome dell'applicazione aziendale** copiato dalla tabella dei dettagli del nodo di amministrazione nella pagina Single Sign-on StorageGRID .
  - d. Lascia selezionato il pulsante di opzione **Integra qualsiasi altra applicazione non presente nella galleria (Non nella galleria)**.
  - e. Seleziona **Crea**.
  - f. Selezionare il link **Inizia** nel **2. Impostare la casella Single Sign-On** oppure selezionare il collegamento **Single Sign-On** sul margine sinistro.
  - g. Selezionare la casella **SAML**.
  - h. Copia l'**URL dei metadati della federazione app**, che puoi trovare in **Certificato di firma SAML del passaggio 3**.
    - i. Vai alla pagina StorageGRID Single Sign-on e incolla l'URL nel campo **URL metadati federazione** che corrisponde al **Nome applicazione aziendale** utilizzato.
2. Dopo aver incollato un URL dei metadati di federazione per ciascun nodo di amministrazione e aver apportato tutte le altre modifiche necessarie alla configurazione SSO, selezionare **Salva** nella pagina StorageGRID Single Sign-on.

## Scarica i metadati SAML per ogni nodo amministrativo

Dopo aver salvato la configurazione SSO, puoi scaricare un file di metadati SAML per ogni nodo amministrativo nel tuo sistema StorageGRID .

### Passi

1. Ripetere questi passaggi per ogni nodo di amministrazione.

- a. Sign in a StorageGRID dal nodo di amministrazione.
- b. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.
- c. Selezionare il pulsante per scaricare i metadati SAML per quel nodo di amministrazione.
- d. Salva il file che caricherai in Azure AD.

## Carica i metadati SAML in ogni applicazione aziendale

Dopo aver scaricato un file di metadati SAML per ogni nodo di amministrazione StorageGRID , eseguire i seguenti passaggi in Azure AD:

### Passi

1. Torna al portale di Azure.
2. Ripetere questi passaggi per ogni applicazione aziendale:



Potrebbe essere necessario aggiornare la pagina Applicazioni aziendali per visualizzare le applicazioni aggiunte in precedenza all'elenco.

- a. Vai alla pagina Proprietà dell'applicazione aziendale.
- b. Impostare **Assegnazione richiesta** su **No** (a meno che non si desideri configurare separatamente le assegnazioni).
- c. Vai alla pagina Single Sign-On.
- d. Completare la configurazione SAML.
- e. Selezionare il pulsante **Carica file metadati** e selezionare il file metadati SAML scaricato per il nodo di amministrazione corrispondente.
- f. Dopo aver caricato il file, seleziona **Salva** e poi **X** per chiudere il riquadro. Verrai reindirizzato alla pagina Imposta Single Sign-On con SAML.
3. Segui i passaggi in "[Utilizza la modalità sandbox](#)" per testare ogni applicazione.

## Crea connessioni al fornitore di servizi (SP) in PingFederate

Puoi utilizzare PingFederate per creare una connessione al provider di servizi (SP) per ogni nodo amministrativo del tuo sistema. Per velocizzare il processo, importerai i metadati SAML da StorageGRID.

### Prima di iniziare

- Hai configurato l'accesso Single Sign-On per StorageGRID e hai selezionato **Ping Federate** come tipo di SSO.
- La **modalità sandbox** è selezionata nella pagina Single sign-on in Grid Manager. Vedere "[Utilizza la modalità sandbox](#)".
- Hai l'\*ID di connessione SP \* per ogni nodo amministrativo nel tuo sistema. È possibile trovare questi valori nella tabella dei dettagli dei nodi di amministrazione nella pagina StorageGRID Single Sign-on.
- Hai scaricato i **metadati SAML** per ogni nodo amministrativo nel tuo sistema.
- Hai esperienza nella creazione di connessioni SP in PingFederate Server.
- Tu hai [ilhttps://docs.pingidentity.com/pingfederate/latest/administrators\\_reference\\_guide/pf\\_administrators\\_reference\\_guide.html](https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html)["Guida di riferimento dell'amministratore"] per PingFederate Server. La documentazione

di PingFederate fornisce istruzioni e spiegazioni dettagliate passo dopo passo.

- Tu hai il "[Autorizzazione di amministratore](#)" per PingFederate Server.

## Informazioni su questo compito

Queste istruzioni riepilogano come configurare PingFederate Server versione 10.3 come provider SSO per StorageGRID. Se si utilizza un'altra versione di PingFederate, potrebbe essere necessario adattare queste istruzioni. Per istruzioni dettagliate sulla tua versione, consulta la documentazione di PingFederate Server.

## Prerequisiti completi in PingFederate

Prima di poter creare le connessioni SP che utilizzerai per StorageGRID, devi completare le attività preliminari in PingFederate. Le informazioni ricavate da questi prerequisiti verranno utilizzate durante la configurazione delle connessioni SP .

### Crea archivio dati

Se non lo hai già fatto, crea un archivio dati per connettere PingFederate al server LDAP di AD FS. Utilizza i valori che hai utilizzato quando "[configurazione della federazione delle identità](#)" in StorageGRID.

- **Tipo:** Directory (LDAP)
- **Tipo LDAP:** Active Directory
- **Nome attributo binario:** immettere **objectGUID** nella scheda Attributi binari LDAP esattamente come mostrato.

### Crea un validatore di credenziali password

Se non l'hai già fatto, crea un validatore di credenziali password.

- **Tipo:** Nome utente LDAP Password Validatore credenziali
- **Archivio dati:** seleziona l'archivio dati che hai creato.
- **Base di ricerca:** immettere le informazioni da LDAP (ad esempio, DC=saml,DC=sgws).
- **Filtro di ricerca:** sAMAccountName=\${username}
- **Ambito:** Sottoalbero

### Crea istanza dell'adattatore IdP

Se non l'hai già fatto, crea un'istanza dell'adattatore IdP.

### Passi

1. Vai su **Autenticazione > Integrazione > Schede IdP**.
2. Selezionare **Crea nuova istanza**.
3. Nella scheda **Tipo**, seleziona **Adattatore IdP modulo HTML**.
4. Nella scheda **IdP Adapter**, seleziona **Aggiungi una nuova riga a 'Validatori di credenziali'**.
5. Seleziona il [validatore di credenziali password](#) che hai creato.
6. Nella scheda **Attributi adattatore**, selezionare l'attributo **username** per **Pseudonimo**.
7. Seleziona **Salva**.

## Crea o importa il certificato di firma

Se non l'hai già fatto, crea o importa il certificato di firma.

### Passi

1. Vai a **Sicurezza > Chiavi e certificati di firma e decrittazione**.
2. Creare o importare il certificato di firma.

## Crea una connessione SP in PingFederate

Quando si crea una connessione SP in PingFederate, si importano i metadati SAML scaricati da StorageGRID per il nodo di amministrazione. Il file di metadati contiene molti dei valori specifici di cui hai bisogno.



È necessario creare una connessione SP per ciascun nodo di amministrazione nel sistema StorageGRID , in modo che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo. Utilizzare queste istruzioni per creare la prima connessione SP . Poi vai a [Crea connessioni SP aggiuntive](#) per creare eventuali connessioni aggiuntive di cui hai bisogno.

### Scegli il tipo di connessione SP

### Passi

1. Vai su **Applicazioni > Integrazione > \*Connessioni SP \***.
2. Seleziona **Crea connessione**.
3. Seleziona **Non utilizzare un modello per questa connessione**.
4. Selezionare **Profilo SSO del browser** e **SAML 2.0** come protocollo.

## Importa metadati SP

### Passi

1. Nella scheda Importa metadati, seleziona **File**.
2. Seleziona il file di metadati SAML scaricato dalla pagina Single Sign-On StorageGRID per il nodo di amministrazione.
3. Esaminare il Riepilogo dei metadati e le informazioni fornite nella scheda Informazioni generali.

L'ID entità del partner e il nome della connessione sono impostati sull'ID di connessione StorageGRID SP . (ad esempio, 10.96.105.200-DC1-ADM1-105-200). L'URL di base è l'IP del nodo di amministrazione StorageGRID .

4. Selezionare **Avanti**.

## Configurare l'SSO del browser IdP

### Passi

1. Dalla scheda Browser SSO, seleziona **Configura Browser SSO**.
2. Nella scheda Profili SAML, seleziona le opzioni \* SP-initiated SSO\*, \* SP-initial SLO\*, **IdP-initiated SSO** e **IdP-initiated SLO**.
3. Selezionare **Avanti**.
4. Nella scheda Durata asserzione, non apportare modifiche.
5. Nella scheda Creazione asserzione, selezionare **Configura creazione asserzione**.

- a. Nella scheda Mappatura identità, selezionare **Standard**.
- b. Nella scheda Contratto attributo, utilizzare **SAML\_SUBJECT** come Contratto attributo e il formato del nome non specificato che è stato importato.
6. Per estendere il contratto, selezionare **Elimina** per rimuovere il `urn:oid`, che non viene utilizzato.

#### Istanza dell'adattatore della mappa

##### Passi

1. Nella scheda Mapping origine autenticazione, selezionare **Mappa nuova istanza adattatore**.
2. Nella scheda Istanza adattatore, selezionare [istanza dell'adattatore](#) che hai creato.
3. Nella scheda Metodo di mappatura, seleziona **Recupera attributi aggiuntivi da un archivio dati**.
4. Nella scheda Origine attributo e ricerca utente, seleziona **Aggiungi origine attributo**.
5. Nella scheda Archivio dati, fornire una descrizione e selezionare [archivio dati](#) hai aggiunto.
6. Nella scheda Ricerca directory LDAP:
  - Immettere il **DN di base**, che deve corrispondere esattamente al valore immesso in StorageGRID per il server LDAP.
  - Per l'ambito di ricerca, selezionare **Sottoalbero**.
  - Per la classe dell'oggetto radice, cercare e aggiungere uno di questi attributi: **objectGUID** o **userPrincipalName**.
7. Nella scheda Tipi di codifica degli attributi binari LDAP, selezionare **Base64** per l'attributo **objectGUID**.
8. Nella scheda Filtro LDAP, immettere **sAMAccountName=\${username}**.
9. Nella scheda Adempimento contratto attributi, seleziona **LDAP (attributo)** dal menu a discesa Origine e seleziona **objectGUID** o **userPrincipalName** dal menu a discesa Valore.
10. Rivedere e quindi salvare la fonte dell'attributo.
11. Nella scheda Failsave Attribute Source, seleziona **Abort the SSO Transaction**.
12. Rivedi il riepilogo e seleziona **Fine**.
13. Selezionare **Fatto**.

#### Configurare le impostazioni del protocollo

##### Passi

1. Nella scheda **Connessione SP \* > \*SSO browser > Impostazioni protocollo**, selezionare **Configura impostazioni protocollo**.
2. Nella scheda URL del servizio consumer di asserzione, accettare i valori predefiniti, che sono stati importati dai metadati SAML StorageGRID (**POST** per Binding e `/api/saml-response` per l'URL dell'endpoint).
3. Nella scheda URL del servizio SLO, accettare i valori predefiniti, che sono stati importati dai metadati SAML StorageGRID (**REDIRECT** per Binding e `/api/saml-logout` per l'URL dell'endpoint).
4. Nella scheda Binding SAML consentiti, deselectare **ARTIFACT** e **SOAP**. Sono richiesti solo **POST** e **REDIRECT**.
5. Nella scheda Criterio di firma, lasciare selezionate le caselle di controllo **Richiedi la firma delle richieste di autorizzazione** e **Firma sempre l'asserzione**.
6. Nella scheda Criterio di crittografia, selezionare **Nessuno**.

7. Rivedi il riepilogo e seleziona **Fine** per salvare le impostazioni del protocollo.
8. Rivedi il riepilogo e seleziona **Fine** per salvare le impostazioni SSO del browser.

## Configurare le credenziali

### Passi

1. Dalla scheda Connessione SP , seleziona **Credenziali**.
2. Dalla scheda Credenziali, seleziona **Configura credenziali**.
3. Seleziona il [certificato di firma](#) che hai creato o importato.
4. Selezionare **Avanti** per andare a **Gestisci impostazioni di verifica della firma**.
  - a. Nella scheda Modello di fiducia, seleziona **Non ancorato**.
  - b. Nella scheda Certificato di verifica della firma, rivedere le informazioni sul certificato di firma, importate dai metadati SAML StorageGRID .
5. Rivedere le schermate di riepilogo e selezionare **Salva** per salvare la connessione SP .

## Crea connessioni SP aggiuntive

Puoi copiare la prima connessione SP per creare le connessioni SP necessarie per ogni nodo amministrativo nella tua griglia. Carichi nuovi metadati per ogni copia.



Le connessioni SP per diversi nodi amministrativi utilizzano impostazioni identiche, ad eccezione dell'ID entità del partner, dell'URL di base, dell'ID connessione, del nome della connessione, della verifica della firma e dell'URL di risposta SLO.

### Passi

1. Selezionare **Azione > Copia** per creare una copia della connessione SP iniziale per ogni nodo amministrativo aggiuntivo.
2. Inserisci l'ID connessione e il Nome connessione per la copia e seleziona **Salva**.
3. Selezionare il file di metadati corrispondente al nodo di amministrazione:
  - a. Selezionare **Azione > Aggiorna con metadati**.
  - b. Seleziona **Scegli file** e carica i metadati.
  - c. Selezionare **Avanti**.
  - d. Seleziona **Salva**.
4. Risolvi l'errore dovuto all'attributo non utilizzato:
  - a. Selezionare la nuova connessione.
  - b. Selezionare **Configura SSO browser > Configura creazione asserzione > Contratto attributo**.
  - c. Elimina la voce per **urn:oid**.
  - d. Seleziona **Salva**.

## Disabilitare l'accesso singolo

Se non si desidera più utilizzare questa funzionalità, è possibile disattivare l'accesso Single Sign-On (SSO). È necessario disabilitare l'accesso singolo prima di poter disabilitare la federazione delle identità.

## Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)" .
- Hai "[autorizzazioni di accesso specifiche](#)" .

## Passi

1. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.

Viene visualizzata la pagina Single Sign-on.

2. Selezionare l'opzione **Disabilitato**.
3. Seleziona **Salva**.

Viene visualizzato un messaggio di avviso che indica che ora gli utenti locali potranno effettuare l'accesso.

4. Selezionare **OK**.

Al successivo accesso a StorageGRID , verrà visualizzata la pagina Sign in a StorageGRID e sarà necessario immettere il nome utente e la password di un utente StorageGRID locale o federato.

## Disattivare e riattivare temporaneamente l'accesso singolo per un nodo di amministrazione

Potresti non essere in grado di accedere a Grid Manager se il sistema Single Sign-On (SSO) non funziona. In questo caso, puoi disattivare e riattivare temporaneamente l'SSO per un nodo di amministrazione. Per disattivare e riattivare l'SSO, è necessario accedere alla shell dei comandi del nodo.

## Prima di iniziare

- Hai "[autorizzazioni di accesso specifiche](#)" .
- Tu hai il `Passwords.txt` file.
- Conosci la password dell'utente root locale.

## Informazioni su questo compito

Dopo aver disabilitato l'SSO per un nodo di amministrazione, puoi accedere a Grid Manager come utente root locale. Per proteggere il sistema StorageGRID , è necessario utilizzare la shell dei comandi del nodo per riabilitare l'SSO sul nodo di amministrazione non appena si esegue la disconnessione.



La disabilitazione dell'SSO per un nodo amministrativo non influisce sulle impostazioni SSO per gli altri nodi amministrativi nella griglia. La casella di controllo **Abilita SSO** nella pagina Single Sign-on in Grid Manager rimane selezionata e tutte le impostazioni SSO esistenti vengono mantenute a meno che non vengano aggiornate.

## Passi

1. Accedi a un nodo di amministrazione:
  - a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
  - b. Inserisci la password elencata nel `Passwords.txt` file.
  - c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede come root, il prompt cambia da `$ A #`.

2. Eseguire il seguente comando:`disable-saml`

Un messaggio indica che il comando si applica solo a questo nodo di amministrazione.

3. Conferma che vuoi disabilitare l'SSO.

Un messaggio indica che l'accesso singolo è disabilitato sul nodo.

4. Da un browser Web, accedi a Grid Manager sullo stesso nodo di amministrazione.

Ora viene visualizzata la pagina di accesso di Grid Manager perché l'SSO è stato disabilitato.

5. Sign in con il nome utente root e la password dell'utente root locale.

6. Se hai disabilitato temporaneamente l'SSO perché dovevi correggere la configurazione dell'SSO:

a. Selezionare **CONFIGURAZIONE > Controllo accessi > Single sign-on**.

b. Modifica le impostazioni SSO errate o obsolete.

c. Seleziona **Salva**.

Selezionando **Salva** dalla pagina Single Sign-on, l'SSO viene automaticamente riattivato per l'intera griglia.

7. Se hai disabilitato temporaneamente l'SSO perché avevi bisogno di accedere a Grid Manager per qualche altro motivo:

a. Esegui qualsiasi compito o compiti che devi svolgere.

b. Selezionare **Esci** e chiudere Grid Manager.

c. Riattivare SSO sul nodo di amministrazione. È possibile eseguire uno dei seguenti passaggi:

- Eseguire il seguente comando: `enable-saml`

Un messaggio indica che il comando si applica solo a questo nodo di amministrazione.

Conferma di voler abilitare l'SSO.

Un messaggio indica che l'accesso singolo è abilitato sul nodo.

◦ Riavviare il nodo della griglia: `reboot`

8. Da un browser Web, accedere a Grid Manager dallo stesso nodo di amministrazione.

9. Verificare che venga visualizzata la pagina Sign in a StorageGRID e che sia necessario immettere le credenziali SSO per accedere a Grid Manager.

## **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 COMMERCIALITÀ 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.