



# **API di gestione tenant**

StorageGRID software

NetApp  
July 23, 2026

# Sommario

- API di gestione tenant ..... 1
  - Scopri l'API di gestione dei tenant di StorageGRID ..... 1
    - operazioni API ..... 1
    - Dettagli operativi ..... 2
    - Invia richieste API ..... 3
  - Versionamento dell'API di gestione dei tenant di StorageGRID ..... 4
    - Determina quali versioni API sono supportate nella release corrente ..... 5
    - Specifica una versione API per una richiesta ..... 5
  - Proteggi contro gli attacchi Cross-Site Request Forgery in StorageGRID ..... 5

# API di gestione tenant

## Scopri l'API di gestione dei tenant di StorageGRID

Puoi eseguire le attività di gestione del sistema utilizzando l'API REST di Tenant Management anziché l'interfaccia utente di Tenant Manager. Ad esempio, potresti voler utilizzare l'API per automatizzare le operazioni o per creare più entità, come gli utenti, in modo più rapido.

API di gestione tenant:

- Utilizza la piattaforma API open source Swagger. Swagger offre un'interfaccia utente intuitiva che permette sia a sviluppatori che a non sviluppatori di interagire con l'API. L'interfaccia utente di Swagger fornisce dettagli e documentazione completi per ogni operazione dell'API.
- Usa ["gestione delle versioni per supportare aggiornamenti non disruptivi"](#).

Per accedere alla documentazione Swagger per l'API di gestione dei tenant:

1. Accedi al Tenant Manager.
2. Dalla parte superiore di Tenant Manager, seleziona l'icona di aiuto e seleziona **API documentation**.

### operazioni API

L'API di gestione dei tenant organizza le operazioni API disponibili nelle seguenti sezioni:

- **account**: Operazioni sull'account tenant corrente, incluso il recupero delle informazioni sull'utilizzo dello storage.
- **auth**: Operazioni per eseguire l'autenticazione della sessione utente.

L'API di gestione dei tenant supporta lo schema di autenticazione Bearer Token. Per accedere come tenant, devi fornire nome utente, password e accountId nel corpo JSON della richiesta di autenticazione (cioè `POST /api/v3/authorize`). Se l'utente viene autenticato correttamente, viene restituito un token di sicurezza. Questo token deve essere fornito nell'intestazione delle richieste API successive ("Authorization: Bearer token").

Per informazioni su come migliorare la sicurezza con autenticazione, vedi ["Proteggi dalle falsificazioni di richieste tra siti \(Cross-Site Request Forgery\)"](#).



Se il single sign-on (SSO) è abilitato per il sistema StorageGRID, devi seguire passaggi diversi per autenticarti. Vedi la ["Istruzioni per usare l'API di gestione della griglia"](#).

- **config**: Operazioni relative alla release del prodotto e alle versioni dell'API di gestione del tenant. Puoi elencare la versione della release del prodotto e le versioni principali dell'API supportate da quella release.
- **container**: Operazioni sui bucket S3.
- **funzionalità-disattivate**: Operazioni per visualizzare le funzionalità che potrebbero essere state disattivate.
- **endpoint**: operazioni per gestire un endpoint. Gli endpoint consentono a un bucket S3 di utilizzare un servizio esterno per la replica StorageGRID CloudMirror, le notifiche o l'integrazione della ricerca.

- **grid-federation-connections:** Operazioni sulle connessioni di federazione di griglia e sulla replica tra griglie.
- **gruppi:** Operazioni per gestire i gruppi di tenant locali e per recuperare i gruppi di tenant federati da una fonte di identità esterna.
- **identity-source:** Operazioni per configurare un'origine di identità esterna e per sincronizzare manualmente le informazioni di gruppi e utenti federati.
- **ilm:** Operazioni sulle impostazioni di gestione del ciclo di vita delle informazioni (ILM).
- **regioni:** Operazioni per determinare quali regioni sono state configurate per il sistema StorageGRID.
- **s3:** Operazioni per la gestione delle chiavi di accesso S3 per gli utenti del tenant.
- **s3-object-lock:** Operazioni sulle impostazioni globali di S3 Object Lock, utilizzate per supportare la conformità normativa.
- **Utenti:** Operazioni per visualizzare e gestire gli utenti del tenant.

## Dettagli operativi

Espandendo ciascuna operazione API, puoi vedere l'azione HTTP, l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (se richiesto) e le possibili risposte.

**groups**
Operations on groups

GET
/org/groups
Lists Tenant User Groups

Parameters
Try it out

| Name                                       | Description                                           |
|--------------------------------------------|-------------------------------------------------------|
| <b>type</b><br>string<br>(query)           | filter by group type                                  |
| <b>limit</b><br>integer<br>(query)         | maximum number of results                             |
| <b>marker</b><br>string<br>(query)         | marker-style pagination offset (value is Group's URN) |
| <b>includeMarker</b><br>boolean<br>(query) | if set, the marker element is also returned           |
| <b>order</b><br>string<br>(query)          | pagination order (desc requires marker)               |

Responses
Response content type
application/json

| Code | Description                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 200  | <div> Example Value Model </div> <pre> {   "responseTime": "2018-02-01T16:22:31.066Z",   "status": "success",   "apiVersion": "2.1" } </pre> |

## Invia richieste API



Qualsiasi operazione API che esegui tramite la pagina web della documentazione API è un'operazione live. Fai attenzione a non creare, aggiornare o eliminare per errore dati di configurazione o altri dati.

### Passaggi

1. Seleziona l'azione HTTP per visualizzare i dettagli della richiesta.
2. Verifica se la richiesta richiede parametri aggiuntivi, come un ID di gruppo o un ID utente. Quindi, recupera questi valori. Potresti dover prima effettuare una richiesta API diversa per ottenere le informazioni di cui hai bisogno.
3. Determina se devi modificare il corpo della richiesta di esempio. In tal caso, puoi selezionare **Model** per conoscere i requisiti di ciascun campo.

4. `${post_edited_translations.segment}`
5. Fornisci i parametri richiesti o modifica il corpo della richiesta come necessario.
6. Seleziona **Esegui**.
7. Esamina il codice di risposta per determinare se la richiesta è andata a buon fine.

## Versionamento dell'API di gestione dei tenant di StorageGRID

`${post_edited_translations.segment}`

Ad esempio, questo URL di richiesta specifica la versione 4 dell'API.

```
https://hostname_or_ip_address/api/v4/authorize
```

La versione principale dell'API viene aggiornata quando vengono apportate modifiche non compatibili con le versioni precedenti. La versione secondaria dell'API viene aggiornata quando vengono apportate modifiche compatibili con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o nuove proprietà.

L'esempio seguente illustra come la versione dell'API viene incrementata in base al tipo di modifiche apportate.

| <code>\${post_edited_translations.segment}</code> | Vecchia versione | <code>\${post_edited_translations.segment}</code> |
|---------------------------------------------------|------------------|---------------------------------------------------|
| <code>\${post_edited_translations.segment}</code> | 2,1              | 2,2                                               |
| Non compatibile con le versioni precedenti        | 2,1              | 3,0                                               |

Quando installi il software StorageGRID per la prima volta, viene abilitata solo la versione più recente dell'API. Tuttavia, quando esegui l'upgrade a una nuova release di funzionalità di StorageGRID, continui ad avere accesso alla versione precedente dell'API per almeno una release di funzionalità di StorageGRID.



Puoi configurare le versioni supportate. Consulta la sezione **config** della documentazione dell'API Swagger per ["API di gestione della griglia"](#) ulteriori informazioni. Dovresti disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API alla versione più recente.

Le richieste obsolete sono contrassegnate come deprecated nei seguenti modi:

- L'intestazione della risposta è "Deprecated: true"
- Il corpo della risposta JSON include "deprecated": true
- Viene aggiunto un avviso di deprecazione a nms.log. Ad esempio:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

## Determina quali versioni API sono supportate nella release corrente

Usa la GET `/versions` richiesta API per restituire un elenco delle versioni principali dell'API supportate. Questa richiesta si trova nella sezione **config** della documentazione Swagger API.

```
GET https://{IP-Address}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

## Specifica una versione API per una richiesta

Puoi specificare la versione dell'API utilizzando un parametro di percorso (`/api/v4`) o un header (`Api-Version: 4`). Se fornisci entrambi i valori, il valore dell'header sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

## Proteggi contro gli attacchi Cross-Site Request Forgery in StorageGRID

Puoi aiutare a proteggerti dagli attacchi Cross-Site Request Forgery (CSRF) contro StorageGRID usando i token CSRF per rafforzare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; gli altri client API possono scegliere se abilitarla quando effettuano l'accesso.

Un utente malintenzionato in grado di attivare una richiesta a un sito diverso (ad esempio tramite un modulo HTTP POST) può far sì che determinate richieste vengano effettuate utilizzando i cookie dell'utente autenticato.

StorageGRID contribuisce a proteggere dagli attacchi CSRF tramite l'utilizzo di token CSRF. Quando questa funzionalità è abilitata, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro specifico del corpo di una richiesta POST.

Per abilitare la funzione, imposta il `csrfToken` parametro su `true` durante l'autenticazione. Il valore predefinito è `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Quando è true, viene impostato un cookie GridCsrfToken con un valore casuale per gli accessi al Grid Manager e il cookie AccountCsrfToken viene impostato con un valore casuale per gli accessi al Tenant Manager.

`${post_edited_translations.segment}`

- L' `X-Csrf-Token` intestazione, con il valore dell'intestazione impostato sul valore del cookie del token CSRF.
- Per gli endpoint che accettano un corpo codificato in formato form-encoded: un parametro del corpo della richiesta codificato in formato `csrfToken` form-encoded.

Per configurare la protezione CSRF, usa ["API di gestione della griglia"](#) o ["API di gestione tenant"](#).



Le richieste che includono un cookie CSRF token impongono anche l'intestazione "Content-Type: application/json" per qualsiasi richiesta che si aspetti un corpo della richiesta in formato JSON, come ulteriore protezione contro gli attacchi CSRF.

## Informazioni sul copyright

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

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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