



Utilizzare l'API se è abilitato l'accesso singolo

StorageGRID software

NetApp
December 03, 2025

Sommario

Utilizzare l'API se è abilitato l'accesso singolo	1
Utilizzare l'API se è abilitato l'accesso singolo (Active Directory)	1
Sign in all'API se è abilitato l'accesso singolo	1
Disconnettersi dall'API se è abilitato l'accesso singolo	6
Utilizzare l'API se è abilitato l'accesso Single Sign-On (Azure)	8
Sign in all'API se è abilitato l'accesso Single Sign-On di Azure	8
Utilizzare l'API se è abilitato l'accesso singolo (PingFederate)	9
Sign in all'API se è abilitato l'accesso singolo	9
Disconnettersi dall'API se è abilitato l'accesso singolo	13

Utilizzare l'API se è abilitato l'accesso singolo

Utilizzare l'API se è abilitato l'accesso singolo (Active Directory)

Se hai "configurato e abilitato l'accesso singolo (SSO)" e si utilizza Active Directory come provider SSO, è necessario inviare una serie di richieste API per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Sign in all'API se è abilitato l'accesso singolo

Queste istruzioni sono valide se si utilizza Active Directory come provider di identità SSO.

Prima di iniziare

- Conosci il nome utente e la password SSO di un utente federato che appartiene a un gruppo di utenti StorageGRID .
- Se vuoi accedere all'API di gestione tenant, devi conoscere l'ID dell'account tenant.

Informazioni su questo compito

Per ottenere un token di autenticazione, puoi utilizzare uno dei seguenti esempi:

- IL storagegrid-ssoauth.py Script Python, che si trova nella directory dei file di installazione StorageGRID(. /rpms per Red Hat Enterprise Linux, . /debs per Ubuntu o Debian, e . /vsphere per VMware).
- Un esempio di flusso di lavoro delle richieste curl.

Il flusso di lavoro curl potrebbe interrompersi se eseguito troppo lentamente. Potresti visualizzare l'errore: A valid SubjectConfirmation was not found on this Response .



Il flusso di lavoro curl di esempio non protegge la password dalla visualizzazione da parte di altri utenti.

Se riscontri un problema di codifica URL, potresti visualizzare l'errore: Unsupported SAML version .

Passi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
 - Utilizzare il storagegrid-ssoauth.py Script Python. Vai al passaggio 2.
 - Utilizzare le richieste curl. Vai al passaggio 3.
2. Se vuoi usare il storagegrid-ssoauth.py script, passa lo script all'interprete Python ed esegui lo script.

Quando richiesto, immettere i valori per i seguenti argomenti:

- Il metodo SSO. Inserisci ADFS o adfs.
- Il nome utente SSO
- Il dominio in cui è installato StorageGRID

- L'indirizzo per StorageGRID
- ID dell'account tenant, se si desidera accedere all'API di gestione tenant.

```
python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****
*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Il token di autorizzazione StorageGRID viene fornito nell'output. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se non utilizzassi l'SSO.

3. Se si desidera utilizzare le richieste curl, attenersi alla seguente procedura.

- Dichiarare le variabili necessarie per effettuare l'accesso.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```



Per accedere all'API di gestione della griglia, utilizzare 0 come TENANTACCOUNTID .

- Per ricevere un URL di autenticazione firmato, inviare una richiesta POST a /api/v3/authorize-saml e rimuovere la codifica JSON aggiuntiva dalla risposta.

Questo esempio mostra una richiesta POST per un URL di autenticazione firmato per TENANTACCOUNTID . I risultati saranno trasmessi a python -m json.tool per rimuovere la codifica JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
-H "accept: application/json" -H "Content-Type: application/json" \
--data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La risposta per questo esempio include un URL firmato codificato in URL, ma non include il livello di codifica JSON aggiuntivo.

```
{  
    "apiVersion": "3.0",  
    "data":  
        "https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...  
        ss1%2BfQ33cvfwA%3D&RelayState=12345",  
        "responseTime": "2018-11-06T16:30:23.355Z",  
        "status": "success"  
}
```

- c. Salva il SAMLRequest dalla risposta per utilizzarla nei comandi successivi.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...ss1%2BfQ33cvfwA%3D'
```

- d. Ottieni un URL completo che includa l'ID della richiesta client da AD FS.

Un'opzione è quella di richiedere il modulo di accesso utilizzando l'URL della risposta precedente.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=  
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"  
id="loginForm"'
```

La risposta include l'ID della richiesta del client:

```
<form method="post" id="loginForm" autocomplete="off"  
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)  
Login.submitLoginRequest();" action="/adfs/ls/?  
SAMLRequest=fZHRT0MwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie  
nt-request-id=00000000-0000-0000-ee02-008000000de" >
```

- e. Salva l'ID della richiesta del client dalla risposta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-008000000de'
```

- f. Invia le tue credenziali all'azione del modulo dalla risposta precedente.

```
curl -x POST "https://$AD_FS_ADDRESS  
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client  
-request-id=$SAMLREQUESTID" \  
--data "UserName=$SAMLUER@$SAMLDOMAIN&Password=  
$SAMPLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS restituisce un reindirizzamento 302, con informazioni aggiuntive nelle intestazioni.



Se l'autenticazione a più fattori (MFA) è abilitata per il tuo sistema SSO, il post del modulo conterrà anche la seconda password o altre credenziali.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRT0MwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Salva il MSISAuth cookie dalla risposta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Invia una richiesta GET alla posizione specificata con i cookie dal POST di autenticazione.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
\$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Le intestazioni della risposta conterranno informazioni sulla sessione AD FS per un successivo utilizzo in caso di disconnessione, mentre il corpo della risposta conterrà SAMLResponse in un campo modulo nascosto.

```

HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1ppi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bk11MnFuUSUzzCUzzCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjoxMjoxOVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
<input type="hidden" name="SAMLResponse"
value="PHNhbw0lJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

- i. Salva il SAMLResponse dal campo nascosto:

```
export SAMLResponse='PHNhbw0lJlc3BvbnN...1scDpSZXNwb25zZT4='
```

- j. Utilizzando il salvato SAMLResponse , crea uno StorageGRID/api/saml-response richiesta di generazione di un token di autenticazione StorageGRID .

Per RelayState , utilizzare l'ID dell'account tenant oppure utilizzare 0 se si desidera accedere all'API di gestione della griglia.

```
curl -x POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
-H "accept: application/json" \
--data-urlencode "SAMLResponse=$SAMLResponse" \
--data-urlencode "RelayState=$TENANTACCOUNTID" \
| python -m json.tool
```

La risposta include il token di autenticazione.

```
{  
    "apiVersion": "3.0",  
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",  
    "responseTime": "2018-11-07T21:32:53.486Z",  
    "status": "success"  
}
```

- a. Salva il token di autenticazione nella risposta come MYTOKEN .

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ora puoi usare MYTOKEN per altre richieste, in modo simile a come utilizzeresti l'API se non si utilizzasse l'SSO.

Disconnettersi dall'API se è abilitato l'accesso singolo

Se è stato abilitato l'accesso singolo (SSO), è necessario inviare una serie di richieste API per disconnettersi dall'API di gestione della griglia o dall'API di gestione dei tenant. Queste istruzioni si applicano se si utilizza Active Directory come provider di identità SSO

Informazioni su questo compito

Se necessario, puoi disconnetterti dall'API StorageGRID effettuando il logout dalla pagina di disconnessione singola della tua organizzazione. In alternativa, è possibile attivare il single logout (SLO) da StorageGRID, che richiede un token portatore StorageGRID valido.

Passi

1. Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true" all'API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \  
-H "accept: application/json" \  
-H "Authorization: Bearer $MYTOKEN" \  
--cookie "sso=true" \  
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{  
    "apiVersion": "3.0",  
    "data":  
        "https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",  
    "responseTime": "2018-11-20T22:20:30.839Z",  
    "status": "success"  
}
```

2. Salva l'URL di disconnessione.

```
export LOGOUT_REQUEST  
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione solo tramite API.

```
HTTP/1.1 302 Found  
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-  
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256  
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018  
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Eliminare il token portatore StorageGRID .

L'eliminazione del token portatore StorageGRID funziona allo stesso modo dell'eliminazione senza SSO. Se non viene specificato `cookie "sso=true", l'utente viene disconnesso da StorageGRID senza che ciò influisca sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \  
-H "accept: application/json" \  
-H "Authorization: Bearer $MYTOKEN" \  
--include
```

UN 204 No Content la risposta indica che l'utente è ora disconnesso.

Utilizzare l'API se è abilitato l'accesso Single Sign-On (Azure)

Se hai "configurato e abilitato l'accesso singolo (SSO)" e si utilizza Azure come provider SSO, è possibile utilizzare due script di esempio per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Sign in all'API se è abilitato l'accesso Single Sign-On di Azure

Queste istruzioni si applicano se si utilizza Azure come provider di identità SSO

Prima di iniziare

- Conosci l'indirizzo email e la password SSO di un utente federato che appartiene a un gruppo di utenti StorageGRID .
- Se vuoi accedere all'API di gestione tenant, devi conoscere l'ID dell'account tenant.

Informazioni su questo compito

Per ottenere un token di autenticazione, è possibile utilizzare i seguenti script di esempio:

- IL `storagegrid-ssoauth-azure.py` Script Python
- IL `storagegrid-ssoauth-azure.js` Script Node.js

Entrambi gli script si trovano nella directory dei file di installazione StorageGRID(./rpms per Red Hat Enterprise Linux, ./debs per Ubuntu o Debian, e ./vsphere per VMware).

Per scrivere la tua integrazione API con Azure, consulta `storagegrid-ssoauth-azure.py` sceneggiatura. Lo script Python invia direttamente due richieste a StorageGRID (prima per ottenere SAMLRequest e poi per ottenere il token di autorizzazione) e chiama anche lo script Node.js per interagire con Azure ed eseguire le operazioni SSO.

Le operazioni SSO possono essere eseguite utilizzando una serie di richieste API, ma non è un'operazione semplice. Il modulo Puppeteer Node.js viene utilizzato per eseguire lo scraping dell'interfaccia Azure SSO.

Se riscontri un problema di codifica URL, potresti visualizzare l'errore: `Unsupported SAML version`.

Passi

1. Installare le dipendenze richieste, come segue:
 - a. Installa Node.js (vedi "<https://nodejs.org/en/download/>").
 - b. Installa i moduli Node.js richiesti (puppeteer e jsdom):

```
npm install -g <module>
```

2. Passare lo script Python all'interprete Python per eseguirlo.

Lo script Python chiamerà quindi lo script Node.js corrispondente per eseguire le interazioni SSO di Azure.

3. Quando richiesto, immettere i valori per i seguenti argomenti (o passarli utilizzando i parametri):
 - L'indirizzo e-mail SSO utilizzato per accedere ad Azure
 - L'indirizzo per StorageGRID
 - ID dell'account tenant, se si desidera accedere all'API di gestione tenant
4. Quando richiesto, immettere la password e prepararsi a fornire un'autorizzazione MFA ad Azure, se richiesto.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.example.com --tenant-account-id 0
Enter the user's SSO password:
*****
Watch for and approve a 2FA authorization request
*****
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion': '3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



Lo script presuppone che l'autenticazione MFA venga eseguita tramite Microsoft Authenticator. Potrebbe essere necessario modificare lo script per supportare altre forme di MFA (ad esempio l'inserimento di un codice ricevuto in un messaggio di testo).

Il token di autorizzazione StorageGRID viene fornito nell'output. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se non utilizzassi l'SSO.

Utilizzare l'API se è abilitato l'accesso singolo (PingFederate)

Se hai "configurato e abilitato l'accesso singolo (SSO)" e utilizzi PingFederate come provider SSO, devi inviare una serie di richieste API per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Sign in all'API se è abilitato l'accesso singolo

Queste istruzioni si applicano se si utilizza PingFederate come provider di identità SSO

Prima di iniziare

- Conosci il nome utente e la password SSO di un utente federato che appartiene a un gruppo di utenti StorageGRID .
- Se vuoi accedere all'API di gestione tenant, devi conoscere l'ID dell'account tenant.

Informazioni su questo compito

Per ottenere un token di autenticazione, puoi utilizzare uno dei seguenti esempi:

- IL `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione StorageGRID(. /rpms per Red Hat Enterprise Linux, ./debs per Ubuntu o Debian, e ./vsphere per VMware).
- Un esempio di flusso di lavoro delle richieste curl.

Il flusso di lavoro curl potrebbe interrompersi se eseguito troppo lentamente. Potresti visualizzare l'errore: A valid SubjectConfirmation was not found on this Response .



Il flusso di lavoro curl di esempio non protegge la password dalla visualizzazione da parte di altri utenti.

Se riscontri un problema di codifica URL, potresti visualizzare l'errore: `Unsupported SAML version`.

Passi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
 - Utilizzare il `storagegrid-ssoauth.py` Script Python. Vai al passaggio 2.
 - Utilizzare le richieste curl. Vai al passaggio 3.
2. Se vuoi usare il `storagegrid-ssoauth.py` script, passa lo script all'interprete Python ed esegui lo script.

Quando richiesto, immettere i valori per i seguenti argomenti:

- Il metodo SSO. È possibile immettere qualsiasi variante di "pingfederate" (PINGFEDERATE, pingfederate e così via).
- Il nome utente SSO
- Il dominio in cui è installato StorageGRID . Questo campo non è utilizzato per PingFederate. Puoi lasciarlo vuoto o inserire qualsiasi valore.
- L'indirizzo per StorageGRID
- ID dell'account tenant, se si desidera accedere all'API di gestione tenant.

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_domain:
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****
*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Il token di autorizzazione StorageGRID viene fornito nell'output. Ora puoi utilizzare il token per altre richieste, in modo simile a come utilizzeresti l'API se non utilizzassi l'SSO.

3. Se si desidera utilizzare le richieste curl, attenersi alla seguente procedura.

- a. Dichiarare le variabili necessarie per effettuare l'accesso.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```



Per accedere all'API di gestione della griglia, utilizzare 0 come TENANTACCOUNTID .

- b. Per ricevere un URL di autenticazione firmato, inviare una richiesta POST a /api/v3/authorize-saml e rimuovere la codifica JSON aggiuntiva dalla risposta.

Questo esempio mostra una richiesta POST per un URL di autenticazione firmato per TENANTACCOUNTID. I risultati verranno passati a python -m json.tool per rimuovere la codifica JSON.

```
curl -x POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
-H "accept: application/json" -H "Content-Type: application/json"
\ 
--data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La risposta per questo esempio include un URL firmato codificato in URL, ma non include il livello di codifica JSON aggiuntivo.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

- c. Salva il SAMLRequest dalla risposta per utilizzarla nei comandi successivi.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

- d. Esporta la risposta e il cookie e ripeti la risposta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

- e. Esporta il valore 'pf.adapterId' e riproduci la risposta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

- f. Esporta il valore 'href' (rimuovi la barra finale /) e riproduci la risposta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

- g. Esporta il valore 'azione':

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

- h. Invia i cookie insieme alle credenziali:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=$SAMPLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER" \
--include
```

- i. Salva il SAMLResponse dal campo nascosto:

```
export SAMLResponse='PHNhbWxwO1Jlc3BvbnN...1scDpSZXNwb25zZT4='
```

- j. Utilizzando il salvato SAMLResponse , crea uno StorageGRID/api/saml-response richiesta di generazione di un token di autenticazione StorageGRID .

Per RelayState , utilizzare l'ID dell'account tenant oppure utilizzare 0 se si desidera accedere all'API di gestione della griglia.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
-H "accept: application/json" \
--data-urlencode "SAMLResponse=$SAMLResponse" \
--data-urlencode "RelayState=$TENANTACCOUNTID" \
| python -m json.tool
```

La risposta include il token di autenticazione.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

- Salva il token di autenticazione nella risposta come MYTOKEN .

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ora puoi usare MYTOKEN per altre richieste, in modo simile a come utilizzeresti l'API se non si utilizzasse l'SSO.

Disconnettersi dall'API se è abilitato l'accesso singolo

Se è stato abilitato l'accesso singolo (SSO), è necessario inviare una serie di richieste API per disconnettersi dall'API di gestione della griglia o dall'API di gestione dei tenant. Queste istruzioni si applicano se si utilizza PingFederate come provider di identità SSO

Informazioni su questo compito

Se necessario, puoi disconnetterti dall'API StorageGRID effettuando il logout dalla pagina di disconnessione singola della tua organizzazione. In alternativa, è possibile attivare il single logout (SLO) da StorageGRID, che richiede un token portatore StorageGRID valido.

Passi

- Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true" all'API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRquest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Salva l'URL di disconnessione.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione solo tramite API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Eliminare il token portatore StorageGRID .

L'eliminazione del token portatore StorageGRID funziona allo stesso modo dell'eliminazione senza SSO. Se non viene specificato `cookie "sso=true", l'utente viene disconnesso da StorageGRID senza che ciò influisca sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

UN 204 No Content la risposta indica che l'utente è ora disconnesso.

```
HTTP/1.1 204 No Content
```

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.