



Use a API se o logon único estiver ativado

StorageGRID

NetApp
March 12, 2025

Índice

Use a API se o logon único estiver ativado	1
Use a API se o logon único estiver ativado (ative Directory)	1
Faça login na API se o logon único estiver ativado	1
Saia da API se o logon único estiver ativado	6
Use a API se o logon único estiver habilitado (Azure)	8
Inicie sessão na API se o início de sessão único do Azure estiver ativado	8
Use a API se o logon único estiver ativado (PingFederate)	9
Faça login na API se o logon único estiver ativado	9
Saia da API se o logon único estiver ativado	13

Use a API se o logon único estiver ativado

Use a API se o logon único estiver ativado (ative Directory)

Se você tiver "[Logon único configurado e habilitado \(SSO\)](#)" e usar o ative Directory como provedor SSO, deverá emitir uma série de solicitações de API para obter um token de autenticação válido para a API de Gerenciamento de Grade ou para a API de Gerenciamento do locatário.

Faça login na API se o logon único estiver ativado

Estas instruções se aplicam se você estiver usando o ative Directory como provedor de identidade SSO.

Antes de começar

- Você conhece o nome de usuário e a senha SSO para um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você quiser acessar a API de gerenciamento do locatário, você sabe o ID da conta do locatário.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar um dos seguintes exemplos:

- O `storagegrid-ssoauth.py` script Python, que está localizado no diretório de arquivos de instalação do StorageGRID (`./rpms` para Red Hat Enterprise Linux, `./debs para Ubuntu ou Debian, e ./vsphere para VMware).`
- Um exemplo de fluxo de trabalho de solicitações curl.

O fluxo de trabalho curl pode ter um tempo limite se você o executar muito lentamente. Você pode ver o erro: `A valid SubjectConfirmation was not found on this Response.`



O fluxo de trabalho cURL de exemplo não protege a senha de ser vista por outros usuários.

Se você tiver um problema de codificação de URL, poderá ver o erro: `Unsupported SAML version.`

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
 - Use o `storagegrid-ssoauth.py` script Python. Avance para o passo 2.
 - Use solicitações curl. Avance para o passo 3.
2. Se você quiser usar o `storagegrid-ssoauth.py` script, passe o script para o interpretador Python e execute o script.

Quando solicitado, insira valores para os seguintes argumentos:

- O método SSO. Introduza ADFS ou adfs.
- O nome de usuário SSO
- O domínio onde o StorageGRID está instalado
- O endereço para StorageGRID

- O ID da conta do locatário, se você quiser acessar a API de gerenciamento do locatário.

```
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
```

O token de autorização StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

3. Se você quiser usar solicitações curl, use o procedimento a seguir.

- a. Declare as variáveis necessárias para iniciar sessão.

```
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'
```



Para acessar a API de gerenciamento de grade, use 0 como TENANTACCOUNTID.

- b. Para receber um URL de autenticação assinada, emita uma SOLICITAÇÃO POST para /api/v3/authorize-saml, e remova a codificação JSON adicional da resposta.

Este exemplo mostra uma SOLICITAÇÃO POST para um URL de autenticação assinada para TENANTACCOUNTID. Os resultados serão passados para `python -m json.tool remove` a codificação 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
```

A resposta para este exemplo inclui um URL assinado que é codificado por URL, mas não inclui a camada adicional de codificação JSON.

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

- c. Salve o `SAMLRequest` da resposta para uso em comandos subsequentes.

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

- d. Obtenha um URL completo que inclua o ID de solicitação do cliente do AD FS.

Uma opção é solicitar o formulário de login usando o URL da resposta anterior.

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

A resposta inclui o ID de solicitação do cliente:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRT0MwFIZfhh...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

- e. Salve o ID de solicitação do cliente da resposta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

- f. Envie suas credenciais para a ação de formulário da resposta anterior.

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

O AD FS retorna um redirecionamento 302, com informações adicionais nos cabeçalhos.



Se a autenticação multifator (MFA) estiver ativada para seu sistema SSO, o post de formulário também conterá a segunda senha ou outras credenciais.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRTomwFIZfhb...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. Salve o MSISAuth cookie da resposta.

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

h. Envie uma SOLICITAÇÃO GET para o local especificado com os cookies do POST de autenticação.

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

Os cabeçalhos de resposta conterão informações de sessão do AD FS para uso posterior de logout e o corpo de resposta contém o SAMLResponse em um campo de formulário oculto.

```
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=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XfXVWx3bk1lMnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LTNmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjoiOVpcMQ==;
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="PHNhbWxwOlJlc3Bvb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

- i. Salve o SAMLResponse do campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb25zZT4='
```

- j. Usando o SAMLResponse, faça uma solicitação StorageGRID/api/saml-response para gerar um token de autenticação StorageGRID.

Para RelayState, use o ID da conta do locatário ou use 0 se quiser entrar na API de gerenciamento de grade.

```
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
```

A resposta inclui o token de autenticação.

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

- a. Salve o token de autenticação na resposta como MYTOKEN.

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

Agora você pode usar MYTOKEN para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

Saia da API se o logon único estiver ativado

Se o logon único (SSO) tiver sido ativado, você deverá emitir uma série de solicitações de API para sair da API de gerenciamento de grade ou da API de gerenciamento de locatário. Estas instruções se aplicam se você estiver usando o ative Directory como provedor de identidade SSO

Sobre esta tarefa

Se necessário, você pode sair da API do StorageGRID fazendo logout da página de logout única da sua organização. Ou, você pode acionar o logout único (SLO) do StorageGRID, que requer um token válido do portador do StorageGRID.

Passos

1. Para gerar uma solicitação de logout assinada, passe "cookie "sso" para a 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
```

Um URL de logout é retornado:


```
{
  "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. Salve o URL de logout.

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

3. Envie uma solicitação para o URL de logout para acionar o SLO e redirecionar de volta para o StorageGRID.

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

A resposta 302 é devolvida. O local de redirecionamento não é aplicável ao logout somente 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. Exclua o token do portador do StorageGRID.

A exclusão do token portador do StorageGRID funciona da mesma forma que sem SSO. Se "cookie "sso" não for fornecido, o usuário será desconetado do StorageGRID sem afetar o estado SSO.

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

Uma 204 No Content resposta indica que o usuário está desconetado agora.

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

Use a API se o logon único estiver habilitado (Azure)

Se você tiver "[Logon único configurado e habilitado \(SSO\)](#)" e usar o Azure como provedor SSO, você pode usar dois scripts de exemplo para obter um token de autenticação válido para a API de Gerenciamento de Grade ou a API de Gerenciamento do localatário.

Inicie sessão na API se o início de sessão único do Azure estiver ativado

Estas instruções se aplicam se você estiver usando o Azure como provedor de identidade SSO

Antes de começar

- Você sabe o endereço de e-mail SSO e a senha de um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você quiser acessar a API de gerenciamento do localatário, você sabe o ID da conta do localatário.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar os seguintes scripts de exemplo:

- O `storagegrid-ssoauth-azure.py` script Python
- O `storagegrid-ssoauth-azure.js` script Node.js

Ambos os scripts estão localizados no diretório de arquivos de instalação do StorageGRID (`./rpms` para o Red Hat Enterprise Linux, `./debs para Ubuntu ou Debian e ./vsphere para VMware).`

Para escrever sua própria integração com a API do Azure, consulte o `storagegrid-ssoauth-azure.py` script. O script Python faz duas solicitações diretamente ao StorageGRID (primeiro para obter o SAMLRequest e depois para obter o token de autorização), e também chama o script Node.js para interagir com o Azure para executar as operações SSO.

As operações SSO podem ser executadas usando uma série de solicitações de API, mas isso não é simples. O módulo Puppeteer Node.js é usado para raspar a interface SSO do Azure.

Se você tiver um problema de codificação de URL, poderá ver o erro: `Unsupported SAML version.`

Passos

1. Instale as dependências necessárias, da seguinte forma:
 - a. Instale o Node.js ("<https://nodejs.org/en/download/>" consulte).
 - b. Instale os módulos Node.js necessários (puppeteer e jsdom):

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

2. Passe o script Python para o interpretador Python para executar o script.

O script Python chamará então o script Node.js correspondente para executar as interações SSO do Azure.

3. Quando solicitado, insira valores para os seguintes argumentos (ou passe-os usando parâmetros):
 - O endereço de e-mail SSO usado para entrar no Azure

- O endereço para StorageGRID
 - O ID da conta do locatário, se você quiser acessar a API de gerenciamento do locatário
4. Quando solicitado, insira a senha e esteja preparado para fornecer uma autorização de MFA ao Azure, se solicitado.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.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'}
```



O script assume que o MFA é feito usando o Microsoft Authenticator. Talvez seja necessário modificar o script para dar suporte a outras formas de MFA (como inserir um código recebido em uma mensagem de texto).

O token de autorização StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

Use a API se o logon único estiver ativado (PingFederate)

Se você tem "[Logon único configurado e habilitado \(SSO\)](#)" e usa o PingFederate como provedor SSO, você deve emitir uma série de solicitações de API para obter um token de autenticação válido para a API de Gerenciamento de Grade ou para a API de Gerenciamento do locatário.

Faça login na API se o logon único estiver ativado

Estas instruções se aplicam se você estiver usando o PingFederate como provedor de identidade SSO

Antes de começar

- Você conhece o nome de usuário e a senha SSO para um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você quiser acessar a API de gerenciamento do locatário, você sabe o ID da conta do locatário.

Sobre esta tarefa

Para obter um token de autenticação, você pode usar um dos seguintes exemplos:

- O `storagegrid-ssoauth.py` script Python, que está localizado no diretório de arquivos de instalação do StorageGRID (`./rpms` para Red Hat Enterprise Linux, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware).
- Um exemplo de fluxo de trabalho de solicitações curl.

O fluxo de trabalho curl pode ter um tempo limite se você o executar muito lentamente. Você pode ver o erro: `A valid SubjectConfirmation was not found on this Response.`



O fluxo de trabalho cURL de exemplo não protege a senha de ser vista por outros usuários.

Se você tiver um problema de codificação de URL, poderá ver o erro: `Unsupported SAML version`.

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
 - Use o `storagegrid-ssoauth.py` script Python. Avance para o passo 2.
 - Use solicitações `curl`. Avance para o passo 3.
2. Se você quiser usar o `storagegrid-ssoauth.py` script, passe o script para o interpretador Python e execute o script.

Quando solicitado, insira valores para os seguintes argumentos:

- O método SSO. Você pode inserir qualquer variação de "pingfederate" (PINGFEDERATE, pingfederate, e assim por diante).
- O nome de usuário SSO
- O domínio onde o StorageGRID está instalado. Este campo não é usado para PingFederate. Você pode deixá-lo em branco ou inserir qualquer valor.
- O endereço para StorageGRID
- O ID da conta do locatário, se você quiser acessar a API de gerenciamento do locatário.

```
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
```

O token de autorização StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

3. Se você quiser usar solicitações `curl`, use o procedimento a seguir.
 - a. Declare as variáveis necessárias para iniciar sessão.

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



Para acessar a API de gerenciamento de grade, use 0 como `TENANTACCOUNTID`.

- b. Para receber um URL de autenticação assinada, emita uma SOLICITAÇÃO POST para `/api/v3/authorize-saml`, e remova a codificação JSON adicional da resposta.

Este exemplo mostra uma SOLICITAÇÃO POST para uma URL de autenticação assinada para TENANTACCOUNTID. Os resultados serão passados para Python -m json.tool para remover a codificação 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
```

A resposta para este exemplo inclui um URL assinado que é codificado por URL, mas não inclui a camada adicional de codificação JSON.

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

c. Salve o SAMLRequest da resposta para uso em comandos subsequentes.

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

d. Exporte a resposta e o cookie e ecoe a resposta:

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

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

e. Exporte o valor 'pf.adapterId' e ecoe a resposta:

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

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

f. Exporte o valor 'href' (remova a barra à direita /) e faça eco da resposta:

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

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

g. Exportar o valor "ação":

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

h. Enviar cookies juntamente com credenciais:

```
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. Salve o SAMLResponse do campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Usando o SAMLResponse, faça uma solicitação StorageGRID/api/saml-response para gerar um token de autenticação StorageGRID.

Para RelayState, use o ID da conta do locatário ou use 0 se quiser entrar na API de gerenciamento de grade.

```
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
```

A resposta inclui o token de autenticação.

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

- a. Salve o token de autenticação na resposta como MYTOKEN.

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

Agora você pode usar MYTOKEN para outras solicitações, semelhante a como você usaria a API se o SSO não estivesse sendo usado.

Saia da API se o logon único estiver ativado

Se o logon único (SSO) tiver sido ativado, você deverá emitir uma série de solicitações de API para sair da API de gerenciamento de grade ou da API de gerenciamento de locatário. Estas instruções se aplicam se você estiver usando o PingFederate como provedor de identidade SSO

Sobre esta tarefa

Se necessário, você pode sair da API do StorageGRID fazendo logout da página de logout única da sua organização. Ou, você pode acionar o logout único (SLO) do StorageGRID, que requer um token válido do portador do StorageGRID.

Passos

1. Para gerar uma solicitação de logout assinada, passe "cookie "sso" para a 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
```

Um URL de logout é retornado:

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

2. Salve o URL de logout.

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

3. Envie uma solicitação para o URL de logout para acionar o SLO e redirecionar de volta para o StorageGRID.

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

A resposta 302 é devolvida. O local de redirecionamento não é aplicável ao logout somente 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. Exclua o token do portador do StorageGRID.

A exclusão do token portador do StorageGRID funciona da mesma forma que sem SSO. Se "cookie "sso" não for fornecido, o usuário será desconetado do StorageGRID sem afetar o estado SSO.

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

Uma 204 No Content resposta indica que o usuário está desconetado agora.

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


Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.