



## **Use a API**

### StorageGRID

NetApp  
October 03, 2025

# Índice

Use a API .....	1
Use a API de gerenciamento de grade .....	1
Recursos de nível superior .....	1
Emitir solicitações de API .....	1
Operações da API Grid Management .....	4
Controle de versão da API Grid Management .....	5
Determine quais versões de API são suportadas na versão atual .....	6
Especifique uma versão da API para uma solicitação .....	6
Proteger contra falsificação de solicitação entre locais (CSRF) .....	7
Use a API se o logon único estiver ativado .....	8
Use a API se o logon único estiver ativado (ative Directory) .....	8
Use a API se o logon único estiver habilitado (Azure) .....	15
Use a API se o logon único estiver ativado (PingFederate) .....	16

# Use a API

## Use a API de gerenciamento de grade

Você pode executar tarefas de gerenciamento do sistema usando a API REST do Grid Management em vez da interface de usuário do Grid Manager. Por exemplo, você pode querer usar a API para automatizar operações ou criar várias entidades, como usuários, mais rapidamente.

### Recursos de nível superior

A API de gerenciamento de grade fornece os seguintes recursos de nível superior:

- `/grid`: O acesso é restrito aos usuários do Grid Manager e é baseado nas permissões de grupo configuradas.
- `/org`: O acesso é restrito a usuários que pertencem a um grupo LDAP local ou federado para uma conta de locatário. Para obter detalhes, [Use uma conta de locatário](#) consulte .
- `/private`: O acesso é restrito aos usuários do Grid Manager e é baseado nas permissões de grupo configuradas. As APIs privadas estão sujeitas a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

### Emitir solicitações de API

A API de gerenciamento de grade usa a plataforma de API de código aberto Swagger. O Swagger fornece uma interface de usuário intuitiva que permite que desenvolvedores e não desenvolvedores realizem operações em tempo real no StorageGRID com a API.

A interface do usuário Swagger fornece detalhes completos e documentação para cada operação da API.

#### O que você vai precisar

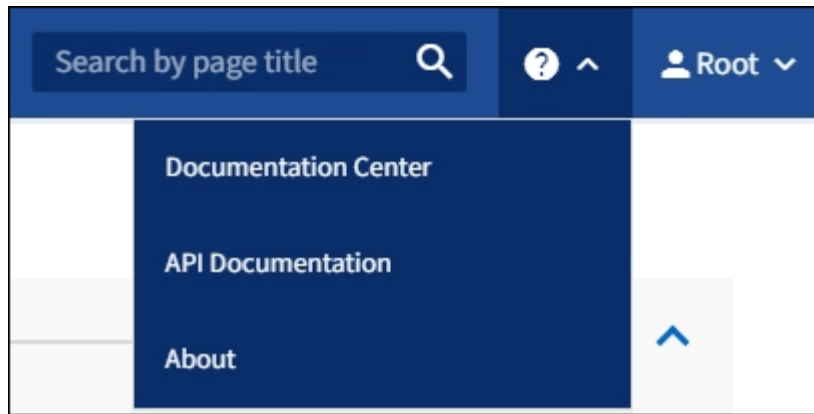
- Você está conectado ao Gerenciador de Grade usando um [navegador da web suportado](#).
- Você tem permissões de acesso específicas.



Todas as operações de API que você executa usando a página da Web do API Docs são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

#### Passos

1. No cabeçalho do Gerenciador de Grade, selecione o ícone de ajuda e selecione **Documentação da API**.



2. Para executar uma operação com a API privada, selecione **ir para a documentação da API privada** na página da API de gerenciamento do StorageGRID.

As APIs privadas estão sujeitas a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

3. Selecione a operação desejada.

Ao expandir uma operação de API, você pode ver as ações HTTP disponíveis, como GET, PUT, UPDATE e DELETE.

4. Selecione uma ação HTTP para ver os detalhes da solicitação, incluindo o URL do endpoint, uma lista de todos os parâmetros necessários ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as possíveis respostas.

GET
/grid/groups
Lists Grid Administrator Groups

Parameters
Try it out

Name	Description
type string (query)	filter by group type Available values : local, federated <div> -- </div>
limit integer (query)	maximum number of results Default value : 25 <div> 25 </div>
marker string (query)	marker-style pagination offset (value is Group's URN) <div> marker - marker-style pagination offset (value </div>
includeMarker boolean (query)	if set, the marker element is also returned <div> -- </div>
order string (query)	pagination order (desc requires marker) Available values : asc, desc <div> -- </div>

Responses
Response content type application/json

Code	Description
200	successfully retrieved Example Value   Model <pre> {   "responseTime": "2021-03-29T14:22:19.673Z",   "status": "success",   "apiVersion": "3.3",   "deprecated": false,   "data": [     {       "displayName": "Developers", </pre>

- Determine se a solicitação requer parâmetros adicionais, como um grupo ou ID de usuário. Em seguida, obtenha esses valores. Talvez você precise emitir uma solicitação de API diferente primeiro para obter as informações de que precisa.
- Determine se você precisa modificar o corpo de solicitação de exemplo. Em caso afirmativo, você pode selecionar **modelo** para aprender os requisitos para cada campo.
- Selecione **Experimente**.
- Forneça quaisquer parâmetros necessários ou modifique o corpo do pedido conforme necessário.
- Selecione **Executar**.
- Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

# Operações da API Grid Management

A API Grid Management organiza as operações disponíveis nas seções a seguir.



Esta lista inclui apenas as operações disponíveis na API pública.

- **\* Contas\*** — operações para gerenciar contas de inquilinos de armazenamento, incluindo a criação de novas contas e recuperação de uso de armazenamento para uma determinada conta.
- **Alarms** — operações para listar alarmes atuais (sistema legado) e retornar informações sobre a integridade da grade, incluindo os alertas atuais e um resumo dos estados de conexão do nó.
- **Alert-history** — operações em alertas resolvidos.
- **Alert-receivers** — operações em recetores de notificação de alerta (e-mail).
- **Alert-rules** — operações em regras de alerta.
- **Alert-silences** — operações em silêncios de alerta.
- **Alertas** — operações em alertas.
- **Audit** — operações para listar e atualizar a configuração da auditoria.
- **Auth** — operações para realizar autenticação de sessão do usuário.

A API de gerenciamento de grade suporta o esquema de autenticação de token do portador. Para fazer login, você fornece um nome de usuário e senha no corpo JSON da solicitação de autenticação (ou seja, `POST /api/v3/authorize`). Se o usuário for autenticado com êxito, um token de segurança será retornado. Esse token deve ser fornecido no cabeçalho de solicitações de API subsequentes ("autorização: Portador *token*").



Se o logon único estiver ativado para o sistema StorageGRID, você deverá executar etapas diferentes para autenticar. Consulte "autenticar na API se o logon único estiver ativado."

Consulte "proteção contra falsificação de solicitação entre sites" para obter informações sobre como melhorar a segurança de autenticação.

- **Certificados de cliente** — operações para configurar certificados de cliente para que o StorageGRID possa ser acessado com segurança usando ferramentas de monitoramento externas.
- **Config** — operações relacionadas à versão do produto e versões da API Grid Management. Você pode listar a versão de lançamento do produto e as principais versões da API de Gerenciamento de Grade suportadas por essa versão, e você pode desativar versões obsoletas da API.
- **Disabled-features** — operações para visualizar recursos que podem ter sido desativados.
- **dns-servers** — operações para listar e alterar servidores DNS externos configurados.
- **Endpoint-domain-nanos** — operações para listar e alterar nomes de domínio de endpoint.
- **Codificação de apagamento** — operações em perfis de codificação de apagamento.
- **Expansão** — operações de expansão (nível de procedimento).
- **Expansion-nanos** — operações em expansão (nível de nó).
- **Expansão-sites** — operações em expansão (nível do site).
- **Grid-networks** — operações para listar e alterar a Grid Network List.
- **\* Grid-passwords\*** — operações para gerenciamento de senhas de grade.

- **Groups** — operações para gerenciar grupos de Administrador de Grade local e recuperar grupos de Administrador de Grade federados de um servidor LDAP externo.
- **Identity-source** — operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo federado e de usuário.
- **ilm** — operações de gerenciamento do ciclo de vida da informação (ILM).
- **Licença** — operações para recuperar e atualizar a licença StorageGRID.
- **Logs** — operações para coletar e baixar arquivos de log.
- **Métricas** — operações em métricas do StorageGRID, incluindo consultas instantâneas de métricas em um único ponto no tempo e consultas de métricas de intervalo ao longo de um intervalo de tempo. A API Grid Management usa a ferramenta de monitoramento de sistemas Prometheus como fonte de dados de back-end. Para obter informações sobre a construção de consultas Prometheus, consulte o site Prometheus.



As métricas que *private* incluem em seus nomes são destinadas apenas para uso interno. Essas métricas estão sujeitas a alterações entre as versões do StorageGRID sem aviso prévio.

- **\* Node-details\*** — operações em detalhes do nó.
- **Node-health** — operações no status de integridade do nó.
- **ntp-servers** — operações para listar ou atualizar servidores NTP (Network Time Protocol) externos.
- **Objects** — operações em objetos e metadados de objetos.
- **Recovery** — operações para o procedimento de recuperação.
- **Recovery-package** — operações para baixar o Recovery Package.
- **Regions** — operações para visualizar e criar regiões.
- **S3-object-lock** — operações em configurações globais de bloqueio de objetos S3D.
- **Server-certificate** — operações para visualizar e atualizar certificados de servidor do Grid Manager.
- **snmp** — operações na configuração SNMP atual.
- **Traffic-classes** — operações para políticas de classificação de tráfego.
- **Não confiável-cliente-rede** — operações na configuração de rede cliente não confiável.
- **Usuários** — operações para visualizar e gerenciar usuários do Grid Manager.

## Controle de versão da API Grid Management

A API de gerenciamento de grade usa o controle de versão para suportar atualizações sem interrupções.

Por exemplo, este URL de solicitação especifica a versão 3 da API.

```
https://hostname_or_ip_address/api/v3/authorize
```

A versão principal da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que são **not compatible** com versões mais antigas. A versão menor da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que **are compatíveis** com versões mais antigas. As alterações compatíveis incluem a adição de novos endpoints ou novas propriedades. O exemplo a seguir ilustra como a versão da API é carregada com base no tipo de alterações feitas.

Tipo de alteração para API	Versão antiga	Nova versão
Compatível com versões mais antigas	2,1	2,2
Não compatível com versões mais antigas	2,1	3,0

Quando você instala o software StorageGRID pela primeira vez, apenas a versão mais recente da API de gerenciamento de grade está ativada. No entanto, quando você atualiza para uma nova versão de recurso do StorageGRID, você continua tendo acesso à versão mais antiga da API para pelo menos uma versão de recurso do StorageGRID.



Você pode usar a API Grid Management para configurar as versões suportadas. Consulte a seção "config" da documentação da API Swagger para obter mais informações. Você deve desativar o suporte para a versão mais antiga depois de atualizar todos os clientes da API Grid Management para usar a versão mais recente.

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Deprecated: True"
- O corpo de resposta JSON inclui "obsoleto": True
- Um aviso obsoleto é adicionado ao nms.log. Por exemplo:

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

## Determine quais versões de API são suportadas na versão atual

Use a seguinte solicitação de API para retornar uma lista das principais versões da API suportada:

```
GET https://{IP-Address}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

## Especifique uma versão da API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (/api/v3) ou um cabeçalho (Api-Version: 3). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.



```
curl https://[IP-Address]/api/v3/grid/accounts
```

```
curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

## Proteger contra falsificação de solicitação entre locais (CSRF)

Você pode ajudar a proteger contra ataques de falsificação de solicitação entre sites (CSRF) contra StorageGRID usando tokens CSRF para melhorar a autenticação que usa cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes de API podem optar por ativá-lo quando fizerem login.

Um invasor que pode acionar uma solicitação para um site diferente (como um POST de formulário HTTP) pode fazer com que certas solicitações sejam feitas usando os cookies do usuário conectado.

O StorageGRID ajuda a proteger contra ataques CSRF usando tokens CSRF. Quando ativado, o conteúdo de um cookie específico deve corresponder ao conteúdo de um cabeçalho específico ou de um parâmetro específico DO corpo DO POST.

Para ativar a funcionalidade, defina o `csrfToken` parâmetro para `true` durante a autenticação. A predefinição é `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 verdadeiro, um `GridCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Grade, e o `AccountCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Tenant.

Se o cookie estiver presente, todas as solicitações que podem modificar o estado do sistema (POST, PUT, PATCH, DELETE) devem incluir um dos seguintes itens:

- O `X-Csrf-Token` cabeçalho, com o valor do cabeçalho definido para o valor do cookie de token CSRF.
- Para endpoints que aceitam um corpo codificado por formulário: Um `csrfToken` parâmetro corpo de solicitação codificado por formulário.

Consulte a documentação da API on-line para obter exemplos e detalhes adicionais.



As solicitações que têm um conjunto de cookies de token CSRF também irão aplicar o `"Content-Type: application/json"` cabeçalho para qualquer solicitação que espera um corpo de solicitação JSON como uma proteção adicional contra ataques CSRF.

# 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.

#### O que você vai precisar

- 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 arquivos de instalação do StorageGRID (`./rpms`` para Linux ou CentOS, para Ubuntu ou Debian, `./debs 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` 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://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=fZHRTToMwFIZfhh...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=fZHRT0MwFIZfhh...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=MjAxOC0xMS0wNzoxNjozMj01OVpcMQ==;
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="PHNhbWxwOlJlc3Bvb3N...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />

```

- i. Salve o SAMLResponse do campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb3N...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 ativo Directory como provedor de identidade SSO

#### Sobre esta tarefa

Se necessário, você pode sair da API do StorageGRID simplesmente 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=true" 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=true" 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

#### O que você vai precisar

- 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 arquivos de instalação do StorageGRID (`./rpms`` para Linux ou CentOS, para Ubuntu ou Debian, `./debs` 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 por 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

#### O que você vai precisar

- 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 arquivos de instalação do StorageGRID (`./rpms` para Linux ou CentOS, para Ubuntu ou Debian, `./debs` 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='PHNhbWxwOlJlc3Bvb3N...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 simplesmente 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=true" 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=true" 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 SOBRESSAIENTES; 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 DOCUMENTOS, 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.