



## 如果启用了单点登录，请使用 **API** StorageGRID

NetApp  
November 04, 2025

# 目录

如果启用了单点登录，请使用 API .....	1
如果启用了单点登录，请使用 API（Active Directory） .....	1
如果启用了单点登录，请登录到 API .....	1
如果启用了单点登录，请注销 API .....	6
如果启用了单点登录，请使用 API（Azure） .....	7
如果启用了 Azure 单点登录，请登录到 API .....	7
如果启用了单点登录，请使用 API（PingFederate） .....	9
如果启用了单点登录，请登录到 API .....	9
如果启用了单点登录，请注销 API .....	12

# 如果启用了单点登录，请使用 API

## 如果启用了单点登录，请使用 API（Active Directory）

如果您有 "已配置并启用单点登录（SSO）" 如果您使用 Active Directory 作为 SSO 提供程序，则必须对一系列 API 请求进行问题描述处理，以获取对网络管理 API 或租户管理 API 有效的身份验证令牌。

### 如果启用了单点登录，请登录到 API

如果您使用 Active Directory 作为 SSO 身份提供程序，则以下说明适用。

#### 开始之前

- 您知道属于 StorageGRID 用户组的联合用户的 SSO 用户名和密码。
- 如果要访问租户管理 API，您知道租户帐户 ID。

#### 关于此任务

要获取身份验证令牌，可以使用以下示例之一：

- `storagegrid-ssoauth.py` Python脚本、位于StorageGRID 安装文件目录中 (`./rpms` 对于Red Hat Enterprise Linux、`./debs` 适用于Ubuntu或Debian、和 `./vsphere` 适用于VMware)。
- cURL 请求的示例工作流。

如果执行速度过慢，则卷曲工作流可能会超时。您可能会看到以下错误：A valid SubjectConfirmation was not found on this Response。



示例 cURL 工作流不会保护密码不会被其他用户看到。

如果您使用的是URL编码问题描述、则可能会看到以下错误：Unsupported SAML version。

#### 步骤

1. 选择以下方法之一以获取身份验证令牌：
  - 使用 `storagegrid-ssoauth.py` Python脚本。转至步骤 2。
  - 使用 `curl` 请求。转至步骤 3。
2. 如果要使用 `storagegrid-ssoauth.py` 脚本、将脚本传递给Python解释器并运行脚本。

出现提示时，输入以下参数的值：

- SSO 方法。输入 ADFS 或 ADFS。
- SSO 用户名
- 安装 StorageGRID 的域
- StorageGRID 的地址
- 要访问租户管理 API 的租户帐户 ID。

```
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
```

输出中提供了 StorageGRID 授权令牌。现在，您可以将令牌用于其他请求，类似于在未使用 SSO 时使用 API 的方式。

3. 如果要使用 curl 请求，请使用以下操作步骤。

a. 声明登录所需的变量。

```
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'
```



要访问网络管理API、请使用0作为 TENANTACCOUNTID。

b. 要接收签名身份验证URL、问题描述 请将POST请求发送到 /api/v3/authorize-saml、并从响应中删除其他JSON编码。

此示例显示了的已签名身份验证URL的POST请求 TENANTACCOUNTID。结果将传递到 `python -m json.tool` 删除JSON编码。

```
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
```

此示例的响应包括一个 URL 编码的签名 URL ，但不包括额外的 JSON 编码层。

```
{
  "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. 保存 SAMLRequest 从响应中获取、以便在后续命令中使用。

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

- d. 从 AD FS 获取包含客户端请求 ID 的完整 URL。

一种方法是使用上一响应中的 URL 请求登录表单。

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

此响应包括客户端请求 ID：

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

- e. 保存响应中的客户端请求 ID。

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

- f. 将您的凭据发送到上一响应中的表单操作。

```
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
```

AD FS 返回 302 重定向，并在标题中显示追加信息。



如果为 SSO 系统启用了多因素身份验证（MFA），则此表单发布还将包含第二个密码或其他凭据。

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRTomwFIZfhh...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. 保存 MSISAuth 响应中的 cookie。

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

h. 使用身份验证 POST 中的 Cookie 将 GET 请求发送到指定位置。

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

响应标头将包含 AD FS 会话信息，以便日后注销时使用，而响应正文将 SAMLResponse 隐藏在一个格式化的字段中。



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

- a. 将响应中的身份验证令牌另存为 MYTOKEN。

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

您现在可以使用 MYTOKEN 对于其他请求、类似于未使用SSO时使用API的方式。

## 如果启用了单点登录，请注销 API

如果已启用单点登录（Single Sign-On，SSO），则必须对一系列 API 请求进行问题描述，才能注销网络管理 API 或租户管理 API。如果您使用 Active Directory 作为 SSO 身份提供程序，则以下说明适用

关于此任务

如果需要、您可以从组织的单点注销页面注销、以注销StorageGRID API。或者，您也可以从 StorageGRID 触发单点注销（SLO），这需要有效的 StorageGRID 令牌。

步骤

1. 要生成签名注销请求、请将`cookie "sso=true "`传递到SLO API:

```
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
```

返回注销 URL：

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

## 2. 保存注销 URL。

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

## 3. 向注销 URL 发送请求以触发 SLO 并重定向回 StorageGRID。

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

返回 302 响应。此重定向位置不适用于纯 API 注销。

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

## 4. 删除 StorageGRID 承载令牌。

删除 StorageGRID 承载令牌的工作方式与不使用 SSO 相同。如果未提供`cookie "sso=true "`、则用户将从StorageGRID中注销、而不会影响SSO状态。

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

答 204 No Content 响应指示用户现在已注销。

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

## 如果启用了单点登录，请使用 **API ( Azure )**

如果您有 "已配置并启用单点登录 ( SSO )" 使用 Azure 作为 SSO 提供程序时，您可以使用两个示例脚本来获取对网络管理 API 或租户管理 API 有效的身份验证令牌。

如果启用了 **Azure** 单点登录，请登录到 **API**

如果您使用 Azure 作为 SSO 身份提供程序，则以下说明适用

## 开始之前

- 您知道属于 StorageGRID 用户组的联合用户的 SSO 电子邮件地址和密码。
- 如果要访问租户管理 API ，您知道租户帐户 ID 。

## 关于此任务

要获取身份验证令牌，可以使用以下示例脚本：

- `storagegrid-ssoauth-azure.py` Python 脚本
- `storagegrid-ssoauth-azure.js` 节点.js脚本

这两个脚本都位于StorageGRID安装文件目录中 (`./rpms` 对于Red Hat Enterprise Linux、`./debs` 适用于Ubuntu或Debian、和 `./vsphere` 适用于VMware)。

要编写您自己的与Azure的API集成、请参见 `storagegrid-ssoauth-azure.py` 脚本。Python 脚本会直接向 StorageGRID 发出两个请求（首先获取 SAMLRequest ，然后再获取授权令牌），同时还会调用 Node.js 脚本与 Azure 交互以执行 SSO 操作。

可以使用一系列 API 请求执行 SSO 操作，但这样做并不简单。puppeteer Node.js 模块用于擦除 Azure SSO 接口。

如果您使用的是URL编码问题描述、则可能会看到以下错误： `Unsupported SAML version.`

## 步骤

1. 安装所需的依赖关系，如下所示：
  - a. 安装 Node.js （请参见 "<https://nodejs.org/en/download/>"）。
  - b. 安装所需的 Node.js 模块（ puppeteer 和 jsdom ）：

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

2. 将 Python 脚本传递给 Python 解释器以运行此脚本。

然后， Python 脚本将调用相应的 Node.js 脚本以执行 Azure SSO 交互。

3. 出现提示时，输入以下参数的值（或使用参数传递这些值）：
  - 用于登录到 Azure 的 SSO 电子邮件地址
  - StorageGRID 的地址
  - 要访问租户管理 API 的租户帐户 ID
4. 出现提示时，输入密码，并在收到请求时准备向 Azure 提供 MFA 授权。

```
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'}
```



此脚本假定 MFA 是使用 Microsoft Authenticator 完成的。您可能需要修改脚本以支持其他形式的MFA (例如、输入在文本消息中收到的代码)。

输出中提供了 StorageGRID 授权令牌。现在，您可以将令牌用于其他请求，类似于在未使用 SSO 时使用 API 的方式。

## 如果启用了单点登录，请使用 API （ PingFederate ）

如果您有 "已配置并启用单点登录（SSO）" 如果使用 PingFederate 作为 SSO 提供程序，则必须对一系列 API 请求进行问题描述 处理，以获取对网格管理 API 或租户管理 API 有效的身份验证令牌。

### 如果启用了单点登录，请登录到 API

如果您使用 PingFederate 作为 SSO 身份提供程序，则以下说明适用

开始之前

- 您知道属于 StorageGRID 用户组的联合用户的 SSO 用户名和密码。
- 如果要访问租户管理 API，您知道租户帐户 ID。

关于此任务

要获取身份验证令牌，可以使用以下示例之一：

- `storagegrid-ssoauth.py` Python脚本、位于StorageGRID 安装文件目录中 (`./rpms` 对于Red Hat Enterprise Linux、`./debs` 适用于Ubuntu或Debian、和 `./vsphere` 适用于VMware)。
- cURL 请求的示例工作流。

如果执行速度过慢，则卷曲工作流可能会超时。您可能会看到以下错误：A valid SubjectConfirmation was not found on this Response。



示例 cURL 工作流不会保护密码不会被其他用户看到。

如果您使用的是URL编码问题描述、则可能会看到以下错误：Unsupported SAML version。

步骤

1. 选择以下方法之一以获取身份验证令牌：
  - 使用 `storagegrid-ssoauth.py` Python脚本。转至步骤 2。
  - 使用 `curl` 请求。转至步骤 3。
2. 如果要使用 `storagegrid-ssoauth.py` 脚本、将脚本传递给Python解释器并运行脚本。

出现提示时，输入以下参数的值：

- SSO 方法。您可以输入"pingfederate"的任何变体(Pingfederate、pingfedate等)。
- SSO 用户名

- 安装 StorageGRID 的域。此字段不用于 PingFederate 。您可以将其留空或输入任何值。
- StorageGRID 的地址
- 要访问租户管理 API 的租户帐户 ID 。

```
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
```

输出中提供了 StorageGRID 授权令牌。现在，您可以将令牌用于其他请求，类似于在未使用 SSO 时使用 API 的方式。

3. 如果要使用 curl 请求，请使用以下操作步骤。

a. 声明登录所需的变量。

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



要访问网络管理API、请使用0作为 TENANTACCOUNTID。

b. 要接收签名身份验证URL、问题描述 请将POST请求发送到 /api/v3/authorize-saml、并从响应中删除其他JSON编码。

此示例显示了一个 POST 请求，用于为 TENANTACCOBTID 提供签名身份验证 URL 。结果将传递到 python -m json.tool 以删除 JSON 编码。

```
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
```

此示例的响应包括一个 URL 编码的签名 URL ，但不包括额外的 JSON 编码层。

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

- c. 保存 SAMLRequest 从响应中获取、以便在后续命令中使用。

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

- d. 导出响应和 cookie，并对响应执行回显：

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

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

- e. 导出 "pf.adapterId" 值，并对响应执行回显：

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

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

- f. 导出 "href" 值（删除后斜杠 /），并对响应执行回显：

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

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

- g. 导出 "act" 值：

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

- h. 发送 Cookie 以及凭据：

```
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. 保存 SAMLResponse 在隐藏字段中:

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

- j. 使用已保存的 SAMLResponse、创建StorageGRID/api/saml-response 生成StorageGRID 身份验证令牌请求。

适用于 RelayState、请使用租户帐户ID或如果要登录到网络管理API、请使用0。

```
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
```

响应包括身份验证令牌。

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

- a. 将响应中的身份验证令牌另存为 MYTOKEN。

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

您现在可以使用 MYTOKEN 对于其他请求、类似于未使用SSO时使用API的方式。

## 如果启用了单点登录，请注销 API

如果已启用单点登录（Single Sign-On，SSO），则必须对一系列 API 请求进行问题描述，才能注销网络管理 API 或租户管理 API。如果您使用 PingFederate 作为 SSO 身份提供程序，则以下说明适用

关于此任务

如果需要、您可以从组织的单点注销页面注销、以注销StorageGRID API。或者，您也可以从 StorageGRID 触发单点注销（SLO），这需要有效的 StorageGRID 令牌。

## 步骤

1. 要生成签名注销请求、请将`cookie "sso=true "`传递到SLO API:

```
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
```

返回注销 URL :

```
{  
  "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. 保存注销 URL 。

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

3. 向注销 URL 发送请求以触发 SLO 并重定向回 StorageGRID 。

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

返回 302 响应。此重定向位置不适用于纯 API 注销。

```
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. 删除 StorageGRID 承载令牌。

删除 StorageGRID 承载令牌的工作方式与不使用 SSO 相同。如果未提供`cookie "sso=true "`、则用户将从StorageGRID中注销、而不会影响SSO状态。

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

答 204 No Content 响应指示用户现在已注销。

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

## 版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。