NetApp

Control access to StorageGRID

StorageGRID

NetApp
March 02, 2022

Table of Contents

Control access to StorageGRID

Change the provisioning passphrase

Use this procedure to change the StorageGRID provisioning passphrase. The passphrase is required for recovery, expansion, and maintenance procedures. The passphrase is also required to download Recovery Package backups that include the grid topology information, grid node console passwords, and encryption keys for the StorageGRID system.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have Maintenance or Root access permissions.
- You have the current provisioning passphrase.

About this task

The provisioning passphrase is required for many installation and maintenance procedures, and for downloading the Recovery Package. The provisioning passphrase is not listed in the `Passwords.txt` file. Make sure to document the provisioning passphrase and keep it in a safe and secure location.

Steps

1. Select **CONFIGURATION** > **Access control**> **Grid passwords**.
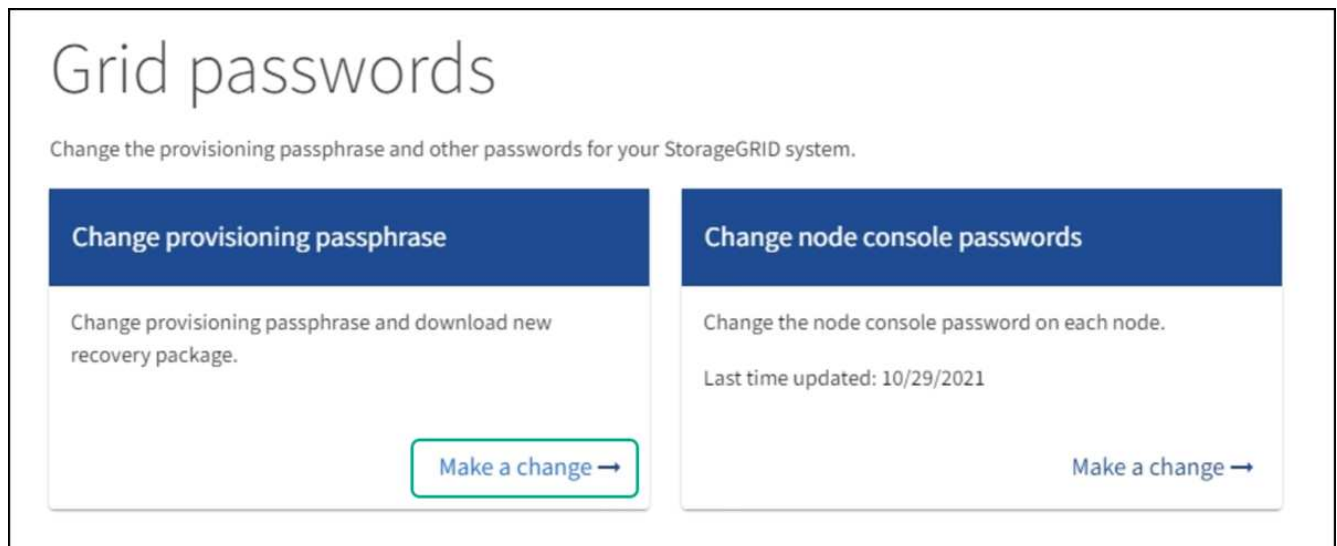
2. Select **Make a change** under **Change provisioning passphrase**.

3. Enter your current provisioning passphrase.

4. Enter the new passphrase. The passphrase must contain at least 8 and no more than 32 characters. Passphrases are case-sensitive.

5. Store the new provisioning passphrase in a secure location. It is required for installation, expansion, and maintenance procedures.

6. Re-enter the new passphrase, and select **Save**.

   The system displays a green success banner when the provisioning passphrase change is complete.

7. Select **Recovery Package**.

8. Enter the new provisioning passphrase to download the new Recovery Package.

   > ⚠ After changing the provisioning passphrase, you must immediately download a new Recovery Package. The Recovery Package file allows you to restore the system if a failure occurs.

Change node console passwords

Each node in your grid has a unique node console password, which you need to log in to the node. Use these steps to change each unique node console password for each node in your grid.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Maintenance or Root access permission.
- You have the current provisioning passphrase.

About this task
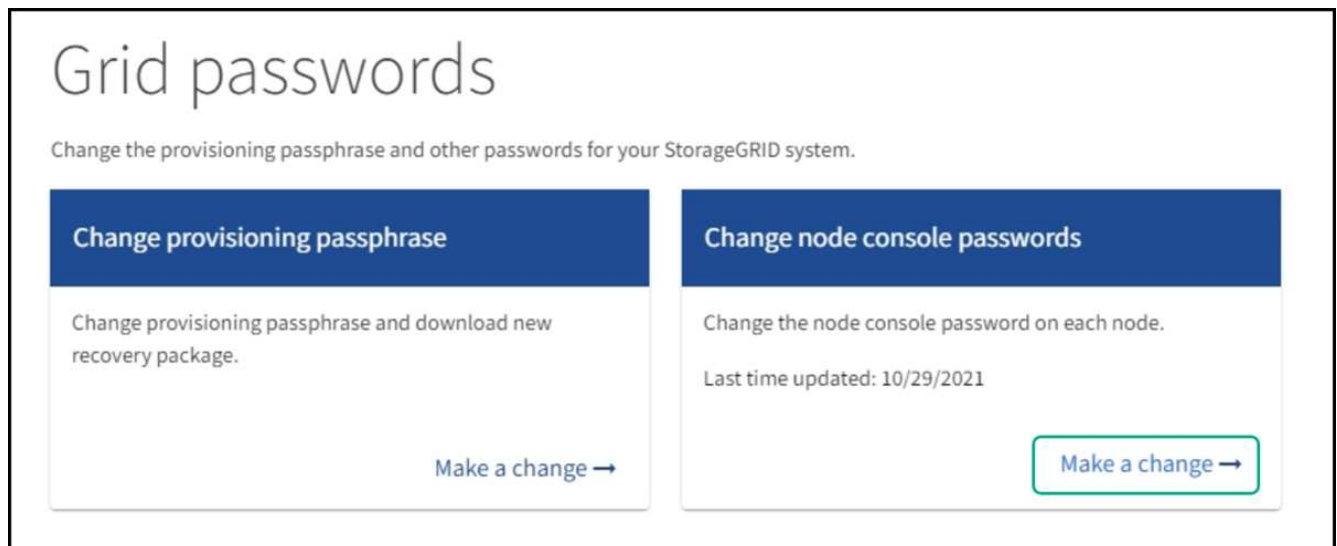
Use the node console password to log in to a node as "admin" using SSH, or to the root user on a VM/physical console connection. The change node console password process creates new passwords for each node in your grid and stores the passwords in an updated `Passwords.txt` file in the Recovery Package. The passwords are listed in the Password column in the Passwords.txt file.

> ℹ️ There are separate SSH access passwords for the SSH keys used for communication between nodes. The SSH access passwords are not changed by this procedure.

Access the wizard

1. Select **CONFIGURATION** > **Access control** > **Grid passwords**.

2. Select **Make a change** under **Change node console passwords**.

Enter the provisioning passphrase

1. Enter your provisioning passphrase.

2. Select **Continue**.

Download the current Recovery Package

1. Select **Download recovery package**.

   You can use the old passwords in the current Recovery Package if the password change process fails for any node.

2. Copy the Recovery Package file (.zip) to two safe, secure, and separate locations.

   ⚠️ The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

3. Select **Continue**.

Change node console passwords

1. Select **Yes** to confirm you want to change the node console passwords.
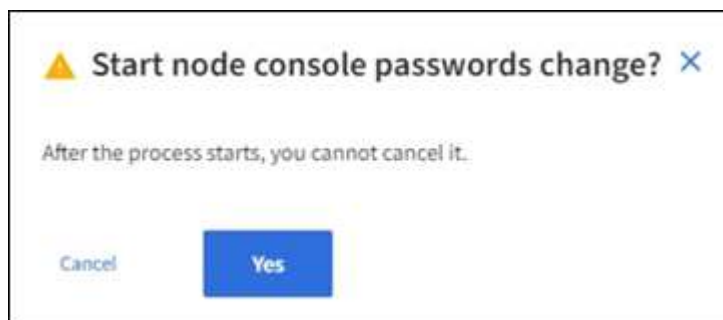
When you select **Yes**, a new Recovery Package is generated with the new passwords. It might take a few minutes to generate the new Recovery Package with the new passwords.

When you select **Cancel** you are returned to the previous page.

2. Select **Download new recovery package**.

Change node console passwords

Each node in your grid has a unique node console password, which you need to log into the node. Use these steps to change the node console password for each node in your grid. The passwords are stored in the recovery package. After you have changed the node console passwords, you must download the updated recovery package with the new node console passwords. **Note**: The SSH access passwords for SSH keys are not changed by this procedure.

✓ Provide provisioning passphrase ——— ✓ Download recovery package ——— **3** Change node console passwords

Download the new recovery package, which contains the new node console passwords. Save this file with a new name. Do not overwrite the old recovery package.

Download new recovery package

Have you downloaded the new recovery package successfully and verified the content?

☐ Yes, I have downloaded the new recovery package successfully and verified the content.

Select **Change node console passwords** to change node console passwords on all nodes.

Change node console passwords

3. When the download completes:

   a. Open the .zip file.

   b. Extract the contents of the .zip file.

   c. Confirm you can open the `Passwords.txt` file and that the contents are readable.

4. Copy the new Recovery Package file (.zip) to two safe, secure, and separate locations.

   ⚠️   Do not overwrite the old Recovery Package.

   You should either just view the `Passwords.txt` file, or if that is not possible, delete the extracted `Passwords.txt` file before copying the Recovery Package to the two separate secure locations. The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

5. Select the check box to indicate you have downloaded the new Recovery Package and verified the content.

6. Select **Change node console passwords** and wait for all node passwords to be updated. This might take a few minutes.

   If passwords are changed for all nodes, a green success banner appears. Go to the next step.

   If there is an error during the update process, a banner message lists the number of nodes that failed to have their passwords changed. The system will automatically retry the process on any node that failed to have its password changed. If the process ends with some nodes still not having a changed password, the **Retry** button appears.

   If the password update failed for one or more nodes:

a. Review the error messages listed in the table.

b. Resolve the issues.

c. Select **Retry**.

> ⓘ Retrying only changes the node console passwords on the nodes that failed during previous password change attempts.

7. After node console passwords have been changed for all nodes, delete the old Recovery Package.

8. Optionally, use the **Recovery package** link to download an additional copy of the new Recovery Package.

Control access through firewalls

When you want to control access through firewalls, you open or close specific ports at the external firewall.

Control access at the external firewall

You can control access to the user interfaces and APIs on StorageGRID Admin Nodes by opening or closing specific ports at the external firewall. For example, you might want to prevent tenants from being able to connect to the Grid Manager at the firewall, in addition to using other methods to control system access.

Port	Description	If port is open…
443	Default HTTPS port for Admin Nodes	Web browsers and management API clients can access the Grid Manager, the Grid Management API, the Tenant Manager, and the Tenant Management API. **Note:** Port 443 is also used for some internal traffic.
8443	Restricted Grid Manager port on Admin Nodes	• Web browsers and management API clients can access the Grid Manager and the Grid Management API using HTTPS. • Web browsers and management API clients cannot access the Tenant Manager or the Tenant Management API. • Requests for internal content will be rejected.
9443	Restricted Tenant Manager port on Admin Nodes	• Web browsers and management API clients can access the Tenant Manager and the Tenant Management API using HTTPS. • Web browsers and management API clients cannot access the Grid Manager or the Grid Management API. • Requests for internal content will be rejected.

(i) Single sign-on (SSO) is not available on the restricted Grid Manager or Tenant Manager ports. You must use the default HTTPS port (443) if you want users to authenticate with single sign-on.

Related information

- Sign in to the Grid Manager

- Create tenant account

- External communications

Use identity federation

Using identity federation makes setting up groups and users faster, and it allows users to sign in to StorageGRID using familiar credentials.

Configure identity federation for Grid Manager

You can configure identity federation in the Grid Manager if you want admin groups and users to be managed in another system such as Active Directory, Azure Active Directory (Azure AD), OpenLDAP, or Oracle Directory Server.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.

- You have specific access permissions.

- You are using Active Directory, Azure AD, OpenLDAP, or Oracle Directory Server as the identity provider.

  (i) If you want to use an LDAP v3 service that is not listed, contact technical support.

- If you plan to use OpenLDAP, you must configure the OpenLDAP server. See Guidelines for configuring an OpenLDAP server.

- If you plan to enable single sign-on (SSO), you have reviewed the requirements for using single sign-on.

- If you plan to use Transport Layer Security (TLS) for communications with the LDAP server, the identity provider is using TLS 1.2 or 1.3. See Supported ciphers for outgoing TLS connections.

About this task

You can configure an identity source for the Grid Manager if you want to import groups from another system such as Active Directory, Azure AD, OpenLDAP, or Oracle Directory Server. You can import the following types of groups:

- Admin groups. The users in admin groups can sign in to the Grid Manager and perform tasks, based on the management permissions assigned to the group.

- Tenant user groups for tenants that do not use their own identity source. Users in tenant groups can sign in to the Tenant Manager and perform tasks, based on the permissions assigned to the group in the Tenant Manager. See Create tenant account and Use a tenant account for details.

Enter the configuration

1. Select **CONFIGURATION** > **Access control** > **Identity federation**.

2. Select **Enable identity federation**.

3. In the LDAP service type section, select the type of LDAP service you want to configure.

Select **Other** to configure values for an LDAP server that uses Oracle Directory Server.

4. If you selected **Other**, complete the fields in the LDAP Attributes section. Otherwise, go to the next step.

   ○ **User Unique Name**: The name of the attribute that contains the unique identifier of an LDAP user. This attribute is equivalent to `sAMAccountName` for Active Directory and `uid` for OpenLDAP. If you are configuring Oracle Directory Server, enter `uid`.

   ○ **User UUID**: The name of the attribute that contains the permanent unique identifier of an LDAP user. This attribute is equivalent to `objectGUID` for Active Directory and `entryUUID` for OpenLDAP. If you are configuring Oracle Directory Server, enter `nsuniqueid`. Each user's value for the specified attribute must be a 32-digit hexadecimal number in either 16-byte or string format, where hyphens are ignored.

   ○ **Group Unique Name**: The name of the attribute that contains the unique identifier of an LDAP group. This attribute is equivalent to `sAMAccountName` for Active Directory and `cn` for OpenLDAP. If you are configuring Oracle Directory Server, enter `cn`.

   ○ **Group UUID**: The name of the attribute that contains the permanent unique identifier of an LDAP group. This attribute is equivalent to `objectGUID` for Active Directory and `entryUUID` for OpenLDAP. If you are configuring Oracle Directory Server, enter `nsuniqueid`. Each group's value for the specified attribute must be a 32-digit hexadecimal number in either 16-byte or string format, where hyphens are ignored.

5. For all LDAP service types, enter the required LDAP server and network connection information in the Configure LDAP server section.

   ○ **Hostname**: The fully qualified domain name (FQDN) or IP address of the LDAP server.

   ○ **Port**: The port used to connect to the LDAP server.

   > The default port for STARTTLS is 389, and the default port for LDAPS is 636. However, you can use any port as long as your firewall is configured correctly.

   ○ **Username**: The full path of the distinguished name (DN) for the user that will connect to the LDAP server.

   For Active Directory, you can also specify the Down-Level Logon Name or the User Principal Name.

   The specified user must have permission to list groups and users and to access the following attributes:

     ▪ `sAMAccountName` or `uid`

     ▪ `objectGUID`, `entryUUID`, or `nsuniqueid`

- cn

- `memberOf` or `isMemberOf`

- **Active Directory**: `objectSid, primaryGroupID, userAccountControl,` and `userPrincipalName`

- **Azure**: `accountEnabled` and `userPrincipalName`

- **Password**: The password associated with the username.

- **Group Base DN**: The full path of the distinguished name (DN) for an LDAP subtree you want to search for groups. In the Active Directory example (below), all groups whose Distinguished Name is relative to the base DN (DC=storagegrid,DC=example,DC=com) can be used as federated groups.

  > The **Group unique name** values must be unique within the **Group Base DN** they belong to.

- **User Base DN**: The full path of the distinguished name (DN) of an LDAP subtree you want to search for users.

  > The **User unique name** values must be unique within the **User Base DN** they belong to.

- **Bind username format** (optional): The default username pattern StorageGRID should use if the pattern cannot be determined automatically.

  Providing **Bind username format** is recommended because it can allow users to sign in if StorageGRID is unable to bind with the service account.

  Enter one of these patterns:

  - **UserPrincipalName pattern (Active Directory and Azure)**: `[USERNAME]@example.com`

  - **Down-level logon name pattern (Active Directory and Azure)**: `example\[USERNAME]`

  - **Distinguished name pattern**: `CN=[USERNAME],CN=Users,DC=example,DC=com`

    Include **[USERNAME]** exactly as written.

6. In the Transport Layer Security (TLS) section, select a security setting.

   - **Use STARTTLS**: Use STARTTLS to secure communications with the LDAP server. This is the recommended option for Active Directory, OpenLDAP, or Other, but this option is not supported for Azure.

   - **Use LDAPS**: The LDAPS (LDAP over SSL) option uses TLS to establish a connection to the LDAP server. You must select this option for Azure.

   - **Do not use TLS**: The network traffic between the StorageGRID system and the LDAP server will not be secured. This option is not supported for Azure.

     > Using the **Do not use TLS** option is not supported if your Active Directory server enforces LDAP signing. You must use STARTTLS or LDAPS.

7. If you selected STARTTLS or LDAPS, choose the certificate used to secure the connection.

   - **Use operating system CA certificate**: Use the default Grid CA certificate installed on the operating system to secure connections.

- **Use custom CA certificate**: Use a custom security certificate.

    If you select this setting, copy and paste the custom security certificate into the CA certificate text box.

Test the connection and save the configuration

After entering all values, you must test the connection before you can save the configuration. StorageGRID verifies the connection settings for the LDAP server and the bind username format, if you provided one.

1. Select **Test connection**.

2. If you did not provide a bind username format:

    - A "Test connection successful" message appears if the connection settings are valid. Select **Save** to save the configuration.

    - A "test connection could not be established" message appears if the connection settings are invalid. Select **Close**. Then, resolve any issues and test the connection again.

3. If you provided a bind username format, enter the username and password of a valid federated user.

    For example, enter your own username and password. Do not include any special characters in the username, such as @ or /.

Test Connection ×

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

> myusername

The username of a federated user.

Test password

> ⦁⦁⦁⦁⦁⦁⦁⦁⦁⦁⦁ 👁

Cancel   **Test Connection**

- A "Test connection successful" message appears if the connection settings are valid. Select **Save** to save the configuration.

- An error message appears if the connection settings, bind username format, or test username and password are invalid. Resolve any issues and test the connection again.

Force synchronization with the identity source

The StorageGRID system periodically synchronizes federated groups and users from the identity source. You can force synchronization to start if you want to enable or restrict user permissions as quickly as possible.

Steps

1. Go to the Identity federation page.

2. Select **Sync server** at the top of the page.

The synchronization process might take some time depending on your environment.

(i) The **Identity federation synchronization failure** alert is triggered if there is an issue synchronizing federated groups and users from the identity source.

Disable identity federation

You can temporarily or permanently disable identity federation for groups and users. When identity federation is disabled, there is no communication between StorageGRID and the identity source. However, any settings you have configured are retained, allowing you to easily reenable identity federation in the future.

About this task

Before you disable identity federation, you should be aware of the following:

- Federated users will be unable to sign in.
- Federated users who are currently signed in will retain access to the StorageGRID system until their session expires, but they will be unable to sign in after their session expires.
- Synchronization between the StorageGRID system and the identity source will not occur, and alerts or alarms will not be raised for accounts that have not been synchronized.
- The **Enable identity federation** check box is disabled if single sign-on (SSO) is set to **Enabled** or **Sandbox Mode**. The SSO Status on the Single Sign-on page must be **Disabled** before you can disable identity federation. See Disable single sign-on.

Steps

1. Go to the Identity federation page.
2. Uncheck the **Enable identity federation** check box.

Guidelines for configuring an OpenLDAP server

If you want to use an OpenLDAP server for identity federation, you must configure specific settings on the OpenLDAP server.

(i) For identity sources that are not ActiveDirectory or Azure, StorageGRID will not automatically block S3 access to users who are disabled externally. To block S3 access, delete any S3 keys for the user and remove the user from all groups.

Memberof and refint overlays

The memberof and refint overlays should be enabled. For more information, see the instructions for reverse group membership maintenance in the OpenLDAP documentation: Version 2.4 Administrator's Guide.

Indexing

You must configure the following OpenLDAP attributes with the specified index keywords:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`

- `olcDbIndex: entryUUID eq`

In addition, ensure the fields mentioned in the help for Username are indexed for optimal performance.

See the information about reverse group membership maintenance in the OpenLDAP documentation: Version 2.4 Administrator's Guide.

Manage admin groups

You can create admin groups to manage the security permissions for one or more admin users. Users must belong to a group to be granted access to the StorageGRID system.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have specific access permissions.
- If you plan to import a federated group, you have configured identity federation and the federated group already exists in the configured identity source.

Create an admin group

Admin groups allow you to determine which users can access which features and operations in the Grid Manager and the Grid Management API.

Access the wizard

1. Select **CONFIGURATION** > **Access control** > **Admin groups**.
2. Select **Create group**.

Choose a group type

You can create a local group or import a federated group.

- Create a local group if you want to assign permissions to local users.
- Create a federated group to import users from the identity source.

Local group

1. Select **Local group**.

2. Enter a display name for the group, which you can update later as required. For example, "Maintenance Users" or "ILM Administrators."

3. Enter a unique name for the group, which you cannot update later.

4. Select **Continue**.

Federated group

1. Select **Federated group**.

2. Enter the name of the group you want to import, exactly as it appears in the configured identity source.

   ◦ For Active Directory and Azure, use the sAMAccountName.

   ◦ For OpenLDAP, use the CN (Common Name).

   ◦ For another LDAP, use the appropriate unique name for the LDAP server.

3. Select **Continue**.

Manage group permissions

1. For **Access mode**, select whether users in the group can change settings and perform operations in the Grid Manager and the Grid Management API or whether they can only view settings and features.

   ◦ **Read-write** (default): Users can change settings and perform the operations allowed by their management permissions.

   ◦ **Read-only**: Users can only view settings and features. They cannot make any changes or perform any operations in the Grid Manager or Grid Management API. Local read-only users can change their own passwords.

   > ⓘ   If a user belongs to multiple groups and any group is set to **Read-only**, the user will have read-only access to all selected settings and features.

2. Select one or more Group permissions.

   You must assign at least one permission to each group; otherwise, users belonging to the group will not be able to sign in to StorageGRID.

3. If you are creating a local group, select **Continue**. If you are creating a federated group, select **Create group** and **Finish**.

Add users (local groups only)

1. Optionally, select one or more local users for this group.

   If you have not yet created local users, you can save the group without adding users. You can add this group to the user on the Users page. See Manage users for details.

2. Select **Create group** and **Finish**.

View and edit admin groups

You can view details for existing groups, modify a group, or duplicate a group.

- To view basic information for all groups, review the table on the Groups page.
- To view all details for a specific group or to edit a group, use the **Actions** menu or the details page.

Task	Actions menu	Details page
View group details	a. Select the check box for the group. b. Select **Actions** > **View group details**.	Select the group name in the table.
Edit display name (local groups only)	a. Select the check box for the group. b. Select **Actions** > **Edit group name**. c. Enter the new name. d. Select **Save changes**.	a. Select the group name to display the details. b. Select the edit icon ✏. c. Enter the new name. d. Select **Save changes**.
Edit access mode or permissions	a. Select the check box for the group. b. Select **Actions** > **View group details**. c. Optionally, change the group's Access mode. d. Optionally, select or unselect Group permissions. e. Select **Save changes**.	a. Select the group name to display the details. b. Optionally, change the group's Access mode. c. Optionally, select or unselect Group permissions. d. Select **Save changes**.

Duplicate a group

1. Select the check box for the group.
2. Select **Actions** > **Duplicate group**.
3. Complete the Duplicate group wizard.

Delete a group

You can delete an admin group when you want to remove the group from the system, and remove all permissions associated with the group. Deleting an admin group removes any users from the group, but does not delete the users.

1. From the Groups page, select the check box for each group you want to remove.
2. Select **Actions** > **Delete group**.
3. Select **Delete groups**.

Group permissions

When creating admin user groups, you select one or more permissions to control access to specific features of the Grid Manager. You can then assign each user to one or more of these admin groups to determine which tasks that user can perform.

You must assign at least one permission to each group; otherwise, users belonging to that group will not be able to sign in to the Grid Manager or the Grid Management API.

By default, any user who belongs to a group that has at least one permission can perform the following tasks:

- Sign in to the Grid Manager
- View the Dashboard
- View the Nodes pages
- Monitor grid topology
- View current and resolved alerts
- View current and historical alarms (legacy system)
- Change their own password (local users only)
- View certain information on the Configuration and Maintenance pages

Interaction between permissions and Access mode

For all permissions, the group's **Access mode** setting determines whether users can change settings and perform operations or whether they can only view the related settings and features. If a user belongs to multiple groups and any group is set to **Read-only**, the user will have read-only access to all selected settings and features.

The following sections describe the permissions you can assign when creating or editing an admin group. Any functionality not explicitly mentioned requires the **Root access** permission.

Root access

This permission provides access to all grid administration features.

Acknowledge alarms (legacy)

This permission provides access to acknowledge and respond to alarms (legacy system). All signed-in users can view current and historical alarms.

If you want a user to monitor grid topology and acknowledge alarms only, you should assign this permission.

Change tenant root password

This permission provides access to the **Change root password** option on the Tenants page, allowing you to control who can change the password for the tenant's local root user. This permission is also used for migrating S3 keys when the S3 key import feature is enabled. Users who do not have this permission cannot see the **Change root password** option.

> ⓘ To grant access to the Tenants page, which contains the **Change root password** option, also assign the **Tenant accounts** permission.

Grid topology page configuration

This permission provides access to the Configuration tabs on the **SUPPORT** > **Tools** > **Grid topology** page.

ILM

This permission provides access to the following **ILM** menu options:

- Rules
- Policies
- Erasure coding
- Regions
- Storage pools

> ⓘ Users must have the **Other grid configuration** and **Grid topology page configuration** permissions to manage storage grades.

Maintenance

Users must have the Maintenance permission to use these options:

- **CONFIGURATION** > **Access control**:
  - Grid passwords
- **MAINTENANCE** > **Tasks**:
  - Decommission
  - Expansion
  - Object existence check
  - Recovery
- **MAINTENANCE** > **System**:
  - Recovery package
  - Software update
- **SUPPORT** > **Tools**:
  - Logs

Users who do not have the Maintenance permission can view, but not edit, these pages:

- **MAINTENANCE** > **Network**:
  - DNS servers
  - Grid Network
  - NTP servers
- **MAINTENANCE** > **System**:
  - License
- **CONFIGURATION** > **Security**:
  - Certificates

◦ Domain names

- **CONFIGURATION** > **Monitoring**:

  ◦ Audit and syslog server

Manage alerts

This permission provides access to options for managing alerts. Users must have this permission to manage silences, alert notifications, and alert rules.

Metrics query

This permission provides access to the **SUPPORT** > **Tools** > **Metrics** page. This permission also provides access to custom Prometheus metrics queries using the **Metrics** section of the Grid Management API.

Object metadata lookup

This permission provides access to the **ILM** > **Object metadata lookup** page.

Other grid configuration

This permission provides access to additional grid configuration options.

> (i) To see these additional options, users must also have the **Grid topology page configuration** permission.

- **ILM**:

  ◦ Storage grades

- **CONFIGURATION** > **Network**:

  ◦ Link cost

- **CONFIGURATION** > **System**:

  ◦ Display options

  ◦ Grid options

  ◦ Storage options

- **SUPPORT** > **Alarms (legacy)**:

  ◦ Custom events

  ◦ Global alarms

  ◦ Legacy email setup

Storage appliance administrator

This permission provides access to the E-Series SANtricity System Manager on storage appliances through the Grid Manager.

Tenant accounts

This permission provides access to the Tenants page, where you can create, edit, and remove tenant accounts. This permission also allows users to view existing traffic classification policies.

Deactivate features with the API

You can use the Grid Management API to completely deactivate certain features in the StorageGRID system. When a feature is deactivated, no one can be assigned permissions to perform the tasks related to that feature.

About this task

The Deactivated Features system allows you to prevent access to certain features in the StorageGRID system. Deactivating a feature is the only way to prevent the root user or users who belong to admin groups with **Root access** permission from being able to use that feature.

To understand how this functionality might be useful, consider the following scenario:

Company A is a service provider who leases the storage capacity of their StorageGRID system by creating tenant accounts. To protect the security of their leaseholders' objects, Company A wants to ensure that its own employees can never access any tenant account after the account has been deployed.

*Company A can accomplish this goal by using the Deactivate Features system in the Grid Management API. By completely deactivating the **Change tenant root password** feature in the Grid Manager (both the UI and the API), Company A can ensure that no Admin user—including the root user and users belonging to groups with the **Root access** permission—can change the password for any tenant account's root user.*

Steps

1. Access the Swagger documentation for the Grid Management API. See Use the Grid Management API.

2. Locate the Deactivate Features endpoint.

3. To deactivate a feature, such as Change tenant root password, send a body to the API like this:

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   When the request is complete, the Change tenant root password feature is disabled. The **Change tenant root password** management permission no longer appears in the user interface, and any API request that attempts to change the root password for a tenant will fail with "403 Forbidden."

Reactivate deactivated features

By default, you can use the Grid Management API to reactivate a feature that has been deactivated. However, if you want to prevent deactivated features from ever being reactivated, you can deactivate the **activateFeatures** feature itself.

> ⚠ The **activateFeatures** feature cannot be reactivated. If you decide to deactivate this feature, be aware that you will permanently lose the ability to reactivate any other deactivated features. You must contact technical support to restore any lost functionality.

Steps

1. Access the Swagger documentation for the Grid Management API.

2. Locate the Deactivate Features endpoint.

3. To reactivate all features, send a body to the API like this:

   ```
   { "grid": null }
   ```

When this request is complete, all features, including the Change tenant root password feature, are reactivated. The **Change tenant root password** management permission now appears in the user interface, and any API request that attempts to change the root password for a tenant will succeed, assuming the user has the **Root access** or **Change tenant root password** management permission.

> (i) The previous example causes *all* deactivated features to be reactivated. If other features have been deactivated that should remain deactivated, you must explicitly specify them in the PUT request. For example, to reactivate the Change tenant root password feature and continue to deactivate the Alarm acknowledgment feature, send this PUT request:
>
> `{ "grid": { "alarmAcknowledgment": true } }`

Manage users

You can view local and federated users. You can also create local users and assign them to local admin groups to determine which Grid Manager features these users can access.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have specific access permissions.

Create a local user

You can create one or more local users and assign each user to one or more local groups. The group's permissions control which Grid Manager and Grid Management API features the user can access.

You can create local users only. Use the external identity source to manage federated users and groups.

The Grid Manager includes one predefined local user, named "root." You cannot remove the root user.

> (i) If single sign-on (SSO) is enabled, local users cannot sign in to StorageGRID.

Access the wizard

1. Select **CONFIGURATION** > **Access control** > **Admin users**.
2. Select **Create user**.

Enter user credentials

1. Enter the user's full name, a unique username, and a password.
2. Optionally, select **Yes** if this user should not have access to the Grid Manager or Grid Management API.
3. Select **Continue**.

Assign to groups

1. Optionally, assign the user to one or more groups to determine the user's permissions.

   If you have not yet created groups, you can save the user without selecting groups. You can add this user to a group on the Groups page.

If a user belongs to multiple groups, the permissions are cumulative. See Manage admin groups for details.

2. Select **Create user** and select **Finish**.

View and edit local users

You can view details for existing local and federated users. You can modify a local user to change the user's full name, password, or group membership. You can also temporarily prevent a user from accessing the Grid Manager and the Grid Management API.

You can edit local users only. Use the external identity source to manage federated users.

- To view basic information for all local and federated users, review the table on the Users page.
- To view all details for a specific user, edit a local user, or change a local user's password, use the **Actions** menu or the details page.

Any edits are applied the next time the user signs out and then signs back in to the Grid Manager.

> (i) Local users can change their own passwords using the **Change Password** option in the Grid Manager banner.

Task	Actions menu	Details page
View user details	a. Select the check box for the user. b. Select **Actions** > **View user details**.	Select the user's name in the table.
Edit full name (local users only)	a. Select the check box for the user. b. Select **Actions** > **Edit full name**. c. Enter the new name. d. Select **Save changes**.	a. Select the user's name to display the details. b. Select the edit icon ✏. c. Enter the new name. d. Select **Save changes**.
Deny or allow StorageGRID access	a. Select the check box for the user. b. Select **Actions** > **View user details**. c. Select the Access tab. d. Select **Yes** to prevent the user from signing in to the Grid Manager or the Grid Management API, or select **No** to allow the user to sign in. e. Select **Save changes**.	a. Select the user's name to display the details. b. Select the Access tab. c. Select **Yes** to prevent the user from signing in to the Grid Manager or the Grid Management API, or select **No** to allow the user to sign in. d. Select **Save changes**.
Change password (local users only)	a. Select the check box for the user. b. Select **Actions** > **View user details**. c. Select the Password tab. d. Enter a new password. e. Select **Change Password**.	a. Select the user's name to display the details. b. Select the Password tab. c. Enter a new password. d. Select **Change Password**.

Task	Actions menu	Details page
Change groups (local users only)	a. Select the check box for the user. b. Select **Actions** > **View user details**. c. Select the Groups tab. d. Optionally, select the link after a group name to view the group's details in a new browser tab. e. Select **Edit groups** to select different groups. f. Select **Save changes**.	a. Select the user's name to display the details. b. Select the Groups tab. c. Optionally, select the link after a group name to view the group's details in a new browser tab. d. Select **Edit groups** to select different groups. e. Select **Save changes**.

Duplicate a user

You can duplicate an existing user to create a new user with the same permissions.

1. Select the check box for the user.
2. Select **Actions** > **Duplicate user**.
3. Complete the Duplicate user wizard.

Delete a user

You can delete a local user to permanently remove that user from the system.

> (i) You cannot delete the root user.

1. From the Users page, select the check box for each user you want to remove.
2. Select **Actions** > **Delete user**.
3. Select **Delete user**.

Use single sign-on (SSO)

Configure single sign-on

When single sign-on (SSO) is enabled, users can only access the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API if their credentials are authorized using the SSO sign-in process implemented by your organization. Local users cannot sign in to StorageGRID.

How single sign-on works

The StorageGRID system supports single sign-on (SSO) using the Security Assertion Markup Language 2.0 (SAML 2.0) standard.

Before enabling single sign-on (SSO), review how the StorageGRID sign-in and sign-out processes are affected when SSO is enabled.
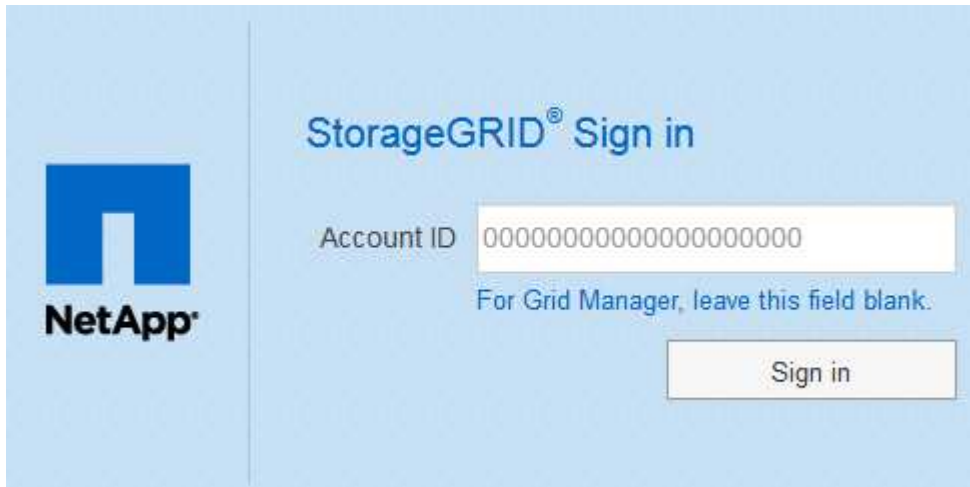
Sign in when SSO is enabled

When SSO is enabled and you sign in to StorageGRID, you are redirected to your organization's SSO page to validate your credentials.

Steps

1. Enter the fully qualified domain name or IP address of any StorageGRID Admin Node in a web browser.

   The StorageGRID Sign in page appears.

   ◦ If this is the first time you have accessed the URL on this browser, you are prompted for an account ID:

   ◦ If you have previously accessed either the Grid Manager or the Tenant Manager, you are prompted to select a recent account or to enter an account ID:

   > ⓘ The StorageGRID Sign in page is not shown when you enter the complete URL for a tenant account (that is, a fully qualified domain name or IP address followed by `/?accountId=20-digit-account-id`). Instead, you are immediately redirected to your organization's SSO sign-in page, where you can sign in with your SSO credentials.
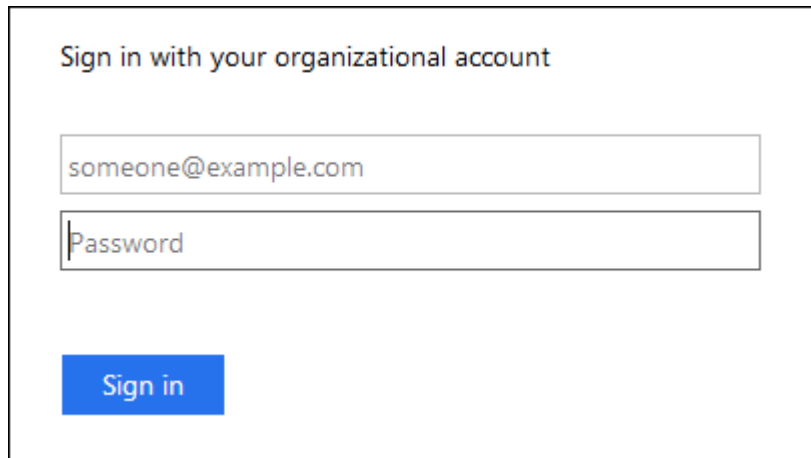
2. Indicate whether you want to access the Grid Manager or the Tenant Manager:

   ◦ To access the Grid Manager, leave the **Account ID** field blank, enter **0** as the account ID, or select **Grid Manager** if it appears in the list of recent accounts.

- To access the Tenant Manager, enter the 20-digit tenant account ID or select a tenant by name if it appears in the list of recent accounts.

3. Select **Sign in**

   StorageGRID redirects you to your organization's SSO sign-in page. For example:

   Sign in with your organizational account

   someone@example.com

   Password

   Sign in

4. Sign in with your SSO credentials.

   If your SSO credentials are correct:

   a. The identity provider (IdP) provides an authentication response to StorageGRID.

   b. StorageGRID validates the authentication response.

   c. If the response is valid and you belong to a federated group with StorageGRID access permissions, you are signed in to the Grid Manager or the Tenant Manager, depending on which account you selected.

   > **(i)** If the service account is inaccessible, you can still sign in, as long as you are an existing user that belongs to a federated group with StorageGRID access permissions.

5. Optionally, access other Admin Nodes, or access the Grid Manager or the Tenant Manager, if you have adequate permissions.

   You do not need to reenter your SSO credentials.

Sign out when SSO is enabled

When SSO is enabled for StorageGRID, what happens when you sign out depends on what you are signed in to and where you are signing out from.

Steps

1. Locate the **Sign Out** link in the top-right corner of the user interface.

2. Select **Sign Out**.

   The StorageGRID Sign in page appears. The **Recent Accounts** drop-down is updated to include **Grid Manager** or the name of the tenant, so you can access these user interfaces more quickly in the future.

If you are signed in to…	And you sign out from…	You are signed out of…
Grid Manager on one or more Admin Nodes	Grid Manager on any Admin Node	Grid Manager on all Admin Nodes **Note:** If you use Azure for SSO, it might take a few minutes to be signed out of all Admin Nodes.
Tenant Manager on one or more Admin Nodes	Tenant Manager on any Admin Node	Tenant Manager on all Admin Nodes
Both Grid Manager and Tenant Manager	Grid Manager	The Grid Manager only. You must also sign out of the Tenant Manager to sign out of SSO.
	Tenant Manager	The Tenant Manager only. You must also sign out of the Grid Manager to sign out of SSO.

> ⓘ The table summarizes what happens when you sign out if you are using a single browser session. If you are signed in to StorageGRID across multiple browser sessions, you must sign out of all browser sessions separately.

Requirements for using single sign-on

Before enabling single sign-on (SSO) for a StorageGRID system, review the requirements in this section.

Identity provider requirements

StorageGRID supports the following SSO identity providers (IdP):

- Active Directory Federation Service (AD FS)
- Azure Active Directory (Azure AD)
- PingFederate

You must configure identity federation for your StorageGRID system before you can configure an SSO identity provider. The type of LDAP service you use for identity federation controls which type of SSO you can implement.

Configured LDAP service type	Options for SSO identity provider
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

AD FS requirements

You can use any of the following versions of AD FS:

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> ⓘ   Windows Server 2016 should be using the KB3201845 update, or higher.

- AD FS 3.0, included with Windows Server 2012 R2 update, or higher.

Additional requirements

- Transport Layer Security (TLS) 1.2 or 1.3
- Microsoft .NET Framework, version 3.5.1 or higher

Server certificate requirements

By default, StorageGRID uses a management interface certificate on each Admin Node to secure access to the Grid Manager, the Tenant Manager, the Grid Management API, and the Tenant Management API. When you configure relying party trusts (AD FS), enterprise applications (Azure), or service provider connections (PingFederate) for StorageGRID, you use the server certificate as the signature certificate for StorageGRID requests.

If you have not already configured a custom certificate for the management interface, you should do so now. When you install a custom server certificate, it is used for all Admin Nodes, and you can use it in all StorageGRID relying party trusts, enterprise applications, or SP connections.

> ⓘ   Using an Admin Node's default server certificate in a relying party trust, enterprise application, or SP connection is not recommended. If the node fails and you recover it, a new default server certificate is generated. Before you can sign in to the recovered node, you must update the relying party trust, enterprise application, or SP connection with the new certificate.

You can access an Admin Node's server certificate by logging in to the command shell of the node and going to the `/var/local/mgmt-api` directory. A custom server certificate is named `custom-server.crt`. The node's default server certificate is named `server.crt`.

Port requirements

Single sign-on (SSO) is not available on the restricted Grid Manager or Tenant Manager ports. You must use the default HTTPS port (443) if you want users to authenticate with single sign-on. See Control access through firewalls.

Confirm federated users can sign in

Before you enable single sign-on (SSO), you must confirm that at least one federated user can sign in to the Grid Manager and in to the Tenant Manager for any existing tenant accounts.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.

- You have specific access permissions.

- You have already configured identity federation.

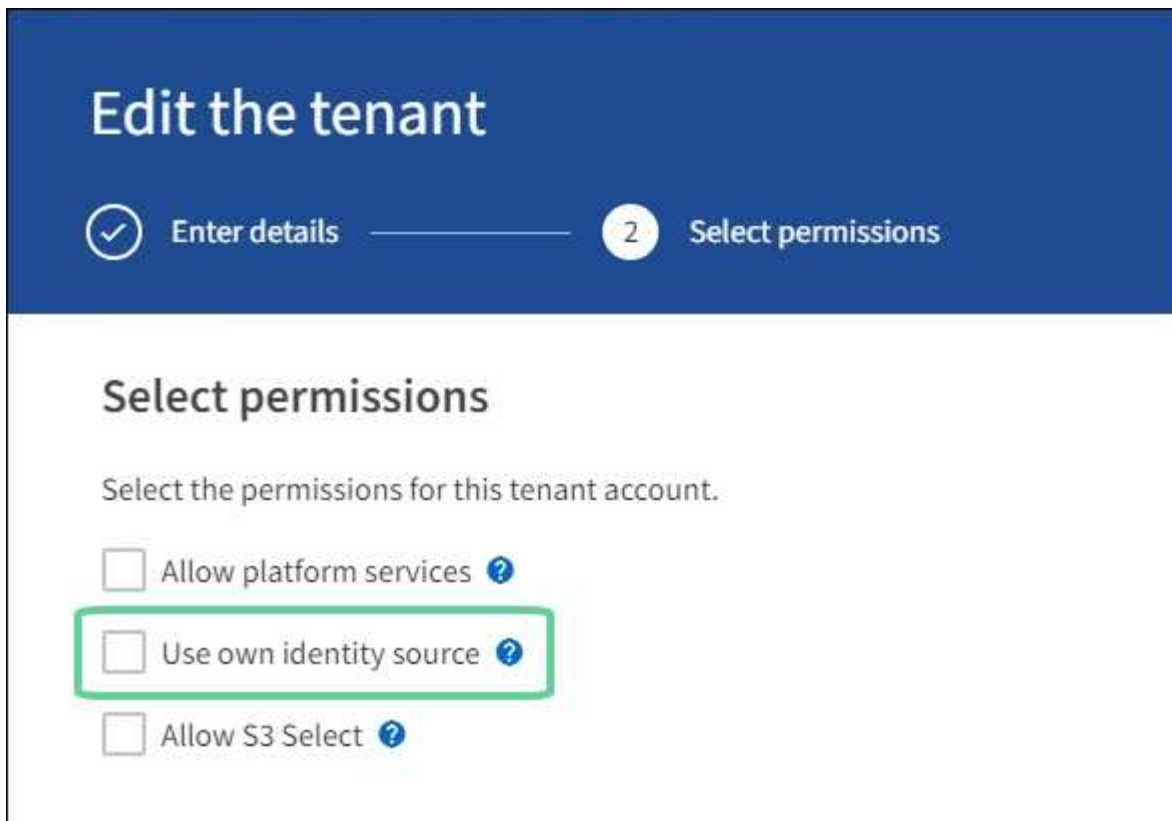**Steps**

1. If there are existing tenant accounts, confirm that none of the tenants is using its own identity source.

   > ⓘ When you enable SSO, an identity source configured in the Tenant Manager is overridden by the identity source configured in the Grid Manager. Users belonging to the tenant's identity source will no longer be able to sign in unless they have an account with the Grid Manager identity source.

   a. Sign in to the Tenant Manager for each tenant account.

   b. Select **ACCESS MANAGEMENT** > **Identity federation**.

   c. Confirm that the **Enable identity federation** check box is not selected.

   d. If it is, confirm that any federated groups that might be in use for this tenant account are no longer required, unselect the check box, and select **Save**.

2. Confirm that a federated user can access the Grid Manager:

   a. From Grid Manager, select **CONFIGURATION** > **Access control** > **Admin groups**.

   b. Ensure that at least one federated group has been imported from the Active Directory identity source and that it has been assigned the Root access permission.

   c. Sign out.

   d. Confirm you can sign back in to the Grid Manager as a user in the federated group.

3. If there are existing tenant accounts, confirm that a federated user who has Root access permission can sign in:

   a. From the Grid Manager, select **TENANTS**.

   b. Select the tenant account, and select **Actions** > **Edit**.

   c. On the Enter details tab, select **Continue**.

   d. If the **Use own identity source** check box is selected, uncheck the box and select **Save**.

The Tenant page appears.

   e. Select the tenant account, select **Sign in**, and sign in to the tenant account as the local root user.

   f. From the Tenant Manager, select **ACCESS MANAGEMENT** > **Groups**.

   g. Ensure that at least one federated group from the Grid Manager has been assigned the Root access permission for this tenant.

   h. Sign out.

   i. Confirm you can sign back in to the tenant as a user in the federated group.

Related information

- Requirements for using single sign-on
- Manage admin groups
- Use a tenant account

Use sandbox mode

You can use sandbox mode to configure and test single sign-on (SSO) before enabling it for all StorageGRID users. After SSO has been enabled, you can return to sandbox mode whenever you need to change or retest the configuration.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Root access permission.
- You have configured identity federation for your StorageGRID system.

- For the identity federation **LDAP service type**, you selected either Active Directory or Azure, based on the SSO identity provider you plan to use.

Configured LDAP service type	Options for SSO identity provider
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

About this task

When SSO is enabled and a user attempts to sign in to an Admin Node, StorageGRID sends an authentication request to the SSO identity provider. In turn, the SSO identity provider sends an authentication response back to StorageGRID, indicating whether the authentication request was successful. For successful requests:

- The response from Active Directory or PingFederate includes a universally unique identifier (UUID) for the user.

- The response from Azure includes a User Principal Name (UPN).

To allow StorageGRID (the service provider) and the SSO identity provider to communicate securely about user authentication requests, you must configure certain settings in StorageGRID. Next, you must use the SSO identity provider's software to create a relying party trust (AD FS), Enterprise Application (Azure) or Service Provider (PingFederate) for each Admin Node. Finally, you must return to StorageGRID to enable SSO.

Sandbox mode makes it easy to perform this back-and-forth configuration and to test all of your settings before you enable SSO. When you are using sandbox mode, users cannot sign in using SSO.

Access sandbox mode

1. Select **CONFIGURATION** > **Access control** > **Single sign-on**.

   The Single Sign-on page appears, with the **Disabled** option selected.

    ⓘ   If the SSO Status options do not appear, confirm you have configured the identity provider as the federated identity source. See Requirements for using single sign-on.

2. Select **Sandbox Mode**.

   The Identity Provider section appears.

Enter identity provider details

1. Select the **SSO type** from the drop-down list.
2. Complete the fields in the Identity Provider section based on the SSO type you selected.

Active Directory

   a. Enter the **Federation service name** for the identity provider, exactly as it appears in Active Directory Federation Service (AD FS).

> (i) To locate the federation service name, go to Windows Server Manager. Select **Tools** > **AD FS Management**. From the Action menu, select **Edit Federation Service Properties**. The Federation Service Name is shown in the second field.

   b. Specify which TLS certificate will be used to secure the connection when the identity provider sends SSO configuration information in response to StorageGRID requests.

- **Use operating system CA certificate**: Use the default CA certificate installed on the operating system to secure the connection.

- **Use custom CA certificate**: Use a custom CA certificate to secure the connection.

  If you select this setting, copy the text of the custom certificate and and paste it in the **CA Certificate** text box.

- **Do not use TLS**: Do not use a TLS certificate to secure the connection.

   c. In the Relying Party section, specify the **Relying party identifier** for StorageGRID. This value controls the name you use for each relying party trust in AD FS.

- For example, if your grid has only one Admin Node and you do not anticipate adding more Admin Nodes in the future, enter `SG` or `StorageGRID`.

- If your grid includes more than one Admin Node, include the string `[HOSTNAME]` in the identifier. For example, `SG-[HOSTNAME]`. This generates a table that shows the relying party identifier for each Admin Node in your system, based on the node's hostname.

> (i) You must create a relying party trust for each Admin Node in your StorageGRID system. Having a relying party trust for each Admin Node ensures that users can securely sign in to and out of any Admin Node.

   d. Select **Save**.

A green check mark appears on the **Save** button for a few seconds.
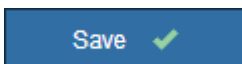
Azure

   a. Specify which TLS certificate will be used to secure the connection when the identity provider sends SSO configuration information in response to StorageGRID requests.

- **Use operating system CA certificate**: Use the default CA certificate installed on the operating system to secure the connection.

- **Use custom CA certificate**: Use a custom CA certificate to secure the connection.

  If you select this setting, copy the text of the custom certificate and and paste it in the **CA Certificate** text box.

◦ **Do not use TLS**: Do not use a TLS certificate to secure the connection.

b. In the Enterprise Application section, specify the **Enterprise application name** for StorageGRID. This value controls the name you use for each enterprise application in Azure AD.

◦ For example, if your grid has only one Admin Node and you do not anticipate adding more Admin Nodes in the future, enter `SG` or `StorageGRID`.

◦ If your grid includes more than one Admin Node, include the string `[HOSTNAME]` in the identifier. For example, `SG-[HOSTNAME]`. This generates a table that shows an enterprise application name for each Admin Node in your system, based on the node's hostname.

> (i) You must create an enterprise application for each Admin Node in your StorageGRID system. Having an enterprise application for each Admin Node ensures that users can securely sign in to and out of any Admin Node.

c. Follow the steps in Create enterprise applications in Azure AD to create an enterprise application for each Admin Node listed in the table.

d. From Azure AD, copy the federation metadata URL for each enterprise application. Then, paste this URL into the corresponding **Federation metadata URL** field in StorageGRID.

e. After you have copied and pasted a federation metadata URL for all Admin Nodes, select **Save**.

A green check mark appears on the **Save** button for a few seconds.

Save ✔
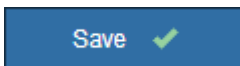
PingFederate

a. Specify which TLS certificate will be used to secure the connection when the identity provider sends SSO configuration information in response to StorageGRID requests.

◦ **Use operating system CA certificate**: Use the default CA certificate installed on the operating system to secure the connection.

◦ **Use custom CA certificate**: Use a custom CA certificate to secure the connection.

If you select this setting, copy the text of the custom certificate and and paste it in the **CA Certificate** text box.

◦ **Do not use TLS**: Do not use a TLS certificate to secure the connection.

b. In the Service Provider (SP) section, specify the **SP connection ID** for StorageGRID. This value controls the name you use for each SP connection in PingFederate.

◦ For example, if your grid has only one Admin Node and you do not anticipate adding more Admin Nodes in the future, enter `SG` or `StorageGRID`.

◦ If your grid includes more than one Admin Node, include the string `[HOSTNAME]` in the identifier. For example, `SG-[HOSTNAME]`. This generates a table that shows the SP connection ID for each Admin Node in your system, based on the node's hostname.

> (i) You must create an SP connection for each Admin Node in your StorageGRID system. Having an SP connection for each Admin Node ensures that users can securely sign in to and out of any Admin Node.

c. Specify the federation metadata URL for each Admin Node in the **Federation metadata URL** field.

Use the following format:

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection
ID>
```

d. Select **Save**.

A green check mark appears on the **Save** button for a few seconds.

Save ✔

Configure relying party trusts, enterprise applications, or SP connections

When the configuration is saved, the Sandbox mode confirmation notice appears. This notice confirms that sandbox mode is now enabled and provides overview instructions.

StorageGRID can remain in sandbox mode as long as required. However, when **Sandbox Mode** is selected on the Single Sign-on page, SSO is disabled for all StorageGRID users. Only local users can sign in.

Follow these steps to configure relying party trusts (Active Directory), complete enterprise applications (Azure), or configure SP connections (PingFederate).

Active Directory

1. Go to Active Directory Federation Services (AD FS).

2. Create one or more relying party trusts for StorageGRID, using each relying party identifier shown in the table on the StorageGRID Single Sign-on page.

   You must create one trust for each Admin Node shown in the table.

   For instructions, go to Create relying party trusts in AD FS.

Azure

1. From the Single sign-on page for the Admin Node you are currently signed in to, select the button to download and save the SAML metadata.

2. Then, for any other Admin Nodes in your grid, repeat these steps:

   a. Sign in to the node.

   b. Select **CONFIGURATION** > **Access control** > **Single sign-on**.

   c. Download and save the SAML metadata for that node.

3. Go to the Azure Portal.

4. Follow the steps in Create enterprise applications in Azure AD to upload the SAML metadata file for each Admin Node into its corresponding Azure enterprise application.

PingFederate

1. From the Single sign-on page for the Admin Node you are currently signed in to, select the button to download and save the SAML metadata.

2. Then, for any other Admin Nodes in your grid, repeat these steps:

   a. Sign in to the node.

   b. Select **CONFIGURATION** > **Access control** > **Single sign-on**.

   c. Download and save the SAML metadata for that node.

3. Go to PingFederate.

4. Create one or more service provider (SP) connections for StorageGRID. Use the SP connection ID for each Admin Node (shown in the table on the StorageGRID Single Sign-on page) and the SAML metadata you downloaded for that Admin Node.

   You must create one SP connection for each Admin Node shown in the table.

Test SSO connections

Before you enforce the use of single sign-on for your entire StorageGRID system, you should confirm that single sign-on and single logout are correctly configured for each Admin Node.

Active Directory

1. From the StorageGRID Single Sign-on page, locate the link in the Sandbox mode message.

   The URL is derived from the value you entered in the **Federation service name** field.
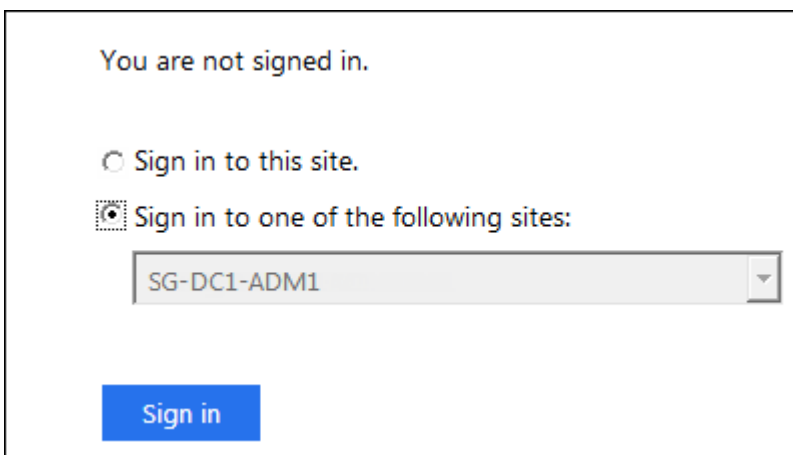

2. Select the link, or copy and paste the URL into a browser, to access your identity provider's sign-on page.

3. To confirm you can use SSO to sign in to StorageGRID, select **Sign in to one of the following sites**, select the relying party identifier for your primary Admin Node, and select **Sign in**.

4. Enter your federated username and password.

   ◦ If the SSO sign-in and logout operations are successful, a success message appears.

   ◦ If the SSO operation is unsuccessful, an error message appears. Fix the issue, clear the browser's cookies, and try again.

5. Repeat these steps to verify the SSO connection for each Admin Node in your grid.

Azure

1. Go to the Single sign-on page in the Azure portal.

2. Select **Test this application**.

3. Enter the credentials of a federated user.

   ◦ If the SSO sign-in and logout operations are successful, a success message appears.

   > ✔ Single sign-on authentication and logout test completed successfully.

   ◦ If the SSO operation is unsuccessful, an error message appears. Fix the issue, clear the browser's cookies, and try again.

4. Repeat these steps to verify the SSO connection for each Admin Node in your grid.

PingFederate

1. From the StorageGRID Single Sign-on page, select the first link in the Sandbox mode message.

   Select and test one link at a time.

2. Enter the credentials of a federated user.

   ◦ If the SSO sign-in and logout operations are successful, a success message appears.

   > ✔ Single sign-on authentication and logout test completed successfully.

   ◦ If the SSO operation is unsuccessful, an error message appears. Fix the issue, clear the browser's cookies, and try again.

3. Select the next link to verify the SSO connection for each Admin Node in your grid.

   If you see a Page Expired message, select the **Back** button in your browser and resubmit your credentials.

Enable single sign-on

When you have confirmed you can use SSO to sign in to each Admin Node, you can enable SSO for your entire StorageGRID system.

> ⓘ When SSO is enabled, all users must use SSO to access the Grid Manager, the Tenant Manager, the Grid Management API, and the Tenant Management API. Local users can no longer access StorageGRID.

1. Select **CONFIGURATION** > **Access control** > **Single sign-on**.

2. Change the SSO Status to **Enabled**.

3. Select **Save**.

4. Review the warning message, and select **OK**.

   Single sign-on is now enabled.

If you are using the Azure Portal and you access StorageGRID from the same computer you use to access Azure, ensure that the Azure Portal user is also an authorized StorageGRID user (a user in a federated group that has been imported into StorageGRID) or log out of the Azure Portal before attempting to sign in to StorageGRID.

Create relying party trusts in AD FS

You must use Active Directory Federation Services (AD FS) to create a relying party trust for each Admin Node in your system. You can create relying party trusts using PowerShell commands, by importing SAML metadata from StorageGRID, or by entering the data manually.

What you'll need

- You have configured single sign-on for StorageGRID and you selected **AD FS** as the SSO type.
- **Sandbox mode** is selected on the Single sign-on page in Grid Manager. See Use sandbox mode.
- You know the fully qualified domain name (or the IP address) and the relying party identifier for each Admin Node in your system. You can find these values in the Admin Nodes detail table on the StorageGRID Single Sign-on page.

You must create a relying party trust for each Admin Node in your StorageGRID system. Having a relying party trust for each Admin Node ensures that users can securely sign in to and out of any Admin Node.

- You have experience creating relying party trusts in AD FS, or you have access to the Microsoft AD FS documentation.
- You are using the AD FS Management snap-in, and you belong to the Administrators group.
- If you are creating the relying party trust manually, you have the custom certificate that was uploaded for the StorageGRID management interface, or you know how to log in to an Admin Node from the command shell.

About this task

These instructions apply to Windows Server 2016 AD FS. If you are using a different version of AD FS, you will notice slight differences in the procedure. See the Microsoft AD FS documentation if you have questions.

Create a relying party trust using Windows PowerShell

You can use Windows PowerShell to quickly create one or more relying party trusts.

Steps

1. From the Windows start menu, right-select the PowerShell icon, and select **Run as Administrator**.

2. At the PowerShell command prompt, enter the following command:

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - For *Admin_Node_Identifier*, enter the Relying Party Identifier for the Admin Node, exactly as it appears on the Single Sign-on page. For example, `SG-DC1-ADM1`.

   - For *Admin_Node_FQDN*, enter the fully qualified domain name for the same Admin Node. (If

necessary, you can use the node's IP address instead. However, if you enter an IP address here, be aware that you must update or recreate this relying party trust if that IP address ever changes.)

3. From Windows Server Manager, select **Tools** > **AD FS Management**.

   The AD FS management tool appears.

4. Select **AD FS** > **Relying Party Trusts**.

   The list of relying party trusts appears.

5. Add an Access Control Policy to the newly created relying party trust:

   a. Locate the relying party trust you just created.

   b. Right-click the trust, and select **Edit Access Control Policy**.

   c. Select an Access Control Policy.

   d. Select **Apply**, and select **OK**

6. Add a Claim Issuance Policy to the newly created Relying Party Trust:

   a. Locate the relying party trust you just created.

   b. Right-click the trust, and select **Edit claim issuance policy**.

   c. Select **Add rule**.

   d. On the Select Rule Template page, select **Send LDAP Attributes as Claims** from the list, and select **Next**.

   e. On the Configure Rule page, enter a display name for this rule.

      For example, **ObjectGUID to Name ID**.

   f. For the Attribute Store, select **Active Directory**.

   g. In the LDAP Attribute column of the Mapping table, type **objectGUID**.

   h. In the Outgoing Claim Type column of the Mapping table, select **Name ID** from the drop-down list.

   i. Select **Finish**, and select **OK**.

7. Confirm that the metadata was imported successfully.

   a. Right-click the relying party trust to open its properties.

   b. Confirm that the fields on the **Endpoints**, **Identifiers**, and **Signature** tabs are populated.

      If the metadata is missing, confirm that the Federation metadata address is correct, or simply enter the values manually.

8. Repeat these steps to configure a relying party trust for all of the Admin Nodes in your StorageGRID system.

9. When you are done, return to StorageGRID and test all relying party trusts to confirm they are configured correctly. See Use Sandbox mode for instructions.

Create a relying party trust by importing federation metadata

You can import the values for each relying party trust by accessing the SAML metadata for each Admin Node.

Steps

1. In Windows Server Manager, select **Tools**, and then select **AD FS Management**.

2. Under Actions, select **Add Relying Party Trust**.

3. On the Welcome page, choose **Claims aware**, and select **Start**.

4. Select **Import data about the relying party published online or on a local network**.

5. In **Federation metadata address (host name or URL)**, type the location of the SAML metadata for this Admin Node:

   ```
   https://Admin_Node_FQDN/api/saml-metadata
   ```

   For `Admin_Node_FQDN`, enter the fully qualified domain name for the same Admin Node. (If necessary, you can use the node's IP address instead. However, if you enter an IP address here, be aware that you must update or recreate this relying party trust if that IP address ever changes.)

6. Complete the Relying Party Trust wizard, save the relying party trust, and close the wizard.

   > (i) When entering the display name, use the Relying Party Identifier for the Admin Node, exactly as it appears on the Single Sign-on page in the Grid Manager. For example, `SG-DC1-ADM1`.

7. Add a claim rule:

   a. Right-click the trust, and select **Edit claim issuance policy**.

   b. Select **Add rule**:

   c. On the Select Rule Template page, select **Send LDAP Attributes as Claims** from the list, and select **Next**.

   d. On the Configure Rule page, enter a display name for this rule.

      For example, **ObjectGUID to Name ID**.

   e. For the Attribute Store, select **Active Directory**.

   f. In the LDAP Attribute column of the Mapping table, type **objectGUID**.

   g. In the Outgoing Claim Type column of the Mapping table, select **Name ID** from the drop-down list.

   h. Select **Finish**, and select **OK**.

8. Confirm that the metadata was imported successfully.

   a. Right-click the relying party trust to open its properties.

   b. Confirm that the fields on the **Endpoints**, **Identifiers**, and **Signature** tabs are populated.

      If the metadata is missing, confirm that the Federation metadata address is correct, or simply enter the values manually.

9. Repeat these steps to configure a relying party trust for all of the Admin Nodes in your StorageGRID system.

10. When you are done, return to StorageGRID and test all relying party trusts to confirm they are configured correctly. See Use Sandbox mode for instructions.

Create a relying party trust manually

If you choose not to import the data for the relying part trusts, you can enter the values manually.

Steps

1. In Windows Server Manager, select **Tools**, and then select **AD FS Management**.

2. Under Actions, select **Add Relying Party Trust**.

3. On the Welcome page, choose **Claims aware**, and select **Start**.

4. Select **Enter data about the relying party manually**, and select **Next**.

5. Complete the Relying Party Trust wizard:

   a. Enter a display name for this Admin Node.

      For consistency, use the Relying Party Identifier for the Admin Node, exactly as it appears on the Single Sign-on page in the Grid Manager. For example, `SG-DC1-ADM1`.

   b. Skip the step to configure an optional token encryption certificate.

   c. On the Configure URL page, select the **Enable support for the SAML 2.0 WebSSO protocol** check box.

   d. Type the SAML service endpoint URL for the Admin Node:

      `https://`*`Admin_Node_FQDN`*`/api/saml-response`

      For *`Admin_Node_FQDN`*, enter the fully qualified domain name for the Admin Node. (If necessary, you can use the node's IP address instead. However, if you enter an IP address here, be aware that you must update or recreate this relying party trust if that IP address ever changes.)

   e. On the Configure Identifiers page, specify the Relying Party Identifier for the same Admin Node:

      `Admin_Node_Identifier`

      For *`Admin_Node_Identifier`*, enter the Relying Party Identifier for the Admin Node, exactly as it appears on the Single Sign-on page. For example, `SG-DC1-ADM1`.

   f. Review the settings, save the relying party trust, and close the wizard.

      The Edit Claim Issuance Policy dialog box appears.

      > (i) If the dialog box does not appear, right-click the trust, and select **Edit claim issuance policy**.

6. To start the Claim Rule wizard, select **Add rule**:

   a. On the Select Rule Template page, select **Send LDAP Attributes as Claims** from the list, and select **Next**.

   b. On the Configure Rule page, enter a display name for this rule.

      For example, **ObjectGUID to Name ID**.

   c. For the Attribute Store, select **Active Directory**.

   d. In the LDAP Attribute column of the Mapping table, type **objectGUID**.

   e. In the Outgoing Claim Type column of the Mapping table, select **Name ID** from the drop-down list.

   f. Select **Finish**, and select **OK**.

7. Right-click the relying party trust to open its properties.

8. On the **Endpoints** tab, configure the endpoint for single logout (SLO):

   a. Select **Add SAML**.

   b. Select **Endpoint Type** > **SAML Logout**.

   c. Select **Binding** > **Redirect**.

   d. In the **Trusted URL** field, enter the URL used for single logout (SLO) from this Admin Node:

   ```
   https://Admin_Node_FQDN/api/saml-logout
   ```

   For `Admin_Node_FQDN`, enter the Admin Node's fully qualified domain name. (If necessary, you can use the node's IP address instead. However, if you enter an IP address here, be aware that you must update or recreate this relying party trust if that IP address ever changes.)

   e. Select **OK**.

9. On the **Signature** tab, specify the signature certificate for this relying party trust:

   a. Add the custom certificate:

      ▪ If you have the custom management certificate you uploaded to StorageGRID, select that certificate.

      ▪ If you do not have the custom certificate, log in to the Admin Node, go the `/var/local/mgmt-api` directory of the Admin Node, and add the `custom-server.crt` certificate file.

      Note: Using the Admin Node's default certificate (`server.crt`) is not recommended. If the Admin Node fails, the default certificate will be regenerated when you recover the node, and you will need to update the relying party trust.

   b. Select **Apply**, and select **OK**.

      The Relying Party properties are saved and closed.

10. Repeat these steps to configure a relying party trust for all of the Admin Nodes in your StorageGRID system.

11. When you are done, return to StorageGRID and test all relying party trusts to confirm they are configured correctly. See Use sandbox mode for instructions.

Create enterprise applications in Azure AD

You use Azure AD to create an enterprise application for each Admin Node in your system.

What you'll need

- You have started configuring single sign-on for StorageGRID and you selected **Azure** as the SSO type.
- **Sandbox mode** is selected on the Single sign-on page in Grid Manager. See Use sandbox mode.
- You have the **Enterprise application name** for each Admin Node in your system. You can copy these values from the Admin Node details table on the StorageGRID Single Sign-on page.

| | You must create an enterprise application for each Admin Node in your StorageGRID system. Having an enterprise application for each Admin Node ensures that users can securely sign in to and out of any Admin Node. |

- You have experience creating enterprise applications in Azure Active Directory.

- You have an Azure account with an active subscription.

- You have one of the following roles in the Azure account: Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the service principal.

Access Azure AD

1. Login to the Azure Portal.

2. Navigate to Azure Active Directory.

3. Select Enterprise applications.

Create enterprise applications and save StorageGRID SSO configuration

In order to save the SSO configuration for Azure in StorageGRID, you must use Azure to create an enterprise application for each Admin Node. You will copy the federation metadata URLs from Azure and paste them into the corresponding **Federation metadata URL** fields on the StorageGRID Single Sign-on page.

1. Repeat the following steps for each Admin Node.

   a. In the Azure Enterprise applications pane, select **New application**.

   b. Select **Create your own application**.

   c. For the name, enter the **Enterprise application name** you copied from the Admin Node details table on the StorageGRID Single Sign-on page.

   d. Leave the **Integrate any other application you don't find in the gallery (Non-gallery)** radio button selected.

   e. Select **Create**.

   f. Select the **Get started** link in the **2. Set up single sign on** box, or select the **Single sign-on** link in the left margin.

   g. Select the **SAML** box.

   h. Copy the **App Federation Metadata Url**, which you can find under **Step 3 SAML Signing Certificate**.

   i. Go to the StorageGRID Single Sign-on page, and paste the URL in the **Federation metadata URL** field that corresponds to the **Enterprise application name** you used.

2. After you have pasted a federation metadata URL for each Admin Node and made all other needed changes to the SSO configuration, select **Save** on the StorageGRID Single Sign-on page.

Download SAML metadata for every Admin Node

After the SSO configuration is saved, you can download a SAML metadata file for each Admin Node in your StorageGRID system.

Repeat these steps for each Admin Node:

1. Sign in to StorageGRID from the Admin Node.

2. Select **CONFIGURATION** > **Access control** > **Single sign-on**.

3. Select the button to download the SAML metadata for that Admin Node.

4. Save the file, which you will upload into Azure AD.

Upload SAML metadata to each enterprise application

After downloading a SAML metadata file for each StorageGRID Admin Node, perform the following steps in Azure AD:

1. Return to the Azure Portal.

2. Repeat these steps for each enterprise application:

   (i) You might need to refresh the Enterprise applications page to see applications you previously added in the list.

   a. Go to the Properties page for the enterprise application.

   b. Set **Assignment required** to **No** (unless you want to separately configure assignments).

   c. Go to the Single sign-on page.

   d. Complete the SAML configuration.

   e. Select the **Upload metadata file** button and select the SAML metadata file you downloaded for the corresponding Admin Node.

   f. After the file loads, select **Save** and then select **X** to close the pane. You are returned to the Set up Single Sign-On with SAML page.

3. Follow the steps in Use sandbox mode to test each application.

Create service provider (SP) connections in PingFederate

You use PingFederate to create a service provider (SP) connection for each Admin Node in your system. To speed up the process, you will import the SAML metadata from StorageGRID.

What you'll need

- You have configured single sign-on for StorageGRID and you selected **Ping Federate** as the SSO type.

- **Sandbox mode** is selected on the Single sign-on page in Grid Manager. See Use sandbox mode.

- You have the **SP connection ID** for each Admin Node in your system. You can find these values in the Admin Nodes detail table on the StorageGRID Single Sign-on page.

- You have downloaded the **SAML metadata** for each Admin Node in your system.

- You have experience creating SP connections in PingFederate Server.

- You have the Administrator's Reference Guide for PingFederate Server. The PingFederate documentation provides detailed step-by-step instructions and explanations.

- You have the Admin permission for PingFederate Server.

About this task

These instructions summarize how to configure PingFederate Server version 10.3 as an SSO provider for StorageGRID. If you are using another version of PingFederate, you might need to adapt these instructions. Refer to the PingFederate Server documentation for detailed instructions for your release.

Complete prerequisites in PingFederate

Before you can create the SP connections you will use for StorageGRID, you must complete prerequisite tasks in PingFederate. You will use information from these prerequisites when you configure the SP connections.

Create data store

If you haven't already, create a data store to connect PingFederate to the AD FS LDAP server. Use the values you used when configuring identity federation in StorageGRID.

- **Type**: Directory (LDAP)
- **LDAP Type**: Active Directory
- **Binary Attribute Name**: Enter **objectGUID** on the LDAP Binary Attributes tab exactly as shown.

Create password credential validator

If you haven't already, create a password credential validator.

- **Type**: LDAP Username Password Credential Validator
- **Data store**: Select the data store you created.
- **Search base**: Enter information from LDAP (for example, DC=saml,DC=sgws).
- **Search filter**: sAMAccountName=${username}
- **Scope**: Subtree

Create IdP adapter instance

If you haven't already, create an IdP adapter instance.

1. Go to **Authentication** > **Integration** > **IdP Adapters**.
2. Select **Create New Instance**.
3. On the Type tab, select **HTML Form IdP Adapter**.
4. On the IdP Adapter tab, select **Add a new row to 'Credential Validators'**.
5. Select the password credential validator you created.
6. On the Adapter Attributes tab, select the **username** attribute for **Pseudonym**.
7. Select **Save**.

Create or import signing certificate

If you haven't already, create or import the signing certificate.

1. Go to **Security** > **Signing & Decryption Keys & Certificates**.
2. Create or import the signing certificate.

Create an SP connection in PingFederate

When you create an SP connection in PingFederate, you import the SAML metadata you downloaded from StorageGRID for the Admin Node. The metadata file contains many of the specific values you need.

> ℹ️ You must create an SP connection for each Admin Node in your StorageGRID system, so that users can securely sign in to and out of any node. Use these instructions to create the first SP connection. Then, go to Create additional SP connections to create any additional connections you need.

Choose SP connection type

1. Go to **Applications** > **Integration** > **SP Connections**.

2. Select **Create Connection**.

3. Select **Do not use a template for this connection**.

4. Select **Browser SSO Profiles** and **SAML 2.0** as the protocol.

Import SP metadata

1. On the Import Metadata tab, select **File**.

2. Choose the SAML metadata file you downloaded from the StorageGRID Single sign-on page for the Admin Node.

3. Review the Metadata Summary and the information on the General Info tab.

   The Partner's Entity ID and the Connection Name are set to the StorageGRID SP connection ID. (for example, 10.96.105.200-DC1-ADM1-105-200). The Base URL is the IP of the StorageGRID Admin Node.

4. Select **Next**.

Configure IdP Browser SSO

1. From the Browser SSO tab, select **Configure Browser SSO**.

2. On the SAML profiles tab, select the **SP-initiated SSO**, **SP-initial SLO**, **IdP-initiated SSO**, and **IdP-initiated SLO** options.

3. Select **Next**.

4. On the Assertion Lifetime tab, make no changes.

5. On the Assertion Creation tab, select **Configure Assertion Creation**.

   a. On the Identity Mapping tab, select **Standard**.

   b. On the Attribute Contract tab, use the **SAML_SUBJECT** as the Attribute Contract and the unspecified name format that was imported.

6. For Extend the Contract, select **Delete** to remove the `urn:oid`, which is not used.

Map adapter instance

1. On the Authentication Source Mapping tab, select **Map New Adapter Instance**.

2. On the Adapter instance tab, select the adapter instance you created.

3. On the Mapping Method tab, select **Retrieve Additional Attributes From a Data Store**.

4. On the Attribute Source & User Lookup tab, select **Add Attribute Source**.

5. On the Data Store tab, provide a description and select the data store you added.

6. On the LDAP Directory Search tab:

   ◦ Enter the **Base DN**, which should exactly match the value you entered in StorageGRID for the LDAP

server.

- For the Search Scope, select **Subtree**.

- For the Root Object Class, search for the **objectGUID** attribute and add it.

7. On the LDAP Binary Attribute Encoding Types tab, select **Base64** for the **objectGUID** attribute.

8. On the LDAP Filter tab, enter **sAMAccountName=${username}**.

9. On the Attribute Contract Fulfillment tab, select **LDAP (attribute)** from the Source drop-down and select **objectGUID** from the Value drop-down.

10. Review and then save the attribute source.

11. On the Failsave Attribute Source tab, select **Abort the SSO Transaction**.

12. Review the summary and select **Done**.

13. Select **Done**.

Configure protocol settings

1. On the **SP Connection** > **Browser SSO** > **Protocol Settings** tab, select **Configure Protocol Settings**.

2. On the Assertion Consumer Service URL tab, accept the default values, which were imported from the StorageGRID SAML metadata (**POST** for Binding and `/api/saml-response` for Endpoint URL).

3. On the SLO Service URLs tab, accept the default values, which were imported from the StorageGRID SAML metadata (**REDIRECT** for Binding and `/api/saml-logout` for Endpoint URL.

4. On the Allowable SAML Bindings tab, unselect **ARTIFACT** and **SOAP**. Only **POST** and **REDIRECT** are required.

5. On the Signature Policy tab, leave the **Require Authn Requests to be Signed** and **Always Sign Assertion** check boxes selected.

6. On the Encryption Policy tab, select **None**.

7. Review the summary and select **Done** to save the protocol settings.

8. Review the summary and select **Done** to save the Browser SSO settings.

Configure credentials

1. From the SP Connection tab, select **Credentials**.

2. From the Credentials tab, select **Configure Credentials**.

3. Select the signing certificate you created or imported.

4. Select **Next** to go to **Manage Signature Verification Settings**.

   a. On the Trust Model tab, select **Unanchored**.

   b. On the Signature Verification Certificate tab, review the signing certificate information, which was imported from the StorageGRID SAML metadata.

5. Review the summary screens and select **Save** to save the SP connection.

Create additional SP connections

You can copy the first SP connection to create the SP connections you need for each Admin Node in your grid. You upload new metadata for each copy.

> ℹ️ The SP connections for different Admin Nodes use identical settings, with the exception of the Partner's Entity ID, Base URL, Connection ID, Connection Name, Signature Verification, and SLO Response URL.

1. Select **Action** > **Copy** to create a copy of the initial SP connection for each additional Admin Node.

2. Enter the Connection ID and Connection Name for the copy, and select **Save**.

3. Choose the metadata file corresponding to the Admin Node:

   a. Select **Action** > **Update with Metadata**.

   b. Select **Choose File** and upload the metadata.

   c. Select **Next**.

   d. Select **Save**.

4. Resolve the error due to the unused attribute:

   a. Select the new connection.

   b. Select **Configure Browser SSO** > **Configure Assertion Creation** > **Attribute Contract**.

   c. Delete the entry for **urn:oid**.

   d. Select **Save**.

Disable single sign-on

You can disable single sign-on (SSO) if you no longer want to use this functionality. You must disable single sign-on before you can disable identity federation.

What you'll need
- You are signed in to the Grid Manager using a supported web browser.
- You have specific access permissions.

Steps
1. Select **CONFIGURATION** > **Access control** > **Single sign-on**.

   The Single Sign-on page appears.

2. Select the **Disabled** option.

3. Select **Save**.

   A warning message appears indicating that local users will now be able to sign in.

⚠️ **Warning**

Disable single sign-on

After you disable SSO or switch to sandbox mode, local users will be able to sign in. Are you sure you want to proceed?

Cancel   OK

4. Select **OK**.

The next time you sign in to StorageGRID, the StorageGRID Sign in page appears and you must enter the username and password for a local or federated StorageGRID user.

Temporarily disable and reenable single sign-on for one Admin Node

You might not be able to sign in to the Grid Manager if the single sign-on (SSO) system goes down. In this case, you can temporarily disable and reenable SSO for one Admin Node. To disable and then reenable SSO, you must access the node's command shell.

What you'll need

- You have specific access permissions.
- You have the `Passwords.txt` file.
- You know the password for the local root user.

About this task

After you disable SSO for one Admin Node, you can sign in to the Grid Manager as the local root user. To secure your StorageGRID system, you must use the node's command shell to reenable SSO on the Admin Node as soon as you sign out.

> (i) Disabling SSO for one Admin Node does not affect the SSO settings for any other Admin Nodes in the grid. The **Enable SSO** check box on the Single Sign-on page in the Grid Manager remains selected, and all existing SSO settings are maintained unless you update them.

Steps

1. Log in to an Admin Node:

   a. Enter the following command: `ssh admin@Admin_Node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Run the following command:`disable-saml`

   A message indicates that the command applies to this Admin Node only.

3. Confirm that you want to disable SSO.

   A message indicates that single sign-on is disabled on the node.

4. From a web browser, access the Grid Manager on the same Admin Node.

   The Grid Manager sign-in page is now displayed because SSO has been disabled.

5. Sign in with the username root and the local root user's password.

6. If you disabled SSO temporarily because you needed to correct the SSO configuration:

    a. Select **CONFIGURATION** > **Access control** > **Single sign-on**.

    b. Change the incorrect or out-of-date SSO settings.

    c. Select **Save**.

       Selecting **Save** from the Single Sign-on page automatically reenables SSO for the entire grid.

7. If you disabled SSO temporarily because you needed to access the Grid Manager for some other reason:

    a. Perform whatever task or tasks you need to perform.

    b. Select **Sign Out**, and close the Grid Manager.

    c. Reenable SSO on the Admin Node. You can perform either of the following steps:

      ▪ Run the following command: `enable-saml`

        A message indicates that the command applies to this Admin Node only.

        Confirm that you want to enable SSO.

        A message indicates that single sign-on is enabled on the node.

      ▪ Reboot the grid node: `reboot`

8. From a web browser, access the Grid Manager from the same Admin Node.

9. Confirm that the StorageGRID Sign in page appears and that you must enter your SSO credentials to access the Grid Manager.