Manage groups and users

StorageGRID 11.8

NetApp
May 17, 2024

Table of Contents

Manage groups and users

Use identity federation

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

Configure identity federation for Tenant Manager

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

Before you begin

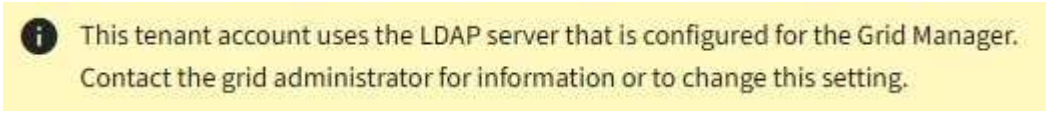
- You are signed in to the Tenant Manager using a supported web browser.
- You belong to a user group that has the Root access permission.
- You are using Active Directory, Azure AD, OpenLDAP, or Oracle Directory Server as the identity provider.

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

About this task

Whether you can configure an identity federation service for your tenant depends on how your tenant account was set up. Your tenant might share the identity federation service that was configured for the Grid Manager. If you see this message when you access the Identity Federation page, you can't configure a separate federated identity source for this tenant.

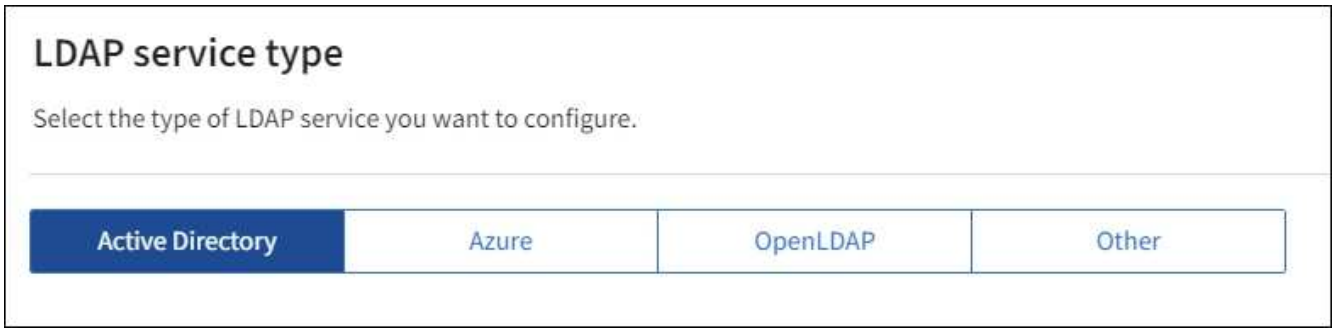


Enter configuration

When you configure identify federation, you provide the values StorageGRID needs to connect to an LDAP service.

Steps

1. Select **ACCESS MANAGEMENT** > **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.

> If you change the password in the future, you must update it on this page.

◦ **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 can't 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.

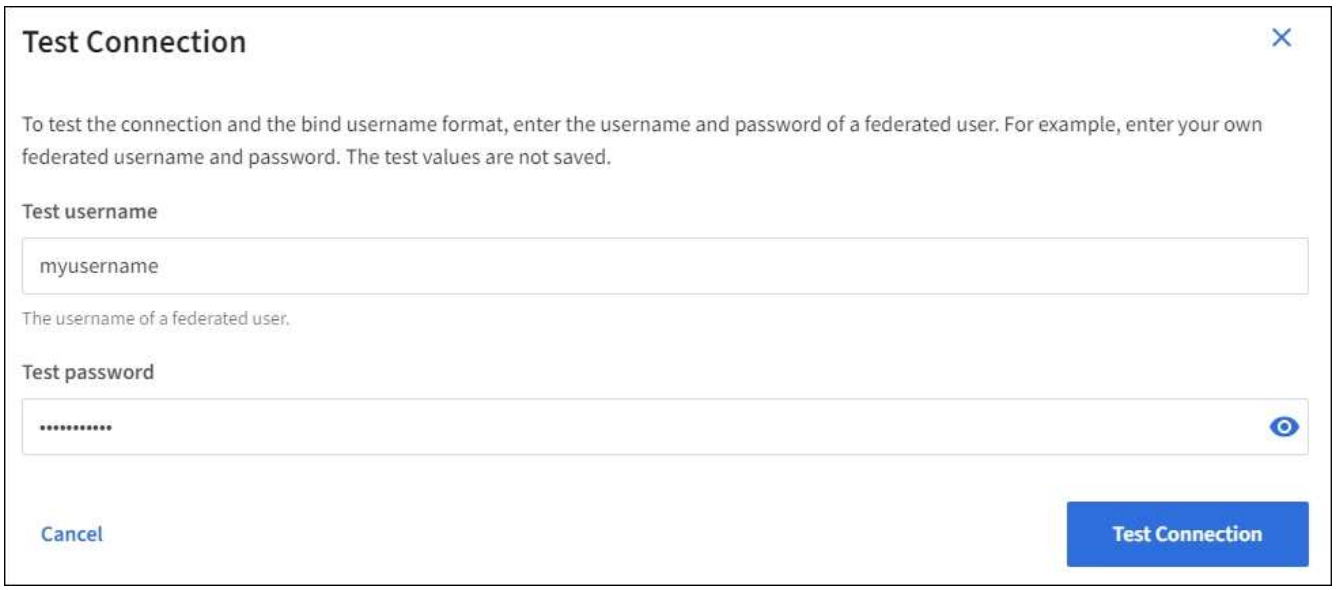
Test the connection and save the configuration

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.

Steps

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. Don't include any special characters in the username, such as @ or /.



   - 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 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.

   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** checkbox 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** checkbox.

Guidelines for configuring OpenLDAP server

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

For identity sources that aren't 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 or 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 tenant groups

Create groups for an S3 tenant

You can manage permissions for S3 user groups by importing federated groups or creating local groups.

Before you begin

- You are signed in to the Tenant Manager using a supported web browser.
- You belong to a user group that has the Root access permission.
- If you plan to import a federated group, you have configured identity federation, and the federated group already exists in the configured identity source.
- If your tenant account has the **Use grid federation connection** permission, you have reviewed the workflow and considerations for cloning tenant groups and users, and you are signed in to the tenant's source grid.

Access the Create group wizard

As your first step, access the Create group wizard.

Steps

1. Select **ACCESS MANAGEMENT** > **Groups**.
2. If your tenant account has the **Use grid federation connection** permission, confirm that a blue banner appears, indicating that new groups created on this grid will be cloned to the same tenant on the other grid in the connection. If this banner does not appear, you might be signed in to the tenant's destination grid.

3. Select **Create group**.

Choose a group type

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

Steps

1. Select the **Local group** tab to create a local group, or select the **Federated group** tab to import a group from the previously configured identity source.

   If single sign-on (SSO) is enabled for your StorageGRID system, users belonging to local groups will not be able to sign in to the Tenant Manager, although they can use client applications to manage the tenant's resources, based on group permissions.

2. Enter the group's name.
   - **Local group**: Enter both a display name and a unique name. You can edit the display name later.

     If your tenant account has the **Use grid federation connection** permission, a cloning error will occur if the same **Unique name** already exists for the tenant on the destination grid.

   - **Federated group**: Enter the unique name. For Active Directory, the unique name is the name associated with the `sAMAccountName` attribute. For OpenLDAP, the unique name is the name associated with the `uid` attribute.
3. Select **Continue**.

Manage group permissions

Group permissions control which tasks users can perform in the Tenant Manager and Tenant Management API.

Steps

1. For **Access mode**, select one of the following:
   - **Read-write** (default): Users can sign in to Tenant Manager and manage the tenant configuration.
   - **Read-only**: Users can only view settings and features. They can't make any changes or perform any operations in the Tenant Manager or Tenant 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 permissions for this group.

   See Tenant management permissions.

3. Select **Continue**.

Set S3 group policy

The group policy determines which S3 access permissions users will have.

Steps

1. Select the policy you want to use for this group.

Group policy	Description
No S3 Access	Default. Users in this group don't have access to S3 resources, unless access is granted with a bucket policy. If you select this option, only the root user will have access to S3 resources by default.
Read Only Access	Users in this group have read-only access to S3 resources. For example, users in this group can list objects and read object data, metadata, and tags. When you select this option, the JSON string for a read-only group policy appears in the text box. You can't edit this string.
Full Access	Users in this group have full access to S3 resources, including buckets. When you select this option, the JSON string for a full-access group policy appears in the text box. You can't edit this string.
Ransomware Mitigation	This example policy applies to all buckets for this tenant. Users in this group can perform common actions, but can't permanently delete objects from buckets that have object versioning enabled. Tenant Manager users who have the **Manage all buckets** permission can override this group policy. Limit the Manage all buckets permission to trusted users, and use Multi-Factor Authentication (MFA) where available.
Custom	Users in the group are granted the permissions you specify in the text box.

2. If you selected **Custom**, enter the group policy. Each group policy has a size limit of 5,120 bytes. You must enter a valid JSON formatted string.

   For detailed information about group policies, including language syntax and examples, see Example group policies.

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)

You can save the group without adding users, or you can optionally add any local users that already exist.

> If your tenant account has the **Use grid federation connection** permission, any users you select when you create a local group on the source grid aren't included when the group is cloned to the destination grid. For this reason, don't select users when you create the group. Instead, select the group when you create the users.

Steps

1. Optionally, select one or more local users for this group.
2. Select **Create group** and **Finish**.

   The group you created appears in the list of groups.

   If your tenant account has the **Use grid federation connection** permission and you are on the tenant's source grid, the new group is cloned to the tenant's destination grid. **Success** appears as the **Cloning status** in the Overview section of the group's detail page.

Create groups for a Swift tenant

You can manage access permissions for a Swift tenant account by importing federated groups or creating local groups. At least one group must have the Swift Administrator permission, which is required to manage the containers and objects for a Swift tenant account.

> Support for Swift client applications has been deprecated and will be removed in a future release.

Before you begin

- You are signed in to the Tenant Manager using a supported web browser.
- You belong to a user group that has the Root access permission.
- If you plan to import a federated group, you have configured identity federation, and the federated group already exists in the configured identity source.

Access the Create group wizard

Steps

As your first step, access the Create group wizard.

1. Select **ACCESS MANAGEMENT** > **Groups**.
2. Select **Create group**.

Choose a group type

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

Steps

1. Select the **Local group** tab to create a local group, or select the **Federated group** tab to import a group from the previously configured identity source.

   If single sign-on (SSO) is enabled for your StorageGRID system, users belonging to local groups will not be able to sign in to the Tenant Manager, although they can use client applications to manage the tenant's resources, based on group permissions.

2. Enter the group's name.
   - **Local group**: Enter both a display name and a unique name. You can edit the display name later.
   - **Federated group**: Enter the unique name. For Active Directory, the unique name is the name associated with the `sAMAccountName` attribute. For OpenLDAP, the unique name is the name associated with the `uid` attribute.
3. Select **Continue**.

Manage group permissions

Group permissions control which tasks users can perform in the Tenant Manager and Tenant Management API.

Steps

1. For **Access mode**, select one of the following:
   - **Read-write** (default): Users can sign in to Tenant Manager and manage the tenant configuration.
   - **Read-only**: Users can only view settings and features. They can't make any changes or perform any operations in the Tenant Manager or Tenant 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 the **Root access** checkbox if group users need to sign in to the Tenant Manager or Tenant Management API.
3. Select **Continue**.

Set Swift group policy

Swift users need administrator permission to authenticate into the Swift REST API to create containers and ingest objects.

1. Select the **Swift administrator** checkbox if group users need to use the Swift REST API to manage containers and objects.
2. 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)

You can save the group without adding users, or you can optionally add any local users that already exist.

Steps

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

If you have not yet created local users, you can add this group to the user on the Users page. See Manage local users.

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

   The group you created appears in the list of groups.

Tenant management permissions

Before you create a tenant group, consider which permissions you want to assign to that group. Tenant management permissions determine which tasks users can perform using the Tenant Manager or the Tenant Management API. A user can belong to one or more groups. Permissions are cumulative if a user belongs to multiple groups.

To sign in to the Tenant Manager or to use the Tenant Management API, users must belong to a group that has at least one permission. All users who can sign in can perform the following tasks:

- View the dashboard
- Change their own password (for local users)

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.

You can assign the following permissions to a group. Note that S3 tenants and Swift tenants have different group permissions.

Permission	Description	Details
Root access	Provides full access to the Tenant Manager and the Tenant Management API.	Swift users must have Root access permission to sign in to the tenant account.
Administrator	Swift tenants only. Provides full access to the Swift containers and objects for this tenant account	Swift users must have the Swift Administrator permission to perform any operations with the Swift REST API.
Manage your own S3 credentials	Allows users to create and remove their own S3 access keys.	Users who don't have this permission don't see the **STORAGE (S3)** > **My S3 access keys** menu option.

Permission	Description	Details
View all buckets	**S3 tenants**: Allows users to view all buckets and bucket configurations. **Swift tenants**: Allows Swift users to view all containers and container configurations using the Tenant Management API.	Users who don't have either the View all buckets or the Manage all buckets permission don't see the **Buckets** menu option. This permission is superseded by the Manage all buckets permission. It does not affect S3 bucket or group polices used by S3 clients or S3 Console. You can only assign this permission to Swift groups from the Tenant Management API. You can't assign this permission to Swift groups using the Tenant Manager.
Manage all buckets	**S3 tenants**: Allows users to use the Tenant Manager and the Tenant Management API to create and delete S3 buckets and to manage the settings for all S3 buckets in the tenant account, regardless of S3 bucket or group policies. **Swift tenants**: Allows Swift users to control the consistency for Swift containers using the Tenant Management API.	Users who don't have either the View all buckets or the Manage all buckets permission don't see the **Buckets** menu option. This permission supersedes the View all buckets permission. It does not affect S3 bucket or group polices used by S3 clients or S3 Console. You can only assign this permission to Swift groups from the Tenant Management API. You can't assign this permission to Swift groups using the Tenant Manager.
Manage endpoints	Allows users to use the Tenant Manager or the Tenant Management API to create or edit platform service endpoints, which are used as the destination for StorageGRID platform services.	Users who don't have this permission don't see the **Platform services endpoints** menu option.
Use S3 Console tab	When combined with the View all buckets or Manage all buckets permission, allows users to view and manage objects from the S3 Console tab on the details page for a bucket.	

Manage groups

Manage your tenant groups as needed to view, edit, or duplicate a group, and more.

Before you begin

- You are signed in to the Tenant Manager using a supported web browser.
- You belong to a user group that has the Root access permission.

View or edit group

You can view and edit the basic information and details for each group.

Steps

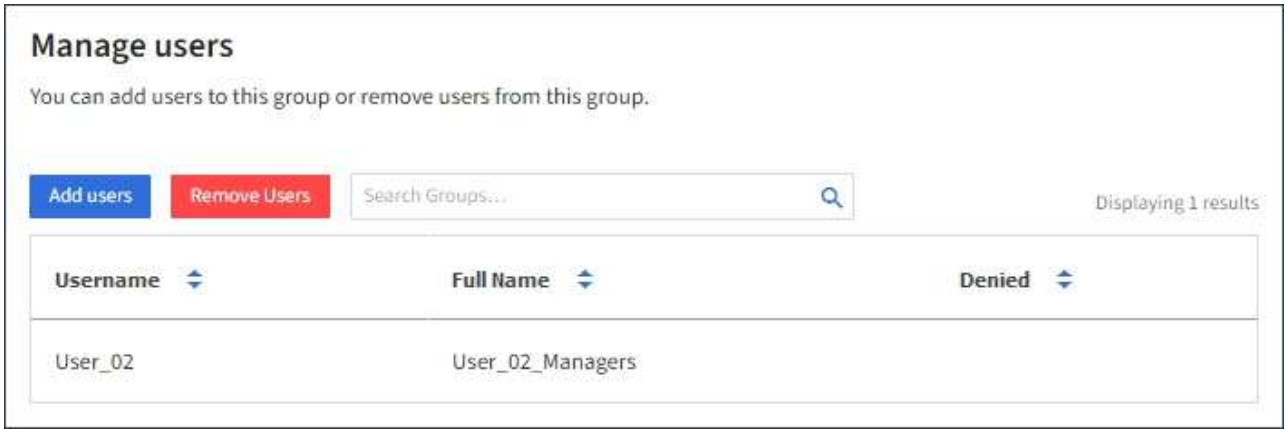
1. Select **ACCESS MANAGEMENT** > **Groups**.
2. Review the information provided on the Groups page, which lists basic information for all local and federated groups for this tenant account.

   If the tenant account has the **Use grid federation connection** permission and you are viewing groups on the tenant's source grid:

   - A banner message indicates that if you edit or remove a group, your changes will not be synced to the other grid.
   - As needed, a banner message indicates if groups were not cloned to the tenant on the destination grid. You can retry a group clone that failed.
3. If you want to change the group's name:
   a. Select the checkbox for the group.
   b. Select **Actions** > **Edit group name**.
   c. Enter the new name.
   d. Select **Save changes.**
4. If you want to view more details or make additional edits, do either of the following:
   - Select the group name.
   - Select the checkbox for the group, and select **Actions** > **View group details**.
5. Review the Overview section, which shows the following information for each group:
   - Display name
   - Unique name
   - Type
   - Access mode
   - Permissions
   - S3 Policy
   - Number of users in this group
   - Additional fields if the tenant account has the **Use grid federation connection** permission and you are viewing the group on the tenant's source grid:
     - Cloning status, either **Success** or **Failure**
     - A blue banner indicating that if you edit or delete this group, your changes will not be synced to the other grid.
6. Edit group settings as needed. See Create groups for an S3 tenant and Create groups for a Swift tenant for details about what to enter.
   a. In the Overview section, change the display name by selecting the name or the edit icon .
   b. On the **Group permissions** tab, update the permissions, and select **Save changes**.
   c. On the **Group policy** tab, make any changes, and select **Save changes**.

- If you are editing an S3 group, optionally select a different S3 group policy or enter the JSON string for a custom policy, as required.
- If you are editing a Swift group, optionally select or clear the **Swift Administrator** checkbox.

7. To add one or more existing local users to the group:
   a. Select the Users tab.



   b. Select **Add users**.
   c. Select the existing users you want to add, and select **Add users**.

      A success message appears in the upper right.

8. To remove local users from the group:
   a. Select the Users tab.
   b. Select **Remove users**.
   c. Select the users you want to remove, and select **Remove users**.

      A success message appears in the upper right.

9. Confirm that you selected **Save changes** for each section you changed.

Duplicate group

You can duplicate an existing group to create new groups more quickly.

> If your tenant account has the **Use grid federation connection** permission and you duplicate a group from the tenant's source grid, the duplicated group will be cloned to the tenant's destination grid.

Steps

1. Select **ACCESS MANAGEMENT** > **Groups**.
2. Select the checkbox for the group you want to duplicate.
3. Select **Actions** > **Duplicate group**.
4. See Create groups for an S3 tenant or Create groups for a Swift tenant for details about what to enter.
5. Select **Create group**.

Retry group clone

To retry a clone that failed:

1. Select each group that indicates *(Cloning failed)* below the group name.
2. Select **Actions** > **Clone groups**.
3. View the status of the clone operation from the details page of each group you're cloning.

For additional information, see Clone tenant groups and users.

Delete one or more groups

You can delete one or more groups. Any users who belong only to a group that is deleted will no longer be able to sign in to the Tenant Manager or use the tenant account.

> If your tenant account has the **Use grid federation connection** permission and you delete a group, StorageGRID will not delete the corresponding group on the other grid. If you need to keep this information in sync, you must delete the same group from both grids.

Steps

1. Select **ACCESS MANAGEMENT** > **Groups**.
2. Select the checkbox for each group you want to delete.
3. Select **Actions** > **Delete group** or **Actions** > **Delete groups**.

   A confirmation dialog box appears.

4. Select **Delete group** or **Delete groups**.

Manage local users

You can create local users and assign them to local groups to determine which features these users can access. The Tenant Manager includes one predefined local user, named "root." Although you can add and remove local users, you can't remove the root user.

> If single sign-on (SSO) is enabled for your StorageGRID system, local users will not be able to sign in to the Tenant Manager or the Tenant Management API, although they can use client applications to access the tenant's resources, based on group permissions.

Before you begin

- You are signed in to the Tenant Manager using a supported web browser.
- You belong to a user group that has the Root access permission.
- If your tenant account has the **Use grid federation connection** permission, you have reviewed the workflow and considerations for cloning tenant groups and users, and you are signed in to the tenant's source grid.

Create a local user

You can create a local user and assign them to one or more local groups to control their access permissions.

S3 users who don't belong to any groups don't have management permissions or S3 group policies applied to them. These users might have S3 bucket access granted through a bucket policy.

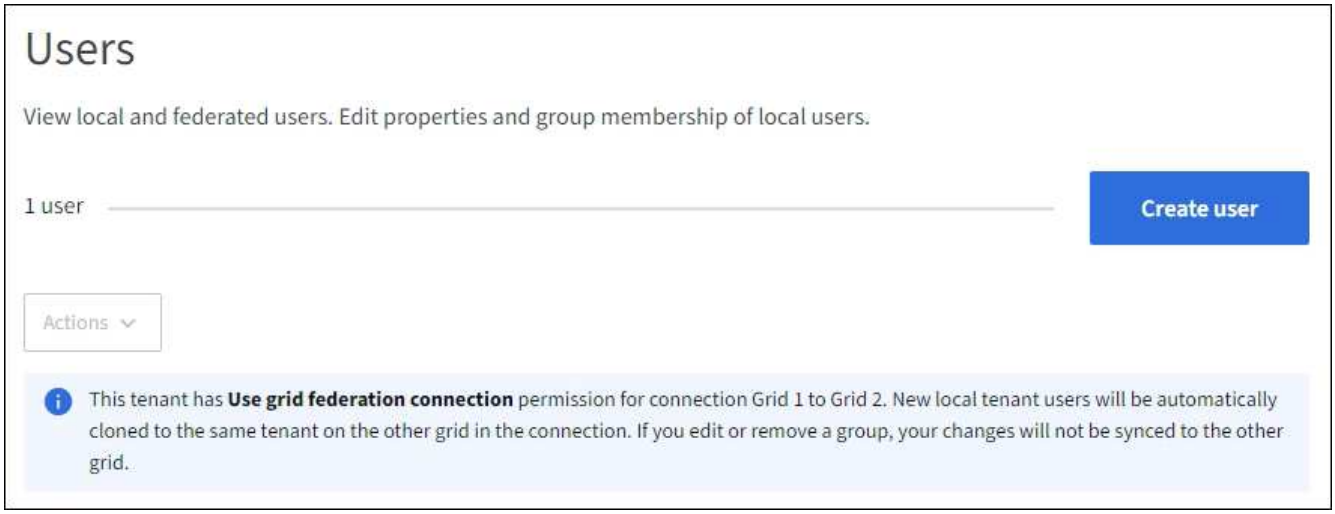
Swift users who don't belong to any groups don't have management permissions or Swift container access.

Access the Create user wizard

Steps

1. Select **ACCESS MANAGEMENT** > **Users**.

   If your tenant account has the **Use grid federation connection** permission, a blue banner indicates that this is the tenant's source grid. Any local users you create on this grid will be cloned to the other grid in the connection.



2. Select **Create user**.

Enter credentials

Steps

1. For the **Enter user credentials** step, complete the following fields.

Field	Description
Full name	The full name for this user, for example, the first name and last name of a person or the name of an application.
Username	The name this user will use to sign in. Usernames must be unique and can't be changed. **Note**: If your tenant account has the **Use grid federation connection** permission, a cloning error will occur if the same **Username** already exists for the tenant on the destination grid.
Password and Confirm password	The password the user will initially use when signing in.

Field	Description
Deny access	Select **Yes** to prevent this user from signing in to the tenant account, even though they might still belong to one or more groups. For example, select **Yes** to temporarily suspend a user's ability to sign in.

2. Select **Continue**.

Assign to groups

Steps

1. Assign the user to one or more local groups to determine which tasks they can perform.

   Assigning a user to groups is optional. If you'd prefer, you can select users when you create or edit groups.

   Users who don't belong to any groups will have no management permissions. Permissions are cumulative. Users will have all permissions for all groups they belong to. See Tenant management permissions.

2. Select **Create user**.

   If your tenant account has the **Use grid federation connection** permission and you are on the tenant's source grid, the new local user is cloned to the tenant's destination grid. **Success** appears as the **Cloning status** in the Overview section of the user's detail page.

3. Select **Finish** to return to the Users page.

View or edit local user

Steps

1. Select **ACCESS MANAGEMENT** > **Users**.
2. Review the information provided on the Users page, which lists basic information for all local and federated users for this tenant account.

   If the tenant account has the **Use grid federation connection** permission and you are viewing the user on the tenant's source grid:

   - A banner message indicates that if you edit or remove a user, your changes will not be synced to the other grid.
   - As needed, a banner message indicates if users were not cloned to the tenant on the destination grid. You can retry a user clone that failed.

3. If you want to change the user's full name:
   a. Select the checkbox for the user.
   b. Select **Actions** > **Edit full name**.
   c. Enter the new name.
   d. Select **Save changes.**
4. If you want to view more details or make additional edits, do either of the following:
   - Select the username.

- Select the checkbox for the user, and select **Actions** > **View user details**.

5. Review the Overview section, which shows the following information for each user:
   - Full name
   - Username
   - User type
   - Denied access
   - Access mode
   - Group membership
   - Additional fields if the tenant account has the **Use grid federation connection** permission and you are viewing the user on the tenant's source grid:
     - Cloning status, either **Success** or **Failure**
     - A blue banner indicating that if you edit this user, your changes will not be synced to the other grid.
6. Edit user settings as needed. See Create local user for details about what to enter.
   a. In the Overview section, change the full name by selecting the name or the edit icon .

      You can't change the username.

   b. On the **Password** tab, change the user's password, and select **Save changes**.
   c. On the **Access** tab, select **No** to allow the user to sign in or select **Yes** to prevent the user from signing in. Then, select **Save changes**.
   d. On the **Access keys** tab, select **Create key** and follow the instructions for creating another user's S3 access keys.
   e. On the **Groups** tab, select **Edit groups** to add the user to groups or remove the user from groups. Then, select **Save changes**.
7. Confirm that you selected **Save changes** for each section you changed.

Duplicate local user

You can duplicate a local user to create a new user more quickly.

> If your tenant account has the **Use grid federation connection** permission and you duplicate a user from the tenant's source grid, the duplicated user will be cloned to the tenant's destination grid.

Steps

1. Select **ACCESS MANAGEMENT** > **Users**.
2. Select the checkbox for the user you want to duplicate.
3. Select **Actions** > **Duplicate user**.
4. See Create local user for details about what to enter.
5. Select **Create user**.

Retry user clone

To retry a clone that failed:

1. Select each user that indicates *(Cloning failed)* below the user name.
2. Select **Actions** > **Clone users**.
3. View the status of the clone operation from the details page of each user you're cloning.

For additional information, see Clone tenant groups and users.

Delete one or more local users

You can permanently delete one or more local users who no longer need to access the StorageGRID tenant account.

> If your tenant account has the **Use grid federation connection** permission and you delete a local user, StorageGRID will not delete the corresponding user on the other grid. If you need to keep this information in sync, you must delete the same user from both grids.

> You must use the federated identity source to delete federated users.

Steps

1. Select **ACCESS MANAGEMENT** > **Users**.
2. Select the checkbox for each user you want to delete.
3. Select **Actions** > **Delete user** or **Actions** > **Delete users**.

   A confirmation dialog box appears.

4. Select **Delete user** or **Delete users**.

Copyright information

Trademark information