Managing system access for tenant users

StorageGRID 11.5

NetApp
January 04, 2024

Table of Contents

Managing system access for tenant users

You grant users access to a tenant account by importing groups from a federated identity source and assigning management permissions. You can also create local tenant groups and users, unless single sign-on (SSO) is in effect for the entire StorageGRID system.

- Using identity federation
- Managing groups
- Managing local users

Using 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.

- Configuring a federated identity source
- Forcing synchronization with the identity source
- Disabling identity federation

Configuring a federated identity source

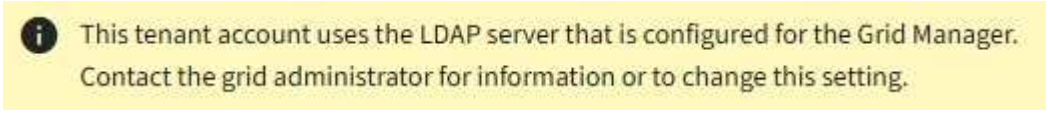
You can configure identity federation if you want tenant groups and users to be managed in another system such as Active Directory, OpenLDAP, or Oracle Directory Server.

What you'll need

- You must be signed in to the Tenant Manager using a supported browser.
- You must have specific access permissions.
- You must be using Active Directory, OpenLDAP, or Oracle Directory Server as the identity provider. If you want to use an LDAP v3 service that is not listed, you must contact technical support.
- 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.

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 cannot configure a separate federated identity source for this tenant.



Steps

1. Select **ACCESS MANAGEMENT** > **Identity federation**.
2. Select **Enable identity federation**.
3. In the LDAP service type section, select **Active Directory**, **OpenLDAP**, or **Other**.

If you select **OpenLDAP**, configure the OpenLDAP server. See the guidelines for configuring an OpenLDAP server.

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.
   - **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. In the Configure LDAP server section, enter the required LDAP server and network connection information.
   - **Hostname**: The server hostname 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`
   - **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.

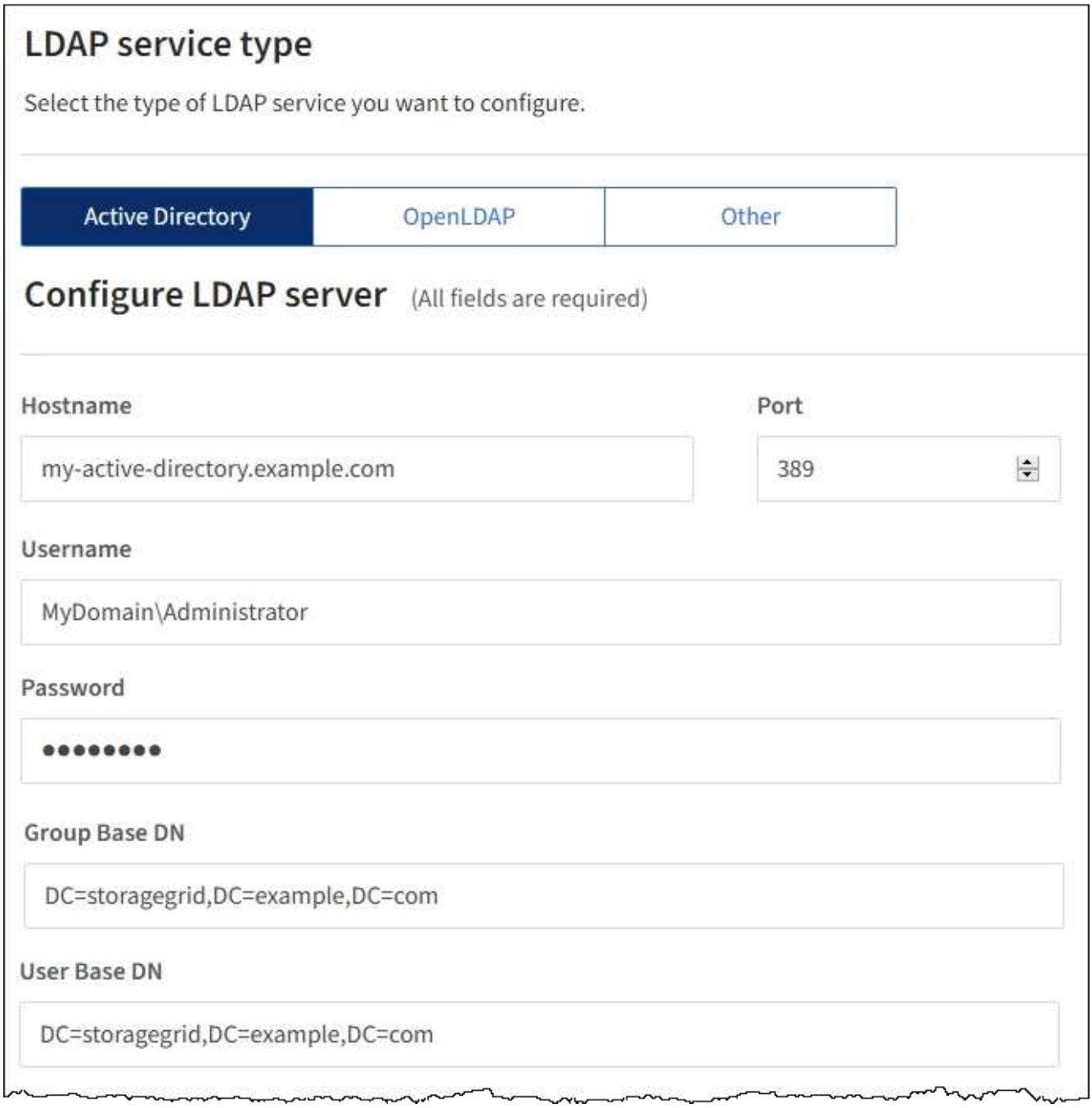
6. In the **Transport Layer Security (TLS)** section, select a security setting.
   - **Use STARTTLS (recommended)**: Use STARTTLS to secure communications with the LDAP server. This is the recommended option.
   - **Use LDAPS**: The LDAPS (LDAP over SSL) option uses TLS to establish a connection to the LDAP server. This option is supported for compatibility reasons.
   - **Do not use TLS**: The network traffic between the StorageGRID system and the LDAP server will not be secured.

     This 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 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.
8. Select **Test connection** to validate your connection settings for the LDAP server.

   A confirmation message appears in the upper right corner of the page if the connection is valid.
9. If the connection is valid, select **Save**.

   The following screenshot shows example configuration values for an LDAP server that uses Active Directory.



Related information

Tenant management permissions

Guidelines for configuring an OpenLDAP server

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.

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 Administrator's Guide for OpenLDAP.

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 Administrator's Guide for OpenLDAP.

Forcing 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.

What you'll need

- You must be signed in to the Tenant Manager using a supported browser.
- You must have specific access permissions.
- The saved identity source must be enabled.

Steps

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

   The Identity federation page appears. The **Sync server** button is at the top right of the page.

   > If the saved identity source is not enabled, the **Sync server** button will not be active.

2. Select **Sync server**.

   A confirmation message is displayed indicating that synchronization started successfully.

Related information

Tenant management permissions

Disabling identity federation

If you configured an identity federation service for this tenant, you can temporarily or permanently disable identity federation for tenant groups and users. When identity federation is disabled, there is no communication between the StorageGRID system and the identity source. However, any settings you have configured are retained, allowing you to easily re-enable identity federation in the future.

What you'll need

- You must be signed in to the Tenant Manager using a supported browser.
- You must have specific access permissions.

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 tenant account 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.

Steps

1. Select **ACCESS MANAGEMENT** > **Identity federation**.
2. Deselect the **Enable identity federation** check box.
3. Select **Save**.

Related information

Tenant management permissions

Managing groups

You assign permissions to user groups to control which tasks tenant users can perform. You can import federated groups from an identity source, such as Active Directory or OpenLDAP, or you can create local groups.

If single sign-on (SSO) is enabled for your StorageGRID system, local users will not be able to sign in to the Tenant Manager, although they can access S3 and Swift resources, based on group permissions.

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. Changes might take up to 15 minutes to take effect because of caching.

Permission	Description
Root Access	Provides full access to the Tenant Manager and the Tenant Management API. **Note:** 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 **Note:** Swift users must have the Swift Administrator permission to perform any operations with the Swift REST API.
Manage Your Own S3 Credentials	S3 tenants only. Allows users to create and remove their own S3 access keys. Users who do not have this permission do not see the **STORAGE (S3)** > **My S3 access keys** menu option.
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. Users who do not have this permission do not see the **Buckets** menu option. • Swift tenants: Allows Swift users to control the consistency level for Swift containers using the Tenant Management API. **Note:** You can only assign the Manage All Buckets permission to Swift groups from the Tenant Management API. You cannot assign this permission to Swift groups using the Tenant Manager.
Manage Endpoints	S3 tenants only. Allows users to use the Tenant Manager or the Tenant Management API to create or edit endpoints, which are used as the destination for StorageGRID platform services. Users who do not have this permission do not see the **Platform services endpoints** menu option.

Related information

Use S3

Use Swift

Creating groups for an S3 tenant

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

What you'll need

- You must be signed in to the Tenant Manager using a supported browser.
- You must 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.

Steps

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

2. Select **Create group**.
3. 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.

4. 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.
5. Select **Continue**.
6. Select an Access mode. 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.
   - **Read-write** (default): Users can log into Tenant Manager and manage the tenant configuration.
   - **Read-only**: Users can only view settings and features. They cannot make any changes or perform any operations in the Tenant Manager or Tenant Management API. Local read-only users can change their own passwords.
7. Select the Group permissions for this group.

See the information about tenant management permissions.

8. Select **Continue**.
9. Select a group policy to determine which S3 access permissions the members of this group will have.
   - **No S3 Access**: Default. Users in this group do not 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 cannot 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 cannot edit this string.
   - **Custom**: Users in the group are granted the permissions you specify in the text box. See the instructions for implementing an S3 client application for detailed information about group policies, including language syntax and examples.
10. 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.

    In this example, members of the group are only permitted to list and access a folder matching their username (key prefix) in the specified bucket. Note that access permissions from other group policies and the bucket policy should be considered when determining the privacy of these folders.

11. Select the button that appears, depending on whether you are creating a federated group or a local group:
    - Federated group: **Create group**

- Local group: **Continue**

If you are creating a local group, step 4 (Add users) appears after you select **Continue**. This step does not appear for federated groups.

12. Select the check box for each user you want to add to the group, then select **Create group**.

    Optionally, you can save the group without adding users. You can add users to the group later, or select the group when you add new users.

13. Select **Finish**.

    The group you created appears in the list of groups. Changes might take up to 15 minutes to take effect because of caching.

Related information

Tenant management permissions

Use S3

Creating 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.

What you'll need

- You must be signed in to the Tenant Manager using a supported browser.
- You must 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.

Steps

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

2. Select **Create group**.
3. 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.

4. 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.
5. Select **Continue**.
6. Select an Access mode. 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.
   - **Read-write** (default): Users can log into Tenant Manager and manage the tenant configuration.
   - **Read-only**: Users can only view settings and features. They cannot make any changes or perform any operations in the Tenant Manager or Tenant Management API. Local read-only users can change their own passwords.
7. Set the Group permission.
   - Select the **Root Access** check box if users need to sign in to the Tenant Manager or Tenant Management API. (Default)
   - Unselect the **Root Access** check box if users do not need access to the Tenant Manager or Tenant Management API. For example, unselect the check box for applications that do not need to access the tenant. Then, assign the **Swift Administrator** permission to allow these users to manage containers and objects.
8. Select **Continue**.

9. Select the **Swift administrator** check box if the user needs to be able to use the Swift REST API.

   Swift users must have the Root Access permission to access the Tenant Manager. However, the Root Access permission does not allow users to authenticate into the Swift REST API to create containers and ingest objects. Users must have the Swift Administrator permission to authenticate into the Swift REST API.

10. Select the button that appears, depending on whether you are creating a federated group or a local group:
    - Federated group: **Create group**
    - Local group: **Continue**

      If you are creating a local group, step 4 (Add users) appears after you select **Continue**. This step does not appear for federated groups.

11. Select the check box for each user you want to add to the group, then select **Create group**.

    Optionally, you can save the group without adding users. You can add users to the group later, or select the group when you create new users.

12. Select **Finish**.

    The group you created appears in the list of groups. Changes might take up to 15 minutes to take effect because of caching.

Related information

Tenant management permissions

Use Swift

Viewing and editing group details

When you view the details for a group, you can change the group's display name, permissions, policies, and the users that belong to the group.

What you'll need

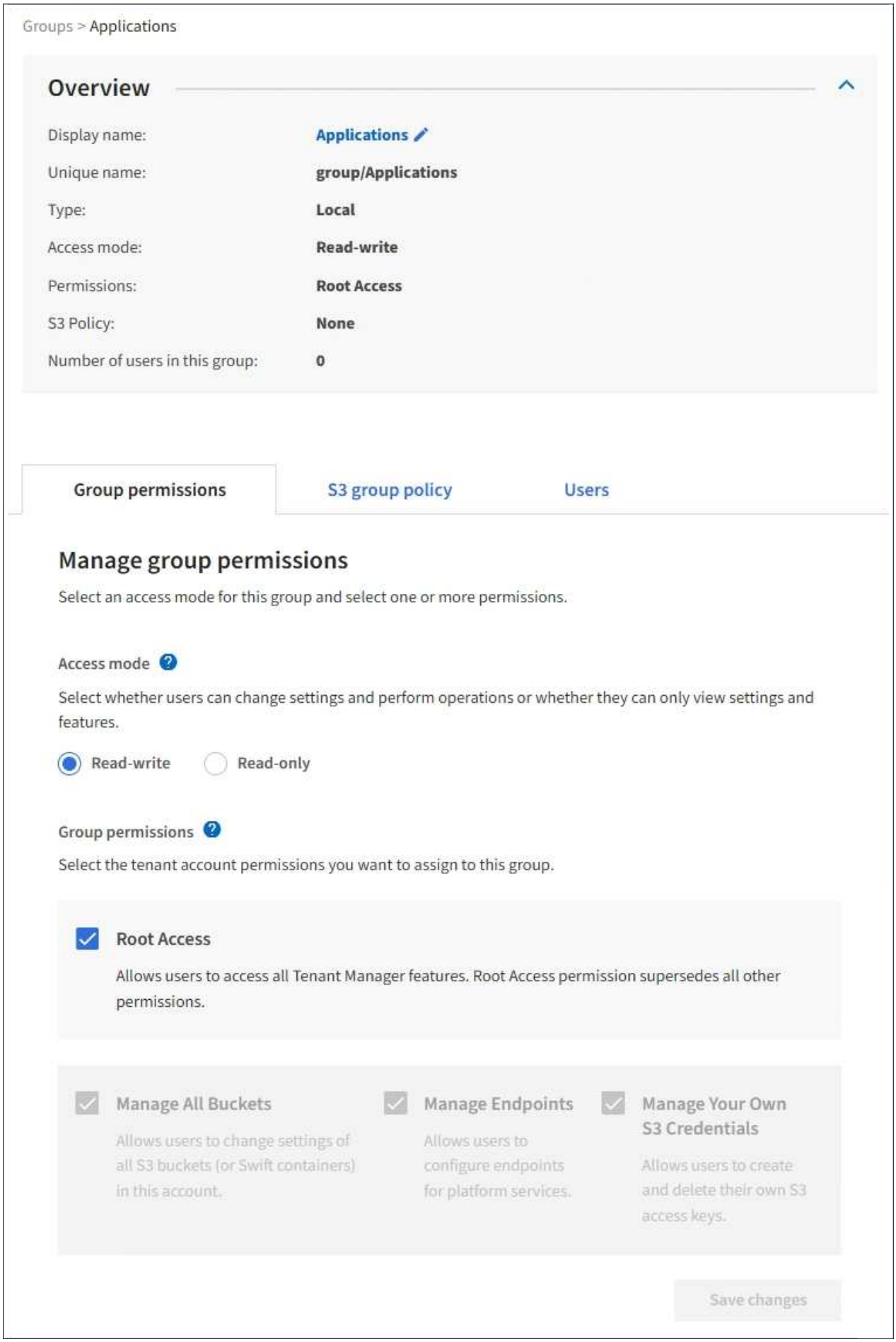
- You must be signed in to the Tenant Manager using a supported browser.
- You must belong to a user group that has the Root Access permission.

Steps

1. Select **ACCESS MANAGEMENT** > **Groups**.
2. Select the name of the group whose details you want to view or edit.

   Alternatively, you can select **Actions** > **View group details**.

   The group details page appears. The following example shows the S3 group details page.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Make changes to the group settings as needed.

> To ensure your changes are saved, select **Save changes** after you make changes in each section. When your changes are saved, a confirmation message appears in the upper right corner of the page.

   a. Optionally, select the display name or edit icon to update the display name.

      You cannot change a group's unique name. You cannot edit the display name for a federated group.

   b. Optionally, update the permissions.

   c. For group policy, make the appropriate changes for your S3 or Swift tenant.

      - If you are editing a group for an S3 tenant, optionally select a different S3 group policy. If you select a custom S3 policy, update the JSON string as required.
      - If you are editing a group for a Swift tenant, optionally select or unselect the **Swift Administrator** check box.

        For more information about the Swift Administrator permission, see the instructions for creating groups for a Swift tenant.

   d. Optionally, add or remove users.

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

   Changes might take up to 15 minutes to take effect because of caching.

Related information

Creating groups for an S3 tenant

Creating groups for a Swift tenant

Adding users to a local group

You can add users to a local group as needed.

What you'll need

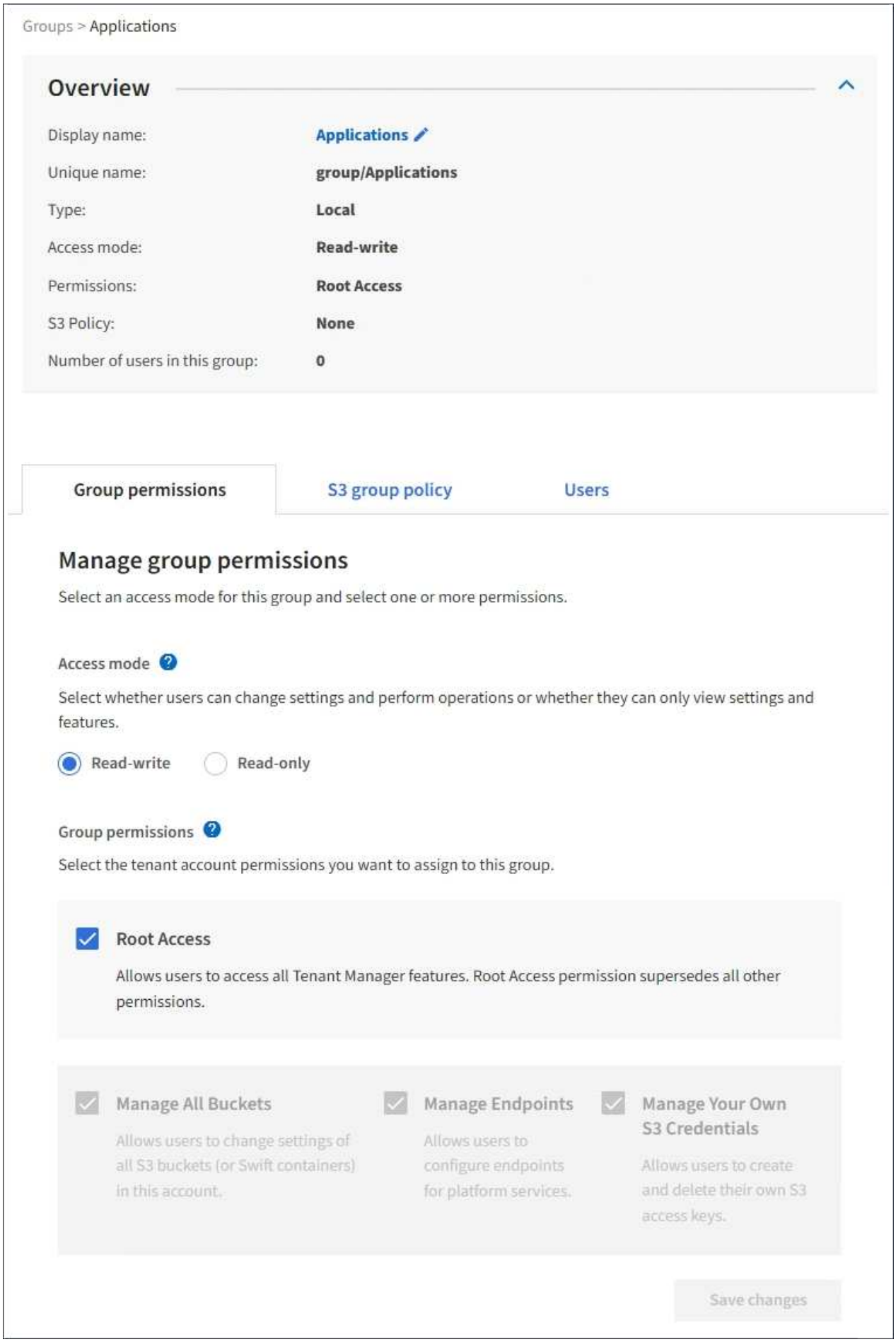
- You must be signed in to the Tenant Manager using a supported browser.
- You must belong to a user group that has the Root Access permission.

Steps

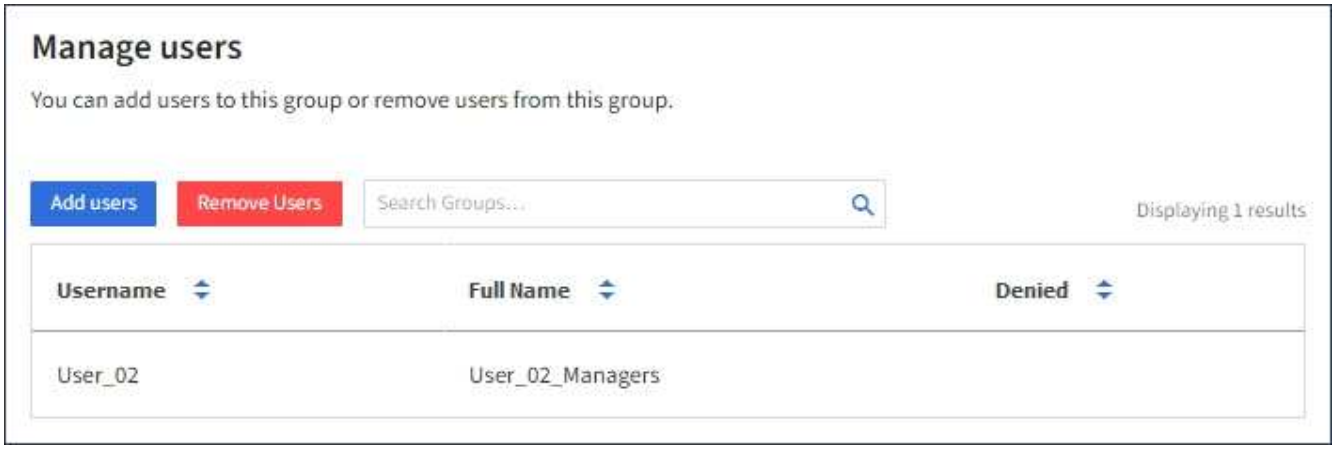
1. Select **ACCESS MANAGEMENT** > **Groups**.
2. Select the name of the local group you want to add users to.

   Alternatively, you can select **Actions** > **View group details**.

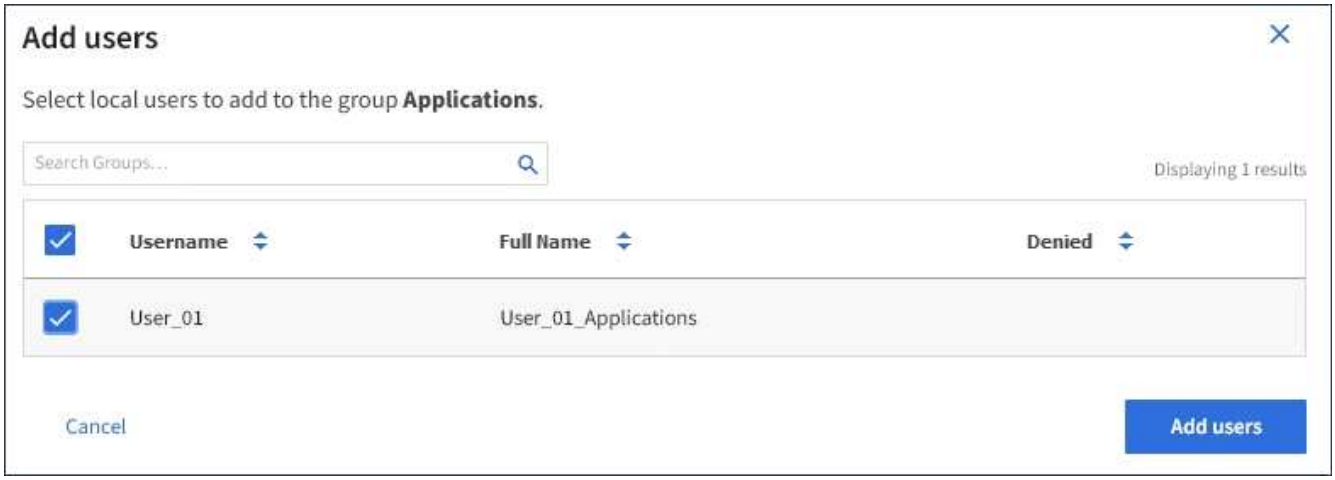
   The group details page appears.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Select **Manage Users**, and then select **Add users**.



4. Select the users you want to add to the group, and then select **Add users**.



A confirmation message appears in the upper right corner of the page. Changes might take up to 15 minutes to take effect because of caching.

Editing a group name

You can edit the display name for a group. You cannot edit the unique name for a group.

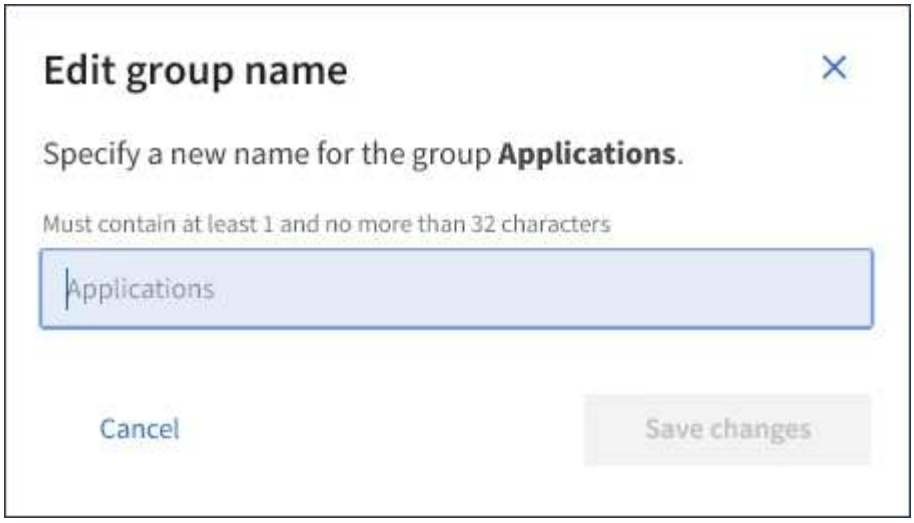
What you'll need

- You must be signed in to the Tenant Manager using a supported browser.
- You must belong to a user group that has the Root Access permission.

Steps

1. Select **ACCESS MANAGEMENT** > **Groups**.
2. Select the check box for the group whose display name you want to edit.
3. Select **Actions** > **Edit group name**.

   The Edit group name dialog box appears.



4. If you are editing a local group, update the display name as needed.

   You cannot change a group's unique name. You cannot edit the display name for a federated group.

5. Select **Save changes**.

   A confirmation message appears in the upper right corner of the page. Changes might take up to 15 minutes to take effect because of caching.

Related information

Tenant management permissions

Duplicating a group

You can create new groups more quickly by duplicating an existing group.

What you'll need

- You must be signed in to the Tenant Manager using a supported browser.
- You must belong to a user group that has the Root Access permission.

Steps

1. Select **ACCESS MANAGEMENT** > **Groups**.
2. Select the check box for the group you want to duplicate.
3. Select **Duplicate group**. For additional details on creating a group, see the instructions for creating groups for an S3 tenant or for a Swift tenant.
4. 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.

5. 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.

6. Select **Continue**.
7. As needed, modify the permissions for this group.
8. Select **Continue**.
9. As needed, if you are duplicating a group for an S3 tenant, optionally select a different policy from the **Add S3 policy** radio buttons. If you selected a custom policy, update the JSON string as required.
10. Select **Create group**.

Related information

Creating groups for an S3 tenant

Creating groups for a Swift tenant

Tenant management permissions

Deleting a group

You can delete a group from the system. Any users who belong only to that group will no longer be able to sign in to the Tenant Manager or use the tenant account.

What you'll need

- You must be signed in to the Tenant Manager using a supported browser.
- You must belong to a user group that has the Root Access permission.

Steps

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

2. Select the check boxes for the groups you want to delete.
3. Select **Actions** > **Delete group**.

   A confirmation message appears.

4. Select **Delete group** to confirm you want to delete the groups indicated in the confirmation message.

   A confirmation message appears in the upper right corner of the page. Changes might take up to 15 minutes to take effect because of caching.

Related information

Tenant management permissions

Managing 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 cannot remove the root user.

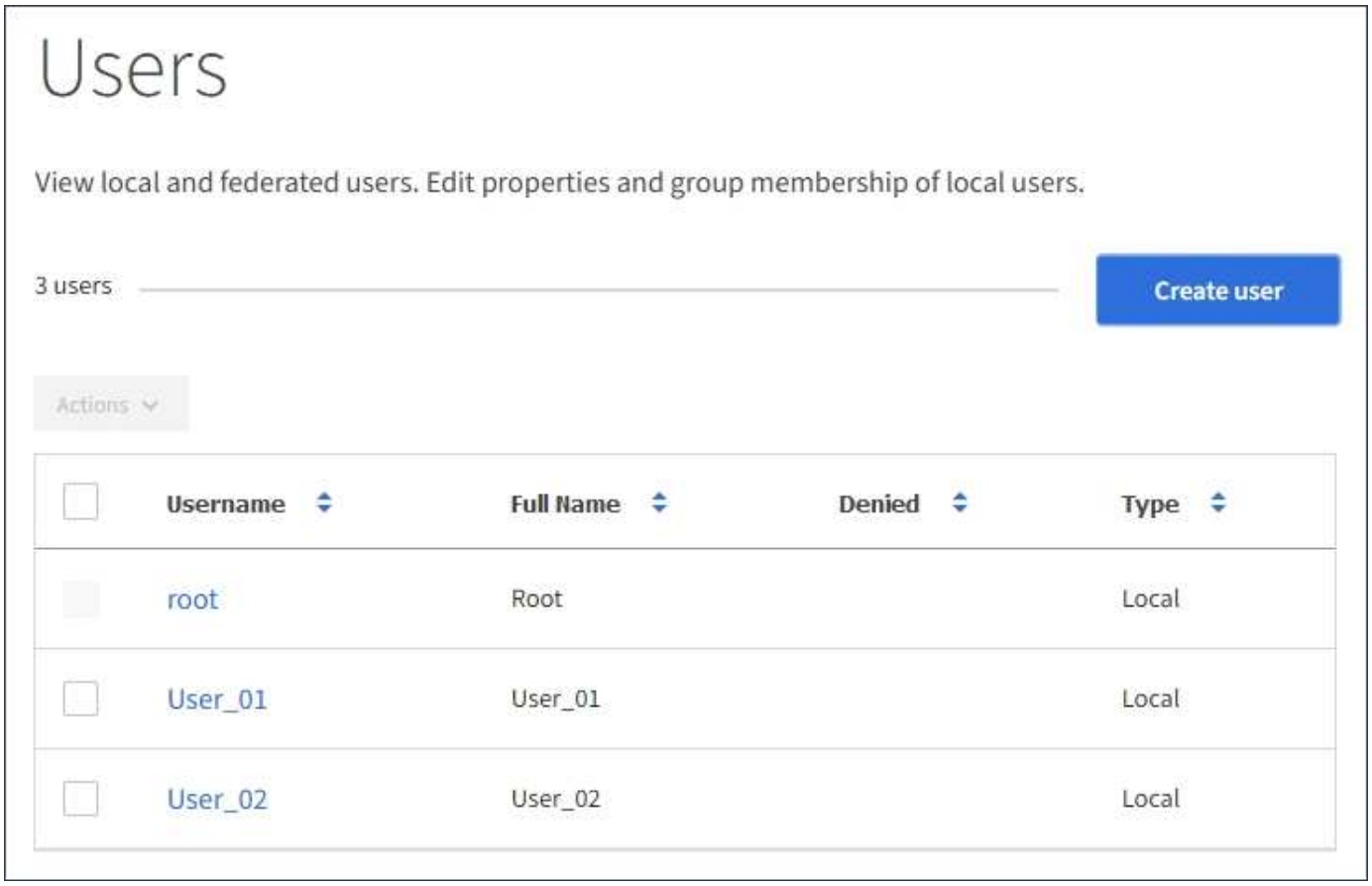
What you’ll need

- You must be signed in to the Tenant Manager using a supported browser.
- You must belong to a read-write user group that has the Root Access permission.

> 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 S3 or Swift client applications to access the tenant’s resources, based on group permissions.

Accessing the Users page

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



Creating local users

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

S3 users who do not belong to any groups do not 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 do not belong to any groups do not have management permissions or Swift container access.

Steps

1. Select **Create user**.
2. Complete the following fields.
   - **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 cannot be changed.
   - **Password**: A password, which is used when the user signs in.
   - **Confirm password**: Type the same password you typed in the Password field.
   - **Deny access**: If you select **Yes**, this user cannot sign in to the tenant account, even though the user might still belong to one or more groups.

     As an example, you can use this feature to temporarily suspend a user's ability to sign in.
3. Select **Continue**.
4. Assign the user to one or more local groups.

Users who do not belong to any groups will have no management permissions. Permissions are cumulative. Users will have all permissions for all groups they belong to.

5. Select **Create user**.

   Changes might take up to 15 minutes to take effect because of caching.

Editing user details

When you edit the details for a user, you can change the user's full name and password, add the user to different groups, and prevent the user from accessing the tenant.

Steps

1. In the Users list, select the name of the user whose details you want to view or edit.

   Alternatively, you can select the check box for the user, and then select **Actions** > **View user details**.

2. Make changes to the user settings as needed.
   a. Change the user's full name as needed by selecting the full name or the edit icon in the Overview section.

      You cannot change the username.

   b. On the **Password** tab, change the user's password as needed.
   c. On the **Access** tab, allow the user to sign in (select **No**), or prevent the user from signing in (select **Yes**) as needed.
   d. On the **Groups** tab, add the user to groups or remove the user from groups as needed.
   e. As necessary for each section, select **Save changes**.

      Changes might take up to 15 minutes to take effect because of caching.

Duplicating local users

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

Steps

1. In the Users list, select the user you want to duplicate.
2. Select **Duplicate user**.
3. Modify the following fields for the new user.
   - **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 cannot be changed.
   - **Password**: A password, which is used when the user signs in.
   - **Confirm password**: Type the same password you typed in the Password field.
   - **Deny access**: If you select **Yes**, this user cannot sign in to the tenant account, even though the user might still belong to one or more groups.

     As an example, you can use this feature to temporarily suspend a user's ability to sign in.

4. Select **Continue**.
5. Select one or more local groups.

   Users who do not belong to any groups will have no management permissions. Permissions are cumulative. Users will have all permissions for all groups they belong to.

6. Select **Create user**.

   Changes might take up to 15 minutes to take effect because of caching.

Deleting local users

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

Using the Tenant Manager, you can delete local users, but not federated users. You must use the federated identity source to delete federated users.

Steps

1. In the Users list, select the check box for the local user you want to delete.
2. Select **Actions** > **Delete user**.
3. In the confirmation dialog box, select **Delete user** to confirm you want to delete the user from the system.

   Changes might take up to 15 minutes to take effect because of caching.

Related information

Tenant management permissions

Copyright information

Trademark information