



# **Controlling administrator access to StorageGRID**

StorageGRID 11.5

NetApp  
August 30, 2024

# Table of Contents

- Controlling administrator access to StorageGRID ..... 1
  - Controlling access through firewalls ..... 1
  - Using identity federation ..... 2
  - Managing admin groups ..... 7
  - Managing local users ..... 16
  - Using single sign-on (SSO) for StorageGRID ..... 18
  - Configuring administrator client certificates ..... 35

# Controlling administrator access to StorageGRID

You can control administrator access to the StorageGRID system by opening or closing firewall ports, managing admin groups and users, configuring single sign-on (SSO), and providing client certificates to allow secure external access to StorageGRID metrics.

- [Controlling access through firewalls](#)
- [Using identity federation](#)
- [Managing admin groups](#)
- [Managing local users](#)
- [Using single sign-on \(SSO\) for StorageGRID](#)
- [Configuring administrator client certificates](#)

## Controlling access through firewalls

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

### Controlling 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.  <b>Note:</b> Port 443 is also used for some internal traffic.
8443	Restricted Grid Manager port on Admin Nodes	<ul style="list-style-type: none"><li>• Web browsers and management API clients can access the Grid Manager and the Grid Management API using HTTPS.</li><li>• Web browsers and management API clients cannot access the Tenant Manager or the Tenant Management API.</li><li>• Requests for internal content will be rejected.</li></ul>

Port	Description	If port is open...
9443	Restricted Tenant Manager port on Admin Nodes	<ul style="list-style-type: none"> <li>• Web browsers and management API clients can access the Tenant Manager and the Tenant Management API using HTTPS.</li> <li>• Web browsers and management API clients cannot access the Grid Manager or the Grid Management API.</li> <li>• Requests for internal content will be rejected.</li> </ul>



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

[Signing in to the Grid Manager](#)

[Creating a tenant account if StorageGRID is not using SSO](#)

[Summary: IP addresses and ports for client connections](#)

[Managing untrusted Client Networks](#)

[Install Ubuntu or Debian](#)

[Install VMware](#)

[Install Red Hat Enterprise Linux or CentOS](#)

## Using identity federation

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

### Configuring identity federation

You can configure identity federation if you want admin 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 Grid Manager using a supported browser.
- You must have specific access permissions.
- If you plan to enable single sign-on (SSO), you must use Active Directory as the federated identity source and AD FS as the identity provider. See "Requirements for using single sign-on."
- 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

You must configure an identity source for the Grid Manager if you want to import the following types of federated groups:

- Administration 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.

## Steps

1. Select **Configuration > Access Control > Identity Federation**.
2. Select **Enable identity federation**.

The fields for configuring the LDAP server appear.

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

You can select **Active Directory**, **OpenLDAP**, or **Other**.



If you select **OpenLDAP**, you must 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.



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 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. Optionally, 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.

The screenshot shows a web interface for configuring an LDAP service. At the top, the title is "LDAP service type". Below the title, there is a instruction: "Select the type of LDAP service you want to configure:". There are three buttons: "Active Directory" (which is selected and highlighted in dark blue), "OpenLDAP", and "Other". Below the buttons, the section is titled "Configure LDAP server" with a note "(All fields are required)". The form contains several input fields: "Hostname" with the value "my-active-directory.example.com", "Port" with a dropdown menu showing "389", "Username" with the value "MyDomain\Administrator", "Password" with a masked field of ten dots, "Group Base DN" with the value "DC=storagegrid,DC=example,DC=com", and "User Base DN" with the value "DC=storagegrid,DC=example,DC=com".

#### Related information

[Supported ciphers for outgoing TLS connections](#)

[Requirements for using single sign-on](#)

[Creating a tenant account](#)

[Use a tenant account](#)

## 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.

### Related information

[OpenLDAP documentation: Version 2.4 Administrator's Guide](#)

## 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 Grid Manager using a supported browser.
- You must have specific access permissions.
- The identity source must be enabled.

### Steps

1. Select **Configuration > Access Control > Identity Federation**.

The Identity Federation page appears. The **Synchronize** button is at the bottom of the page.

#### Synchronize

---

StorageGRID periodically synchronizes federated groups and users from the configured LDAP server. Clicking the button below will immediately start the synchronization process against the saved LDAP server.

Synchronize

2. Click **Synchronize**.

A confirmation message indicates that synchronization started successfully. 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.

## Disabling 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.

### What you'll need

- You must be signed in to the Grid 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 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.

### Steps

1. Select **Configuration > Access Control > Identity Federation**.
2. Uncheck the **Enable Identity Federation** check box.
3. Click **Save**.

### Related information

[Disabling single sign-on](#)

## Managing 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.

### Creating admin groups

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

### What you'll need

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

- If you plan to import a federated group, you must have configured identity federation and the federated group must already exist in the configured identity source.

## Steps

1. Select **Configuration > Access Control > Admin Groups**.

The Admin Groups page appears and lists any existing admin groups.

### Admin Groups

Add and manage local and federated user groups, allowing member users to sign in to the Grid Manager. Set group permissions to control access to specific pages and features.

<input type="button" value="+ Add"/> <input type="button" value="Clone"/> <input type="button" value="Edit"/> <input type="button" value="x Remove"/>				
	Name	ID	Group Type	Access Mode
<input checked="" type="radio"/>	Flintstone	264083d0-23b5-3046-9bd4-88b7097731ab	Federated	Read-write
<input type="radio"/>	Simpson	cc8ad11f-68d0-f84a-af29-e7a6fcdc63a2	Federated	Read-only
<input type="radio"/>	ILM (read-only group)	88446141-9599-4543-b183-9c227ce7767a	Local	Read-only
<input type="radio"/>	API Developers	974b2faa-f9a1-4cfc-b364-914cdba2905f	Local	Read-write
<input type="radio"/>	ILM Admins (read-write)	a528c0c2-2417-4559-86ed-f0d2e31da820	Local	Read-write
<input type="radio"/>	Maintenance Users	7e3400ec-de8c-45a7-8bb8-e1496b362a8d	Local	Read-write


Group Type:  Show  rows per page

2. Select **Add**.


The Add Group dialog box appears.


## Add Group

Create a new local group or import a group from the external identity source.












Group Type   Local  Federated

Display Name

Unique Name 

Access Mode   Read-write  Read-only

### Management Permissions

- |  |   |
|--|---|
| <input type="checkbox"/> Root Access                  | <input type="checkbox"/> Manage Alerts                     |
| <input type="checkbox"/> Acknowledge Alarms           | <input type="checkbox"/> Grid Topology Page Configuration  |
| <input type="checkbox"/> Other Grid Configuration     | <input type="checkbox"/> Tenant Accounts                   |
| <input type="checkbox"/> Change Tenant Root Password  | <input type="checkbox"/> Maintenance                       |
| <input type="checkbox"/> Metrics Query                | <input type="checkbox"/> ILM                                 |
| <input type="checkbox"/> Object Metadata Lookup      | <input type="checkbox"/> Storage Appliance Administrator  |

Cancel

Save

- For Group Type, select **Local** if you want to create a group that will be used only within StorageGRID, or select **Federated** if you want to import a group from the identity source.
- If you selected **Local**, enter a display name for the group. The display name is the name that appears in the Grid Manager. For example, "Maintenance Users" or "ILM Administrators."
- Enter a unique name for the group.
  - Local**: Enter whatever unique name you want. For example, "ILM Administrators."
  - Federated**: Enter the group's name exactly as it appears in the configured identity source.
- 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.

- Select one or more management 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.

8. Select **Save**.

The new group is created. If this is a local group, you can now add one or more users. If this is a federated group, the identity source manages which users belong to the group.

## Related information

[Managing local users](#)

## Admin 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.

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

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.

### Manage Alerts

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

### Acknowledge Alarms (legacy system)

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.

## Grid Topology Page Configuration

This permission provides access to the following menu options:

- Configuration tabs available from the pages in **Support > Tools > Grid Topology**.
- **Reset event counts** link on the **Nodes > Events** tab.

## Other Grid Configuration

This permission provides access to additional grid configuration options.



To see these additional options, users must also have the Grid Topology Page Configuration permission.

- **Alarms** (legacy system):
  - Global Alarms
  - Legacy Email Setup
- **ILM**:
  - Storage Pools
  - Storage Grades
- **Configuration > Network Settings**
  - Link Cost
- **Configuration > System Settings**:
  - Display Options
  - Grid Options
  - Storage Options
- **Configuration > Monitoring**:
  - Events
- **Support**:
  - AutoSupport

## Tenant Accounts

This permission provides access to the **Tenants > Tenant Accounts** page.



Version 1 of the Grid Management API (which has been deprecated) uses this permission to manage tenant group policies, reset Swift admin passwords, and manage root user S3 access keys.

## Change Tenant Root Password

This permission provides access to the **Change Root Password** option on the Tenant Accounts page, allowing you to control who can change the password for the tenant's local root user. Users who do not have this permission cannot see the **Change Root Password** option.



You must assign the Tenant Accounts permission to the group before you can assign this permission.

## Maintenance

This permission provides access to the following menu options:

- **Configuration > System Settings:**
    - Domain Names\*
    - Server Certificates\*
  - **Configuration > Monitoring:**
    - Audit\*
  - **Configuration > Access Control:**
    - Grid Passwords
  - **Maintenance > Maintenance Tasks**
    - Decommission
    - Expansion
    - Recovery
  - **Maintenance > Network:**
    - DNS Servers\*
    - Grid Network\*
    - NTP Servers\*
  - **Maintenance > System:**
    - License\*
    - Recovery Package
    - Software Update
  - **Support > Tools:**
    - Logs
- Users who do not have the Maintenance permission can view, but not edit, the pages marked with an asterisk.

## 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.

## ILM

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

- **Erasure Coding**
- **Rules**
- **Policies**

## • Regions



Access to the **ILM > Storage Pools** and **ILM > Storage Grades** menu options is controlled by the Other Grid Configuration and Grid Topology Page Configuration permissions.

### Object Metadata Lookup

This permission provides access to the **ILM > Object Metadata Lookup** menu option.

### Storage Appliance Administrator

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

### 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.

### Deactivating features from the Grid Management 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 the 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.*

#### Reactivating 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.

For details, see the instructions for implementing S3 or Swift client applications.

## Steps

1. Access the Swagger documentation for 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.”

4. 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.



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 } }
```

## Related information

[Using the Grid Management API](#)

## Modifying an admin group

You can modify an admin group to change the permissions associated with the group. For local admin groups, you can also update the display name.

### What you'll need

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

## Steps

1. Select **Configuration > Access Control > Admin Groups**.
2. Select the group.

If your system includes more than 20 items, you can specify how many rows are shown on each page at



one time. You can then use your browser's find feature to search for a specific item in the currently displayed rows.

3. Click **Edit**.
4. Optionally, for local groups, enter the group's name that will appear to users, for example, "Maintenance Users."

You cannot change the unique name, which is the internal group name.

5. Optionally, change the group's Access Mode.
  - **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.

6. Optionally, add or remove group permissions.

See information about admin group permissions.

7. Select **Save**.

#### Related information

[Admin group permissions](#)

## Deleting an admin 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 admin users from the group, but does not delete the admin users.

#### What you'll need

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

#### About this task

When you delete a group, users assigned to that group will lose all access privileges to the Grid Manager, unless they are granted privileges by a different group.

#### Steps

1. Select **Configuration > Access Control > Admin Groups**.
2. Select the name of the group.

If your system includes more than 20 items, you can specify how many rows are shown on each page at one time. You can then use your browser's find feature to search for a specific item in the currently displayed rows.

3. Select **Remove**.

4. Select **OK**.

## Managing local users

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

The Grid Manager includes one predefined local user, named “root.” Although you can add and remove local users, you cannot remove the root user.



If single sign-on (SSO) has been enabled, local users cannot sign in to StorageGRID.

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

### Creating a local user

If you have created local admin groups, you can create one or more local users and assign each user to one or more groups. The group’s permissions control which Grid Manager features the user can access.

#### About this task

You can only create local users, and you can only assign these users to local admin groups. Federated users and federated groups are managed using the external identity source.

#### Steps

1. Select **Configuration > Access Control > Admin Users**.
2. Click **Create**.
3. Enter the user’s display name, unique name, and password.
4. Assign the user to one or more groups that govern the access permissions.

The list of group names is generated from the Groups table.

5. Click **Save**.

#### Related information

[Managing admin groups](#)

### Modifying a local user’s account

You can modify a local admin user’s account to update the user’s display name or group membership. You can also temporarily prevent a user from accessing the system.

#### About this task

You can edit local users only. Federated user details are automatically synchronized with the external identity source.

#### Steps

1. Select **Configuration > Access Control > Admin Users**.
2. Select the user you want to edit.

If your system includes more than 20 items, you can specify how many rows are shown on each page at one time. You can then use your browser's find feature to search for a specific item in the currently displayed rows.

3. Click **Edit**.
4. Optionally, make changes to the name or group membership.
5. Optionally, to prevent the user from accessing the system temporarily, check **Deny Access**.
6. Click **Save**.

The new settings are applied the next time the user signs out and then signs back in to the Grid Manager.

## Deleting a local user's account

You can delete accounts for local users that no longer require access to the Grid Manager.

### Steps

1. Select **Configuration > Access Control > Admin Users**.
2. Select the local user you want to delete.



You cannot delete the predefined root local user.

If your system includes more than 20 items, you can specify how many rows are shown on each page at one time. You can then use your browser's find feature to search for a specific item in the currently displayed rows.

3. Click **Remove**.
4. Click **OK**.

## Changing a local user's password

Local users can change their own passwords using the **Change Password** option in the Grid Manager banner. In addition, users who have access to the Admin Users page can change passwords for other local users.

### About this task

You can change passwords for local users only. Federated users must change their own passwords in the external identity source.

### Steps

1. Select **Configuration > Access Control > Admin Users**.
2. From the Users page, select the user.

If your system includes more than 20 items, you can specify how many rows are shown on each page at one time. You can then use your browser's find feature to search for a specific item in the currently displayed rows.

3. Click **Change Password**.
4. Enter and confirm the password, and click **Save**.

# Using single sign-on (SSO) for StorageGRID

The StorageGRID system supports single sign-on (SSO) using the Security Assertion Markup Language 2.0 (SAML 2.0) standard. When SSO is enabled, all users must be authenticated by an external identity provider before they can access the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API. Local users cannot sign in to StorageGRID.

- [How single sign-on works](#)
- [Requirements for using single sign-on](#)
- [Configuring single sign-on](#)

## How single sign-on works

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

### Signing in when SSO is enabled

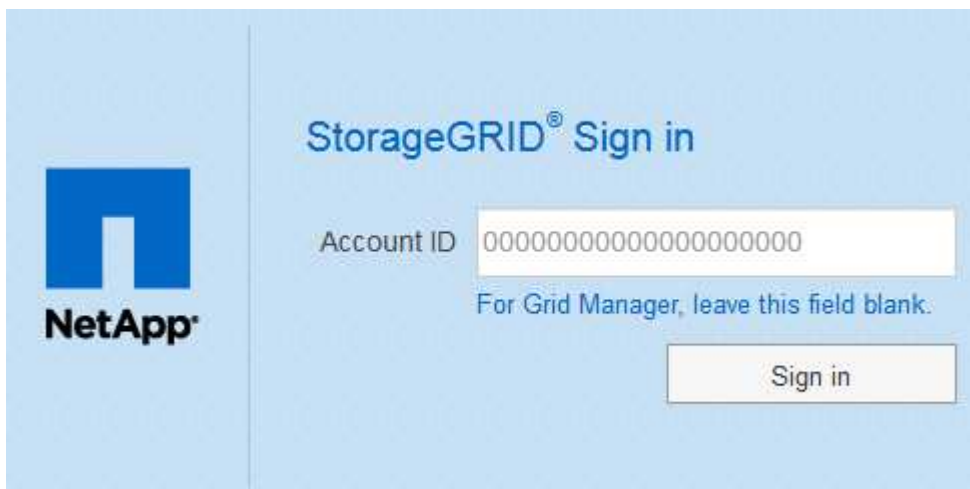
When SSO is enabled and you sign in to StorageGRID, you are redirected to your organization's SSO page to validate your credentials.

#### Steps

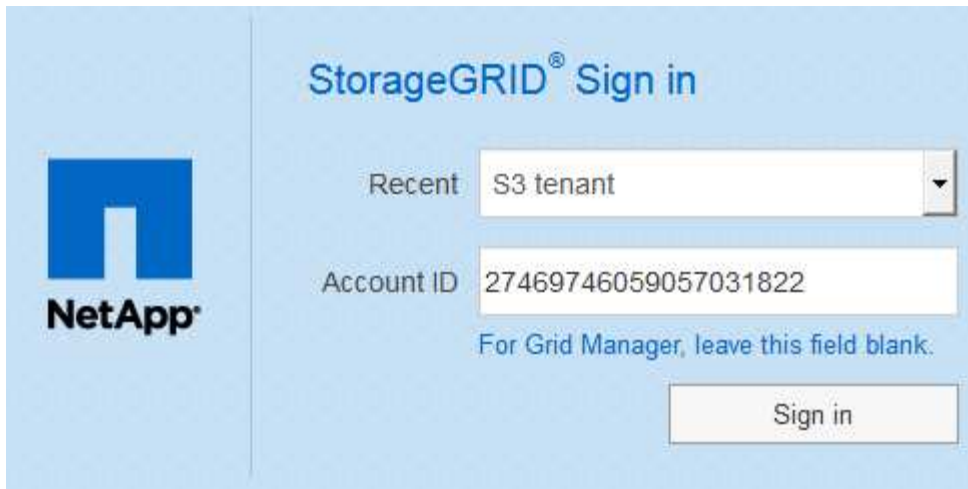
1. Enter the fully qualified domain name or IP address of any StorageGRID Admin Node in a web browser.

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:



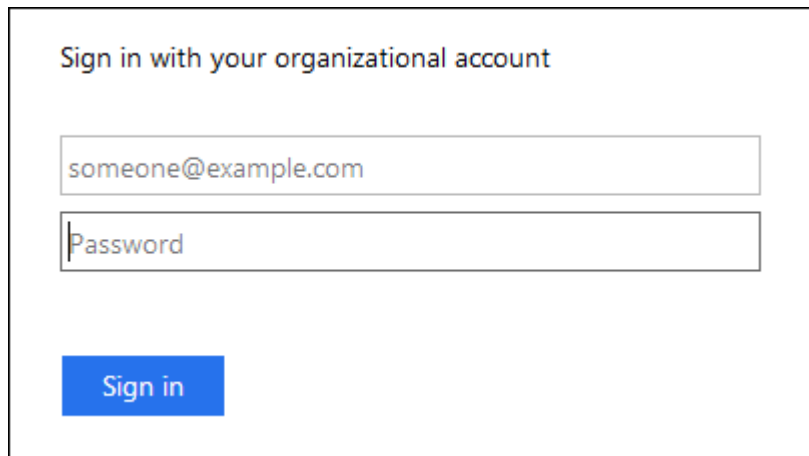
The screenshot shows the StorageGRID Sign in page. On the left is the NetApp logo. The main heading is "StorageGRID® Sign in". Below the heading, there is a "Recent" dropdown menu with "S3 tenant" selected. Below that is an "Account ID" text input field containing "27469746059057031822". A note below the field says "For Grid Manager, leave this field blank." At the bottom right is a "Sign in" button.



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. Click **Sign in**

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



The screenshot shows an SSO sign-in page with the heading "Sign in with your organizational account". It features two text input fields: the first contains "someone@example.com" and the second is labeled "Password". Below the fields is a blue "Sign in" button.

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 that has adequate access permission, you are signed in to the Grid Manager or the Tenant Manager, depending on which account you selected.

- 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.

### Signing 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

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



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.

#### Identity provider requirements

The identity provider (IdP) for SSO must meet the following requirements:

- Either of the following versions of Active Directory Federation Service (AD FS):
  - AD FS 4.0, included with Windows Server 2016



Windows Server 2016 should be using the [KB3201845 update](#), or higher.

- AD FS 3.0, included with Windows Server 2012 R2 update, or higher.
- Transport Layer Security (TLS) 1.2 or 1.3
- Microsoft .NET Framework, version 3.5.1 or higher

## Server certificate requirements

StorageGRID uses a Management Interface Server 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 SSO relying party trusts for StorageGRID in AD FS, you use the server certificate as the signature certificate for StorageGRID requests to AD FS.

If you have not already installed a custom server 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.



Using an Admin Node's default server certificate in the AD FS relying party trust 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 in AD FS 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`.

## Related information

[Controlling access through firewalls](#)

[Configuring a custom server certificate for the Grid Manager and the Tenant Manager](#)

## Configuring 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.

- [Confirming federated users can sign in](#)
- [Using sandbox mode](#)
- [Creating relying party trusts in AD FS](#)
- [Testing relying party trusts](#)
- [Enabling single sign-on](#)
- [Disabling single sign-on](#)
- [Temporarily disabling and reenabling single sign-on for one Admin Node](#)

## Confirming 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 must be signed in to the Grid Manager using a supported browser.
- You must have specific access permissions.
- You are using Active Directory as the federated identity source and AD FS as the identity provider.

### [Requirements for using single sign-on](#)

### 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 Control > 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 click **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 click **Edit Account**.
    - c. If the **Uses Own Identity Source** check box is selected, uncheck the box and click **Save**.



## Edit Tenant Account

### Tenant Details

Display Name

Uses Own Identity Source

Allow Platform Services

Storage Quota (optional)

Cancel

Save

The Tenant Accounts page appears.

- d. Select the tenant account, click **Sign In**, and sign in to the tenant account as the local root user.
- e. From the Tenant Manager, click **Access Control > Groups**.
- f. Ensure that at least one federated group from the Grid Manager has been assigned the Root Access permission for this tenant.
- g. Sign out.
- h. Confirm you can sign back in to the tenant as a user in the federated group.

### Related information

[Requirements for using single sign-on](#)

[Managing admin groups](#)

[Use a tenant account](#)

### Using sandbox mode

You can use sandbox mode to configure and test Active Directory Federation Services (AD FS) relying party trusts before you enforce single sign-on (SSO) for StorageGRID users. After SSO is enabled, you can reenabling sandbox mode to configure or test new and existing relying party trusts. Reenabling sandbox mode temporarily disables SSO for StorageGRID users.

### What you'll need

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

### About this task

When SSO is enabled and a user attempts to sign in to an Admin Node, StorageGRID sends an authentication request to AD FS. In turn, AD FS sends an authentication response back to StorageGRID, indicating whether the authorization request was successful. For successful requests, the response includes a universally unique identifier (UUID) for the user.

To allow StorageGRID (the service provider) and AD FS (the identity provider) to communicate securely about user authentication requests, you must configure certain settings in StorageGRID. Next, you must use AD FS to create a relying party trust for every 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.



Using sandbox mode is highly recommended, but not strictly required. If you are prepared to create AD FS relying party trusts immediately after you configure SSO in StorageGRID, and you do not need to test the SSO and single logout (SLO) processes for each Admin Node, click **Enabled**, enter the StorageGRID settings, create a relying party trust for each Admin Node in AD FS, and then click **Save** to enable SSO.

## Steps

1. Select **Configuration > Access Control > Single Sign-on**.

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

### Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status    Disabled    Sandbox Mode    Enabled

Save



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

2. Select the **Sandbox Mode** option.

The Identity Provider and Relying Party settings appear. In the Identity Provider section, the **Service Type** field is read only. It shows the type of identity federation service you are using (for example, Active Directory).

3. In the Identity Provider section:

- a. Enter the Federation Service name, exactly as it appears in AD FS.



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 whether you want to use Transport Layer Security (TLS) 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 and paste the certificate in the **CA Certificate** text box.

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

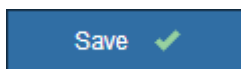
4. In the Relying Party section, specify the relying party identifier you will use for StorageGRID Admin Nodes when you configure relying party trusts.

- 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 includes a relying party identifier for each Admin Node, based on the node's hostname.

NOTE: 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.

5. Click **Save**.

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



- The Sandbox mode confirmation notice appears, confirming that sandbox mode is now enabled. You can use this mode while you use AD FS to configure a relying party trust for each Admin Node and test the single sign-in (SSO) and single logout (SLO) processes.

### Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status    Disabled    Sandbox Mode    Enabled

**Sandbox mode**

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

### Related information

[Requirements for using single sign-on](#)

### Creating 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.

### Creating a relying party trust using Windows PowerShell

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

#### What you'll need

- You have configured SSO in StorageGRID, and you know the fully qualified domain name (or the IP address) and the relying party identifier for each Admin Node in your system.



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.

#### About this task

These instructions apply to AD FS 4.0, which is included with Windows Server 2016. If you are using AD FS 3.0, which is included with Windows 2012 R2, you will notice slight differences in the procedure. See the Microsoft AD FS documentation if you have questions.

#### Steps

1. From the Windows start menu, right-click the PowerShell icon, and select **Run as Administrator**.
2. At the PowerShell command prompt, enter the following command:

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifier" -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. Click **Apply**, and click **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. Click **Add rule**.
  - d. On the Select Rule Template page, select **Send LDAP Attributes as Claims** from the list, and click **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. Click **Finish**, and click **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.

### Creating 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.

#### What you'll need

- You have configured SSO in StorageGRID, and you know the fully qualified domain name (or the IP address) and the relying party identifier for each Admin Node in your system.



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.

#### About this task

These instructions apply to AD FS 4.0, which is included with Windows Server 2016. If you are using AD FS 3.0, which is included with Windows 2012 R2, you will notice slight differences in the procedure. See the Microsoft AD FS documentation if you have questions.

## Steps

1. In Windows Server Manager, click **Tools**, and then select **AD FS Management**.
2. Under Actions, click **Add Relying Party Trust**.
3. On the Welcome page, choose **Claims aware**, and click **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.



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. Click **Add rule**:
  - c. On the Select Rule Template page, select **Send LDAP Attributes as Claims** from the list, and click **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. Click **Finish**, and click **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.

## Creating a relying party trust manually

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

### What you'll need

- You have configured SSO in StorageGRID, and you know the fully qualified domain name (or the IP address) and the relying party identifier for each Admin Node in your system.



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 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.
- 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.

### About this task

These instructions apply to AD FS 4.0, which is included with Windows Server 2016. If you are using AD FS 3.0, which is included with Windows 2012 R2, you will notice slight differences in the procedure. See the Microsoft AD FS documentation if you have questions.

### Steps

1. In Windows Server Manager, click **Tools**, and then select **AD FS Management**.
2. Under Actions, click **Add Relying Party Trust**.
3. On the Welcome page, choose **Claims aware**, and click **Start**.
4. Select **Enter data about the relying party manually**, and click **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.



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

6. To start the Claim Rule wizard, click **Add rule**:
  - a. On the Select Rule Template page, select **Send LDAP Attributes as Claims** from the list, and click **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. Click **Finish**, and click **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. Click **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. Click **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. Click **Apply**, and click **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.

### Testing relying party trusts

Before you enforce the use of single sign-on (SSO) for StorageGRID, confirm that single sign-on and single logout (SLO) are correctly configured. If you created a relying party trust for each Admin Node, confirm you can use SSO and SLO for each Admin Node.

### What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have specific access permissions.
- You have configured one or more relying party trusts in AD FS.

### Steps

1. Select **Configuration > Access Control > Single Sign-on**.

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

2. In the instructions for sandbox mode, locate the link to your identity provider's sign-on page.

The URL is derived from the value you entered in the **Federated Service Name** field.

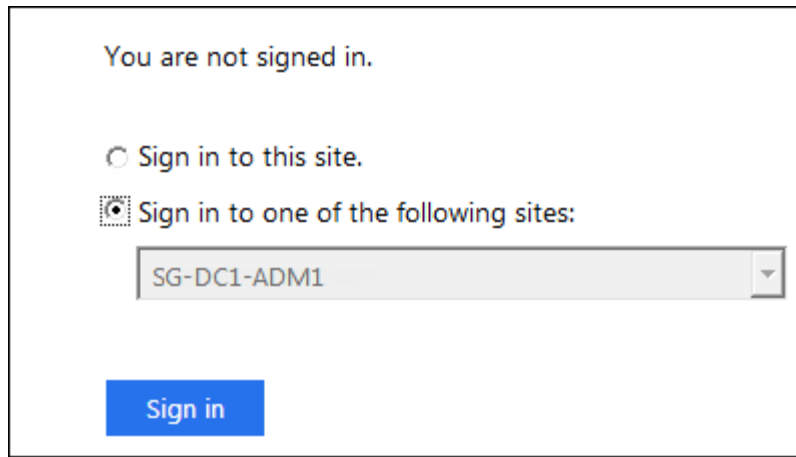
#### Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

3. Click the link, or copy and paste the URL into a browser, to access your identity provider's sign-on page.
4. 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 click **Sign in**.



You are prompted to enter your username and password.

5. Enter your federated username and password.
  - 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.
6. Repeat the previous steps to confirm you can sign in to any other Admin Nodes.

If all SSO sign-in and logout operations are successful, you are ready to enable SSO.

## Enabling single sign-on

After using sandbox mode to test all of your StorageGRID relying party trusts, you are ready to enable single sign-on (SSO).

### What you'll need

- You must have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts.
- You must have tested all relying party trusts using sandbox mode.

### Steps

1. Select **Configuration > Access Control > Single Sign-on**.

The Single Sign-on page appears with **Sandbox Mode** selected.

2. Change the SSO Status to **Enabled**.
3. Click **Save**.

A warning message appears.

## Warning

### Enable single sign-on

After you enable SSO, no local users—including the root user—will be able to sign in to the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API.

Before proceeding, confirm the following:

- You have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts.
- You have tested all relying party trusts using sandbox mode.

Are you sure you want to enable single sign-on?

Cancel

OK

4. Review the warning, and click **OK**.

Single sign-on is now 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.

### Disabling 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 must be signed in to the Grid Manager using a supported browser.
- You must 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. Click **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. Click **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 disabling and reenabling 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 must have specific access permissions.
- You must have the `Passwords.txt` file.
- You must 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.



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. Click **Save**.

Clicking **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. Click **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.

#### Related information

[Configuring single sign-on](#)

## Configuring administrator client certificates

You can use client certificates to allow authorized external clients to access the StorageGRID Prometheus database. Client certificates provide a secure way to use external tools to monitor StorageGRID.

If you need to access StorageGRID using an external monitoring tool, you must upload or generate a client certificate using the Grid Manager and copy the certificate information to the external tool.

## Adding administrator client certificates

To add a client certificate, you can provide your own certificate or generate one using the Grid Manager.

### What you'll need

- You must have the Root Access permission.
- You must be signed in to the Grid Manager using a supported browser.
- You must know the IP address or domain name of the Admin Node.
- You must have configured the StorageGRID Management Interface Server Certificate and have the corresponding CA bundle
- If you want to upload your own certificate, the public key and private key for the certificate must be available on your local computer.

### Steps

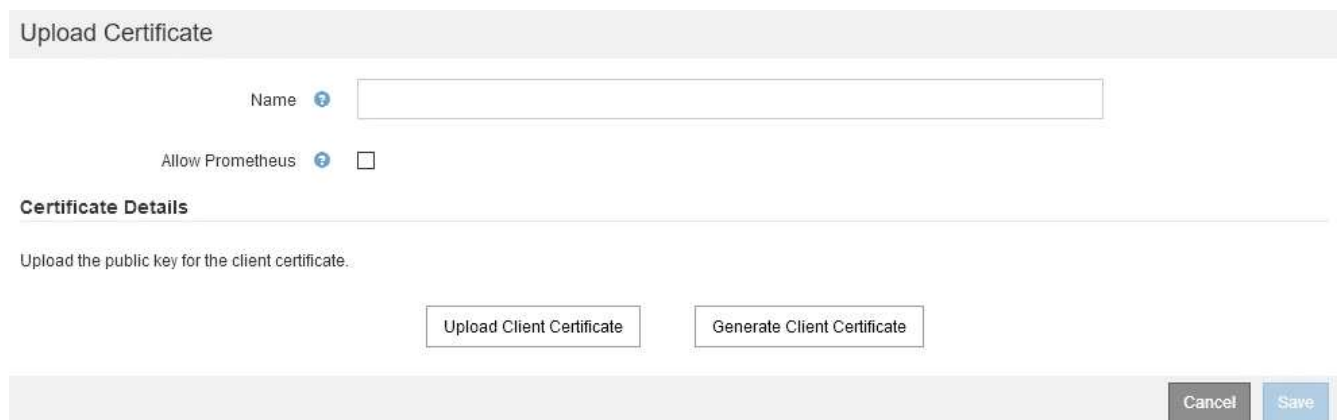
1. In the Grid Manager, select **Configuration > Access Control > Client Certificates**.

The Client Certificates page appears.



2. Select **Add**.

The Upload Certificate page appears.



3. Type a name between 1 and 32 characters for the certificate.
4. To access Prometheus metrics using your external monitoring tool, select the **Allow Prometheus** check box.
5. Upload or generate a certificate:
  - a. To upload a certificate, go [here](#).
  - b. To generate a certificate, go [here](#).

6. To upload a certificate:
  - a. Select **Upload Client Certificate**.
  - b. Browse for the public key for the certificate.

After you upload the public key for the certificate, the **Certificate metadata** and **Certificate PEM** fields are populated.

Upload Certificate

Name ?

Allow Prometheus ?

**Certificate Details**

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Uploaded file name: client (1).crt

Certificate metadata ?

```

Subject DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Serial Number: 0D:0E:FC:16:75:B8:BE:3E:7D:47:4D:05:49:08:F3:7B:E8:4A:71:90
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Issued On: 2020-06-19T22:11:56.000Z
Expires On: 2021-06-19T22:11:56.000Z
SHA-1 Fingerprint: 13:AA:D6:06:2B:90:FE:B7:7B:EB:1A:83:BE:C3:62:39:B7:A6:E7:F0
SHA-256 Fingerprint: 5C:29:06:6B:CF:81:50:B8:4F:A9:56:F7:A7:AB:3C:36:FA:3D:B7:32:A4:C9:74:85:2C:8D:E6:67:37:C3:AC:60
          
```

Certificate PEM ?

```

-----BEGIN CERTIFICATE-----
MIIDmzCCAoOgAwIBAgIUUDQ78FnW4vj59R00FSQjze+hKcZAwDQYJKoZIhvcNAQEL
BQAwDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbgG1mb3JuaWEwEjAQBgNVBAcM
CVN1bm55dmFsZTEUMBIGA1UECgwLRXhhbXBsZS5BdDBy4xCzAJBgNVBAsMAk1UMRkw
FwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMB4XDTEwMDYxOTIyMTE1N1oXDTEwMDYx
OTIyMTE1N1owDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbgG1mb3JuaWEwEjAQB
BgNVBAcMNVN1bm55dmFsZTEUMBIGA1UECgwLRXhhbXBsZS5BdDBy4xCzAJBgNVBAsM
Ak1UMRkwFwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBcGkCAQEAAVgq2MNjvVotLeGtq1Co4coJmsQ2ygrRhuwSza0bgMnjf
cwUgHNVPXGuG1zY/Tl37r3Dk5buZfyGYAeJ6mqbQA6cE3ypOp5Hx7Cm/ANJkmFw6
          
```

Copy certificate to clipboard


Cancel


Save

- c. Select **Copy certificate to clipboard** and paste the certificate to your external monitoring tool.
  - d. Use an editing tool to copy and paste the private key to your external monitoring tool.
  - e. Select **Save** to save the certificate in the Grid Manager.
7. To generate a certificate:
  - a. Select **Generate Client Certificate**.
  - b. Enter the domain name or IP address of the Admin Node.
  - c. Optionally, enter an X.509 subject, also referred to as the Distinguished Name (DN), to identify the administrator who owns the certificate.
  - d. Optionally, select the number of days the certificate is valid. The default is 730 days.
  - e. Select **Generate**.

The **Certificate metadata**, **Certificate PEM**, and **Certificate private key** fields are populated.


Upload Certificate

Name  test-certificate-generate


Allow Prometheus 

**Certificate Details**


Upload the public key for the client certificate.

**Certificate metadata** 


```
Subject DN: /CN=test.com
Serial Number: 08:F8:FB:78:B2:13:E4:DF:54:83:3D:35:56:6F:2A:03:53:B0:E2:0
A
Issuer DN: /CN=test.com
Issued On: 2020-11-20T22:44:46.000Z
Expires On: 2022-11-20T22:44:46.000Z
SHA-1 Fingerprint: 6E:DB:8C:F8:3E:20:88:E4:C6:42:52:5F:32:7E:E7:93:66:69:F3:3
D
SHA-256 Fingerprint: 73:D3:51:83:ED:D3:89:AD:7B:89:4C:AF:AE:34:76:B6:42:FE:0D:
EF:78:C0:A4:66:C2:EB:65:64:C3:D4:7A:B0
```

**Certificate PEM** 

```
-----BEGIN CERTIFICATE-----
MIICyxCChbOgAwIBAgIUCPj7dxITSN9Ugz01Vm8qA1Ow4gwwDQYJKoZIhvcNAQEL
BQAwEzERMAsGA1UEAwwIdGVudC5jb20wHhcNMjA1MTIwNDQ2WWhcMjIwNDQ2W
MjI0NDQ2WjATMREwDwYDVQQDDAh0ZXN0LmNvbTCCASAwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAR02dB9mx2jFrGuBb2ZMjcidf/tcKxLb8Gm+4vIwt1gwrR
KgH291B9YIQn/Vo729R2mNKRyBwkyQTkGCO2Ixxv0STBLEIWFb3eTgcIcMyt1V1F
OasBWy402xxjnK3/X+AX+6x2WZLsVe+3CDjGu4ic0V/uVQax4yA1T9SoEnjBmOa
LCVjL6iVnkUGS8GkyUFeOaoMjsL6TN1QeoFv9VEB0xBKCP4D7FDbaIy2f9Ng5rS
EEOQLNtNxCasLO4D7j2qFqOYUpFJ3MOoh1x0nSpQ7825KfYwVtDKg5v52P9UBM
1o8GeucofaW+dbpLZhp09N1VtFhqbXe9AaxN8e+kCAwEAAaMXMBUwEwYDVROBBAw
```

**Certificate private key** 

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAT2OH2bHaM+sa4Fv2kyNyJ1/+1NwEu0Eab718jC2KWC/BFe
AdneUH1ghCf9Wjwb1HaY0oxIHCTJBOQYI6kjG+/RjMEt4h29eKxOBwigsK2VWU7
OwF2jPg7bP6Ooxf964Bf7xN12kixV75IICMa7iJaRX+5VDPHjIDVP1KqgeM9Y5oe
JWmVqJwRQYFI2uTJQ948qgyOwvpm2VDOgW/1UQHTeEoKngFeUNtojLZ/02DmtJS
Q8Cge202xoxJxm7gPulNmoW65h8kUncw6iHXH8fmlDvxnkp9j5W0MqDm/nY/xQEw
jw266h9pb51uk+k2k703VW0WGPCFd70DPE3yyOQIDAQABaoIBAQCFEUY4pE0Hqev
2uEL6De4yXMTwG/8Gn+W8mvdgQB4xWEGQxk1kiEUG+HTYxrfJen6XXOvACDYAC/
Hh1Q67xDVpRjdpuR0xr1W8evveEmpBw99MgH9Y2UGx6Yub9USJaqfDv7A4Nvaon
MxaYJREBlvAR7f2x2xXVY8b0zRPAjznoYCa1Lor5YOK73e0G8naTmwIdm2Ym6EE
```

 You will not be able to view the certificate private key after you close this dialog. To save the keys for future reference, copy and paste the values to another location.

f. Select **Copy certificate to clipboard** and paste the certificate to your external monitoring tool.

g. Select **Copy private key to clipboard** and paste the key to your external monitoring tool.



You will not be able to view the private key after you close the dialog box. Copy the key to a safe location.

h. Select **Save** to save the certificate in the Grid Manager.

8. Configure the following settings on your external monitoring tool, such as Grafana.



A Grafana example is shown in the following screenshot:

The screenshot displays the Grafana configuration interface for a Prometheus connection. The 'Name' field is set to 'sg-prometheus' and is marked as the 'Default' connection with a toggle switch. The 'HTTP' section includes a 'URL' field set to 'https://admin-node.example.com:9091', an 'Access' dropdown set to 'Server (default)', and a 'Whitelisted Cookies' section with an 'Add' button. The 'Auth' section has several toggle switches: 'Basic auth' (off), 'With Credentials' (off), 'TLS Client Auth' (on), 'With CA Cert' (on), 'Skip TLS Verify' (off), and 'Forward OAuth Identity' (off). The 'TLS/SSL Auth Details' section shows 'CA Cert' and 'Client Cert' fields, both containing the text 'Begins with ---BEGIN CERTIFICATE---'. The 'ServerName' field is set to 'admin-node.example.com'.

a. **Name:** Enter a name for the connection.

StorageGRID does not require this information, but you must provide a name to test the connection.

b. **URL:** Enter the domain name or IP address for the Admin Node. Specify HTTPS and port 9091.

For example: `https://admin-node.example.com:9091`

- c. Enable **TLS Client Authorization** and **With CA Cert**.
- d. Copy and paste the Management Interface Server Certificate or CA bundle to **CA Cert** under TLS/SSL Auth Details.
- e. **ServerName**: Enter the domain name of the Admin Node.

ServerName must match the domain name as it appears in the Management Interface Server Certificate.

- f. Save and test the certificate and private key that you copied from StorageGRID or a local file.

You can now access the Prometheus metrics from StorageGRID with your external monitoring tool.

For information about the metrics, see the instructions for monitoring and troubleshooting StorageGRID.

### Related information

[Using StorageGRID security certificates](#)

[Configuring a custom server certificate for the Grid Manager and the Tenant Manager](#)

[Monitor & troubleshoot](#)

## Editing administrator client certificates

You can edit a certificate to change its name, enable or disable Prometheus access, or upload a new certificate when the current one has expired.

### What you'll need

- You must have the Root Access permission.
- You must be signed in to the Grid Manager using a supported browser.
- You must know the IP address or domain name of the Admin Node.
- If you want to upload a new certificate and private key, they must be available on your local computer.

### Steps

1. Select **Configuration > Access Control > Client Certificates**.

The Client Certificates page appears. The existing certificates are listed.

Certificate expiration dates are listed in the table. If a certificate will expire soon or is already expired, a message appears in the table and an alert is triggered.

<input type="button" value="+ Add"/> <input type="button" value="✎ Edit"/> <input type="button" value="✕ Remove"/>			
	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. Select the radio button to the left of the certificate you want to edit.
3. Select **Edit**.

The Edit Certificate dialog box appears.

Edit Certificate test-certificate-generate

Name

Allow Prometheus

---

**Certificate Details**

Upload the public key for the client certificate.

Upload Client Certificate
Generate Client Certificate

Certificate metadata

```

Subject DN: /CN=test.com
Serial Number: 0C:11:87:6C:1E:FD:13:16:F3:F2:06:D9:DA:6D:BC:CE:2A:A9:C3:53
Issuer DN: /CN=test.com
Issued On: 2020-11-23T15:53:33.000Z
Expires On: 2022-11-23T15:53:33.000Z
SHA-1 Fingerprint: AE:E6:70:A7:D3:C3:39:7A:09:F9:62:9B:81:8A:87:CD:43:16:89:A7
SHA-256 Fingerprint: 63:07:BF:FF:08:1E:84:F1:D4:67:C6:16:B0:35:26:00:C6:A3:13:11:7E:5E:9
0:EC:7A:7B:EF:23:14:55:3D:56

```

Certificate PEM

```

-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUDBGHbE79Exbz8gbZ2m28ziqpw1MwDQYJKoZIhvcNAQEL
BQAweERMASGA1UEAwIdGVzdC5jb20wHhcNMjAxMTIzMTU1MzZmWWhcNMjIxMTIz
MTU1MzZmWjAUMREwDwYDVQQDDAh0ZXN0LmNvbTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBBAKdgEeneCDFDs1jvlnX9ow6oPrdU7m2EN6SS6xdVI155sCH+
hkwO5a2Mym7EhbNrfwOt2nMjQkcaKIrk8OAmutRgG6N1N12FIW0qY0uzFQ0QddLq
n7ymFw6w8a9zYSu7bLp84Yn0/LSDPk+h3Jio7Mxt2X70Lt52DRwFmbLNvEvYEtTS
h+FbNh885AIRO2eLxvC0IRij1bySe7EwK+Wmc97HdxRSgyxIWk6BD47XC+d0rv55
wvtjc/41qc5xsE6XmJs2yJg4VAPr10y8Icwa9fz00+xPwIdC0NwXkpWJXeBnCoXx
YqQxbWzjr+iVLJqLTMxU8zTIT30zUqN00M82GJUCAwEAAaMKMBUwEwYDVR0RBAAw

```

Copy certificate to clipboard

Cancel Save

4. Make the desired changes to the certificate.
5. Select **Save** to save the certificate in the Grid Manager.
6. If you uploaded a new certificate:
  - a. Select **Copy certificate to clipboard** to paste the certificate to your external monitoring tool.
  - b. Use an editing tool to copy and paste the new private key to your external monitoring tool.
  - c. Save and test the certificate and private key in your external monitoring tool.
7. If you generated a new certificate:
  - a. Select **Copy certificate to clipboard** to paste the certificate to your external monitoring tool.
  - b. Select **Copy private key to clipboard** to paste the certificate to your external monitoring tool.



You will not be able to view or copy the private key after you close the dialog box. Copy the key to a safe location.

c. Save and test the certificate and private key in your external monitoring tool.

## Removing administrator client certificates

If you no longer need a certificate, you can remove it.

### What you'll need

- You must have the Root Access permission.
- You must be signed in to the Grid Manager using a supported browser.

### Steps

1. Select **Configuration > Access Control > Client Certificates**.

The Client Certificates page appears. The existing certificates are listed.

	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. Select the radio button to the left of the certificate you want to remove.
3. Select **Remove**.

A confirmation dialog box appears.

**Warning**

Delete certificate

Are you sure you want to delete the certificate "test-certificate-generate"?

Cancel OK

4. Select **OK**.

The certificate is removed.

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.