



Using single sign-on (SSO) for StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

This PDF was generated from <https://docs.netapp.com/us-en/storagegrid-115/admin/how-sso-works.html> on April 11, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Using single sign-on (SSO) for StorageGRID 1
 - How single sign-on works 1
 - Requirements for using single sign-on 3
 - Configuring single sign-on 4

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

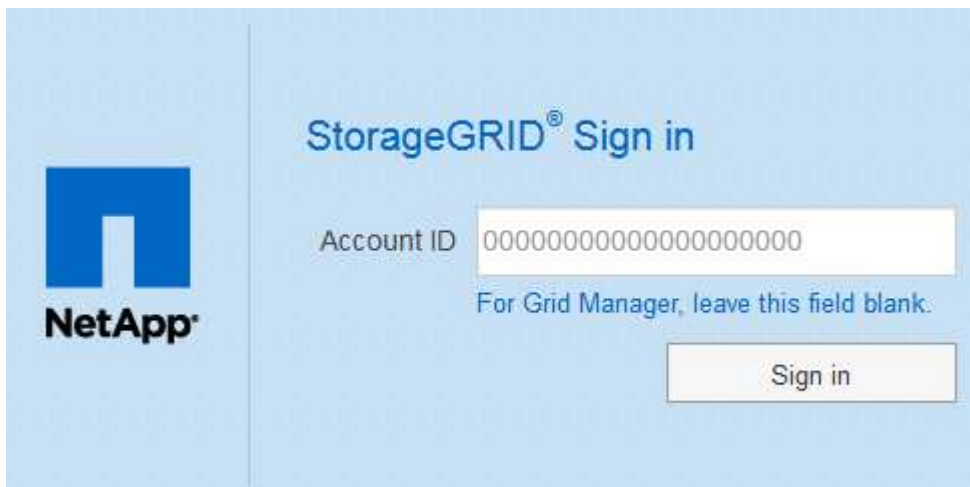
When SSO is enabled and you sign in to StorageGRID, you are redirected to your organization's SSO page to validate your credentials.

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:

A screenshot of the StorageGRID Sign in page. On the left is the NetApp logo. The main heading is 'StorageGRID® Sign in'. Below it is a text input field labeled 'Account ID' containing a long string of zeros. A note below the field says 'For Grid Manager, leave this field blank.' At the bottom right is a 'Sign in' button.

- 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:



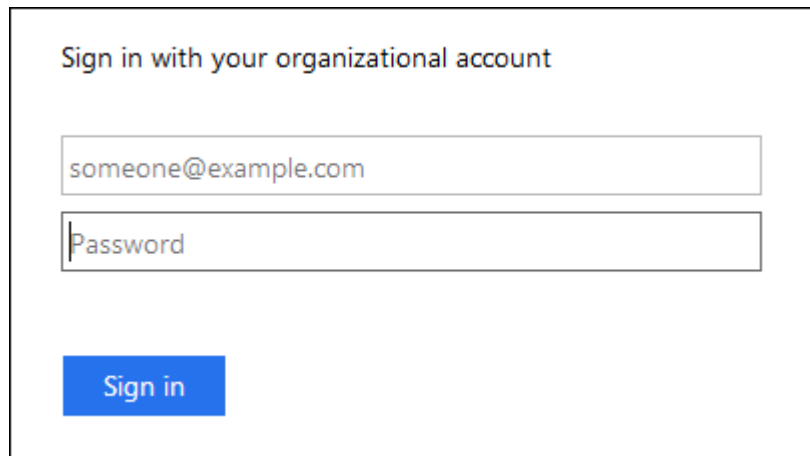
The image shows the StorageGRID Sign in page. On the left is the NetApp logo. The main heading is 'StorageGRID® Sign in'. Below this, there is a 'Recent' dropdown menu showing 'S3 tenant'. Below that is an 'Account ID' field containing the number '27469746059057031822'. A note below the field says 'For 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 image shows an example of an SSO sign-in page. The heading is 'Sign in with your organizational account'. Below this are two input fields: the first contains the email address 'someone@example.com' and the second is labeled 'Password'. At the bottom left 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.

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

You do not need to reenter your SSO credentials.

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

1. Locate the **Sign Out** link in the top-right corner of the user interface.
2. 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_Identifer" -MetadataURL  
"https://Admin_Node_FQDN/api/saml-metadata"
```

- For *Admin_Node_Identifier*, enter the Relying Party Identifier for the Admin Node, exactly as it appears on the Single Sign-on page. For example, SG-DC1-ADM1.
- For *Admin_Node_FQDN*, enter the fully qualified domain name for the same Admin Node. (If necessary, you can use the node's IP address instead. However, if you enter an IP address here, be aware that you must update or recreate this relying party trust if that IP address ever changes.)

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

The AD FS management tool appears.

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

The list of relying party trusts appears.

5. Add an Access Control Policy to the newly created relying party trust:
 - a. Locate the relying party trust you just created.
 - b. Right-click the trust, and select **Edit Access Control Policy**.
 - c. Select an Access Control Policy.

- d. 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 not signed in.

☐ Sign in to this site.

☒ Sign in to one of the following sites:

SG-DC1-ADM1

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](#)

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.