Set up SSO with SAML

StorageGRID software

NetApp
July 22, 2026

Table of Contents

Set up SSO with SAML

Learn about setting up SSO in StorageGRID using SAML

Setting up single sign-on (SSO) in StorageGRID allows StorageGRID (the service provider) and the SSO identity provider to communicate securely about user authentication requests.

You can set up SSO in StorageGRID using OpenID Connect (OIDC) or SAML. Follow these high-level steps to set up SSO in StorageGRID using SAML or learn about setting up SSO using OIDC.

Configure SSO

Select the Configure SSO wizard for SAML. Then, configure SSO with your identity provider and enter sandbox mode.

Learn about configuring SSO using SAML

Configure identity provider

Based on the SSO identity provider you plan to use, you can select either Active Directory or Entra ID for the identity federation LDAP service type.

- For Active Directory Federation Service (AD FS), you can use the AD FS, Entra ID, or PingFederate identity provider.
- For Entra ID, you can only use the Entra ID identity provider.

Use the SSO identity provider's software to configure SAML for each Admin Node in your grid.

- Learn about creating an application group for each Admin Node in Active Directory
- Learn about creating an application for each Admin Node in Entra ID
- Learn about creating a service provider connection for each Admin Node in PingFederate

Test configuration

After configuring SAML for each Admin Node, return to the Configure SSO wizard and test the configuration.

Learn about testing the configuration for SSO

Enable SSO

Enable SSO for all StorageGRID users.

Learn about enabling SSO for StorageGRID users

Configure SSO in StorageGRID using SAML

Follow the Configure SSO wizard for SAML and enter sandbox mode to configure and test single sign-on (SSO) before enabling it for all StorageGRID users. After you enable SSO, you can return to sandbox mode when needed to change or retest the configuration.

Before you begin

- You are signed in to the Grid Manager using a supported web browser.
- You have the Root access permission.
- You have configured identity federation for your StorageGRID system.
- For the identity federation **LDAP service type**, you selected either Active Directory or Entra ID, based on the SSO identity provider you plan to use.

Configured LDAP service type	Options for SSO identity provider
Active Directory Federation Service (AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

About this task

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

- The response from Active Directory or PingFederate includes a universally unique identifier (UUID) for the user.
- The response from Entra ID includes a User Principal Name (UPN).

To allow StorageGRID (the service provider) and the SSO identity provider to communicate securely about user authentication requests, you complete these tasks:

1. Configure settings in StorageGRID.
2. Use the SSO identity provider's software to create a relying party trust (AD FS), Enterprise Application (Entra ID), or Service Provider (PingFederate) for each Admin Node.
3. Return to StorageGRID to enable SSO.

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

Step 1: Provide identity provider details

Access the wizard and complete the fields on the Provide identity provider details page.

Steps

1. Access the wizard:
   a. Select **Configuration** > **Access control** > **Single sign-on**. The Single sign-on page appears.

      If the Configure SSO settings button is disabled, confirm you have configured the identity provider as the federated identity source. Refer to Requirements and considerations for single sign-on.

   b. Select **Configure SSO settings**. The Provide identity provider details page appears.
2. Under **Protocol**, select **SAML**.
3. Select the **SSO type** from the drop-down list.
4. If you selected Active Directory as the SSO type, enter the **Federation service name** for the identity provider, exactly as it appears in Active Directory Federation Service (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.

5. Specify which TLS certificate will be used to secure the connection when the identity provider sends SSO configuration information in response to StorageGRID requests.
   - **Use operating system CA certificate**: Use the default CA certificate installed on the operating system to secure the connection.
   - **Use custom CA certificate**: Use a custom CA certificate to secure the connection.

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

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

     If you change the CA certificate, immediately restart the mgmt-api service on the Admin Nodes and test for a successful SSO into the Grid Manager.

6. Select **Continue**. The Provide relying party identifier page appears.

Step 2: Provide relying party trusts, enterprise applications, or SP connections

Complete the fields in Step 2 of the wizard based on the SSO type you selected.

Active Directory

Complete the fields in the **Provide relying party identifier** step.

Steps

1. Specify the **Relying party identifier** for StorageGRID. This value controls the name you use for each relying party trust in AD FS.
   - For example, if your grid has only one Admin Node and you don't 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]`. Including this string results in a table that shows the relying party identifier for each Admin Node in the grid, based on the node's hostname.

   > ⓘ 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.

2. Select **Save and enter sandbox mode**.

Entra ID

Complete the fields in the **Configure enterprise applications** step.

Steps

1. In the Enterprise Application section, specify the **Enterprise application name** for StorageGRID. This value controls the name you use for each enterprise application in Entra ID.
   - For example, if your grid has only one Admin Node and you don't 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]`. Including this string results in a table that shows an enterprise application name for each Admin Node in your system, based on the node's hostname.

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

2. Follow the steps in Create enterprise applications in Entra ID to create an enterprise application for each Admin Node listed in the table.
3. From Entra ID, copy the federation metadata URL for each enterprise application. Then, paste this URL into the corresponding **Federation metadata URL** field in StorageGRID.
4. After you have copied and pasted a federation metadata URL for all Admin Nodes, select **Save and enter sandbox mode**.

PingFederate

Complete the fields in the **Provide SP connection ID** step.

Steps

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

- For example, if your grid has only one Admin Node and you don't 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]`. Including this string results in a table that shows the SP connection ID for each Admin Node in your system, based on the node's hostname.

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

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

   Use the following format:

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

3. Select **Save and enter sandbox mode**.

Step 3: Configure relying party trusts, enterprise applications, or SP connections

After you save the configuration and enter sandbox mode, you can complete and test the configuration for the SSO type you selected.

StorageGRID can remain in sandbox mode as long as required. However, only federated users and local users can sign in.

Active Directory

Steps

1. Go to Active Directory Federation Services (AD FS).
2. Create one or more relying party trusts for StorageGRID, using each relying party identifier shown in the table on the Configure SSO page.

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

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

Entra ID

Steps

1. From the Single sign-on page for the Admin Node you are currently signed in to, select the button to download and save the SAML metadata.
2. Then, for any other Admin Nodes in your grid, repeat these steps:
   a. Sign in to the node.
   b. Select **Configuration** > **Access control** > **Single sign-on**.
   c. Download and save the SAML metadata for that node.
3. Go to the Azure portal.
4. Follow the steps in Create enterprise applications in Entra ID to upload the SAML metadata file for each Admin Node into its corresponding Entra ID enterprise application.

PingFederate

Steps

1. From the Single sign-on page for the Admin Node you are currently signed in to, select the button to download and save the SAML metadata.
2. Then, for any other Admin Nodes in your grid, repeat these steps:
   a. Sign in to the node.
   b. Select **Configuration** > **Access control** > **Single sign-on**.
   c. Download and save the SAML metadata for that node.
3. Go to PingFederate.
4. Create one or more service provider (SP) connections for StorageGRID. Use the SP connection ID for each Admin Node (shown in the table on the Configure SSO page) and the SAML metadata you downloaded for that Admin Node.

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

Step 4: Test configuration

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

Active Directory

Steps

1. From the Configure SSO page, locate the link on the Test configuration step of the wizard.

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

2. Select the link, or copy and paste the URL into a browser, to access your identity provider's sign-on page.
3. To confirm you can use SSO to sign in to StorageGRID, select **Sign in to one of the following sites**, select the relying party identifier for your primary Admin Node, and select **Sign in**.
4. Enter your federated username and password.
   - If the SSO sign-in and logout operations are successful, a success message appears.
   - If the SSO operation is unsuccessful, an error message appears. Fix the issue, clear the browser's cookies, and try again.
5. Repeat these steps to verify the SSO connection for each Admin Node in your grid.

Entra ID

Steps

1. Go to the Single sign-on page in the Azure portal.
2. Select **Test this application**.
3. Enter the credentials of a federated user.
   - If the SSO sign-in and logout operations are successful, a success message appears.
   - If the SSO operation is unsuccessful, an error message appears. Fix the issue, clear the browser's cookies, and try again.
4. Repeat these steps to verify the SSO connection for each Admin Node in your grid.

PingFederate

Steps

1. From the Configure SSO page, select the first link in the Sandbox mode message.

   Select and test one link at a time.

2. Enter the credentials of a federated user.
   - If the SSO sign-in and logout operations are successful, a success message appears.
   - If the SSO operation is unsuccessful, an error message appears. Fix the issue, clear the browser's cookies, and try again.
3. Select the next link to verify the SSO connection for each Admin Node in your grid.

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

Step 5: Enable single sign-on

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

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

Steps

1. From the Test configuration step of the configure SSO wizard, select **Enable SSO**.
2. Review the warning message, and select **Enable SSO**.

   Single sign-on is now enabled. The Single sign-on page appears and now includes the details for the SSO you just configured.

3. To edit the configuration, select **Edit**.
4. To disable single sign-on, select **Disable SSO**.

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

What's next?

After configuring SSO using SAML, configure the identity provider for the Admin Nodes.

If your identity provider is…	You need to…
Active directory	Create an application group for each Admin Node
Entra ID	Create an application for each Admin Node
PingFederate	Create a service provider connection for each Admin Node

Create relying party trusts in AD FS for SAML in StorageGRID

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

Before you begin

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

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

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

About this task

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

Create a relying party trust using Windows PowerShell

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

Steps

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

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

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

   The AD FS management tool appears.
4. Select **AD FS** > **Relying Party Trusts**.

   The list of relying party trusts appears.
5. Add an Access Control Policy to the newly created relying party trust:
   a. Locate the relying party trust you just created.
   b. Right-click the trust, and select **Edit Access Control Policy**.
   c. Select an Access Control Policy.
   d. Select **Apply**, and select **OK**
6. Add a Claim Issuance Policy to the newly created Relying Party Trust:
   a. Locate the relying party trust you just created.
   b. Right-click the trust, and select **Edit claim issuance policy**.

c. Select **Add rule**.

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

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

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

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

g. In the LDAP Attribute column of the Mapping table, type **objectGUID** or select **User-Principal-Name**.

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

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

7. Confirm that the metadata was imported successfully.

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

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

If the metadata is missing, confirm that the Federation metadata address is correct, or 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're configured correctly.

Create a relying party trust by importing federation metadata

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

Steps

1. In Windows Server Manager, select **Tools**, and then select **AD FS Management**.
2. Under Actions, select **Add Relying Party Trust**.
3. On the Welcome page, choose **Claims aware**, and select **Start**.
4. Select **Import data about the relying party published online or on a local network**.
5. In **Federation metadata address (host name or URL)**, type the location of the SAML metadata for this Admin Node:

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

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

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

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

7. Add a claim rule:
   a. Right-click the trust, and select **Edit claim issuance policy**.
   b. Select **Add rule**:
   c. On the Select Rule Template page, select **Send LDAP Attributes as Claims** from the list, and select **Next**.
   d. On the Configure Rule page, enter a display name for this rule.

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

   e. For the Attribute Store, select **Active Directory**.
   f. In the LDAP Attribute column of the Mapping table, type **objectGUID** or select **User-Principal-Name**.
   g. In the Outgoing Claim Type column of the Mapping table, select **Name ID** from the drop-down list.
   h. Select **Finish**, and select **OK**.
8. Confirm that the metadata was imported successfully.
   a. Right-click the relying party trust to open its properties.
   b. Confirm that the fields on the **Endpoints**, **Identifiers**, and **Signature** tabs are populated.

      If the metadata is missing, confirm that the Federation metadata address is correct, or 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.

Create a relying party trust manually

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

Steps

1. In Windows Server Manager, select **Tools**, and then select **AD FS Management**.
2. Under Actions, select **Add Relying Party Trust**.
3. On the Welcome page, choose **Claims aware**, and select **Start**.
4. Select **Enter data about the relying party manually**, and select **Next**.
5. Complete the Relying Party Trust wizard:
   a. Enter a display name for this Admin Node.

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

   b. Skip the step to configure an optional token encryption certificate.
   c. On the Configure URL page, select the **Enable support for the SAML 2.0 WebSSO protocol** checkbox.
   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, select **Add rule**:
   a. On the Select Rule Template page, select **Send LDAP Attributes as Claims** from the list, and select **Next**.
   b. On the Configure Rule page, enter a display name for this rule.

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

   c. For the Attribute Store, select **Active Directory**.
   d. In the LDAP Attribute column of the Mapping table, type **objectGUID** or select **User-Principal-Name**.
   e. In the Outgoing Claim Type column of the Mapping table, select **Name ID** from the drop-down list.
   f. Select **Finish**, and select **OK**.
7. Right-click the relying party trust to open its properties.
8. On the **Endpoints** tab, configure the endpoint for single logout (SLO):
   a. Select **Add SAML**.
   b. Select **Endpoint Type** > **SAML Logout**.
   c. Select **Binding** > **Redirect**.
   d. In the **Trusted URL** field, enter the URL used for single logout (SLO) from this Admin Node:

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

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

   e. Select **OK**.
9. On the **Signature** tab, specify the signature certificate for this relying party trust:
   a. Add the custom certificate:
      - If you have the custom management certificate you uploaded to StorageGRID, select that certificate.

- If you don't 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.

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

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

The Relying Party properties are saved and closed.

10. Repeat these steps to configure a relying party trust for all of the Admin Nodes in your StorageGRID system.
11. When you are done, return to StorageGRID and test all relying party trusts to confirm they are configured correctly.

Create enterprise applications in Entra ID for SAML in StorageGRID

Use Entra ID to create an enterprise application for each Admin Node for SAML in your system.

Before you begin

- You have started configuring single sign-on for StorageGRID and you selected **Entra ID** as the SSO type.
- You have entered sandbox mode in Grid Manager.
- You have the **Enterprise application name** for each Admin Node in your system. You can copy these values from the Admin Node details table on the Configure SSO page.

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

- You have experience creating enterprise applications in Entra ID.
- You have an Entra ID account with an active subscription.
- You have one of the following roles in the Entra ID account: Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the service principal.

Step 1: Access Entra ID

Steps

1. Log in to the Azure Portal.
2. Navigate to Entra ID.
3. Select Enterprise applications.

Step 2: Create enterprise applications and save StorageGRID SSO configuration

To save the SSO configuration for Entra ID in StorageGRID, you must use Entra ID to create an enterprise

application for each Admin Node. You will copy the federation metadata URLs from Entra ID and paste them into the corresponding **Federation metadata URL** fields on the Configure SSO page.

Steps

1. Repeat the following steps for each Admin Node.
   a. In the Entra ID Enterprise applications pane, select **New application**.
   b. Select **Create your own application**.
   c. For the name, enter the **Enterprise application name** you copied from the Admin Node details table on the Configure SSO page.
   d. Leave the **Integrate any other application you don't find in the gallery (Non-gallery)** radio button selected.
   e. Select **Create**.
   f. Select the **Get started** link in the **2. Set up single sign on** box, or select the **Single sign-on** link in the left margin.
   g. Select the **SAML** box.
   h. Copy the **App Federation Metadata Url**, which you can find under **Step 3 SAML Signing Certificate**.
   i. Go to the Configure SSO page, and paste the URL in the **Federation metadata URL** field that corresponds to the **Enterprise application name** you used.
2. After you have pasted a federation metadata URL for each Admin Node and made all other needed changes to the SSO configuration, select **Save** on the Configure SSO page.

Step 3: Download SAML metadata for every Admin Node

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

Steps

1. Repeat these steps for each Admin Node.
   a. Sign in to StorageGRID from the Admin Node.
   b. Select **Configuration** > **Access control** > **Single sign-on**.
   c. Select the button to download the SAML metadata for that Admin Node.
   d. Save the file, which you will upload into Entra ID.

Step 4: Upload SAML metadata to each enterprise application

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

Steps

1. Return to the Azure Portal.
2. Repeat these steps for each enterprise application:

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

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

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

c. Go to the Single sign-on page.

d. Complete the SAML configuration.

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

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

3. Test each application.

Create service provider connections in PingFederate for SAML in StorageGRID

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

Before you begin

- You have configured single sign-on for StorageGRID and you selected **Ping Federate** as the SSO type.
- You have entered sandbox mode in Grid Manager.
- You have the **SP connection ID** for each Admin Node in your system. You can find these values in the Admin Nodes detail table on the Configure SSO page.
- You have downloaded the **SAML metadata** for each Admin Node in your system.
- You have experience creating SP connections in PingFederate Server.
- You have the Administrator's Reference Guide for PingFederate Server. The PingFederate documentation provides detailed step-by-step instructions and explanations.
- You have the Admin permission for PingFederate Server.

About this task

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

Complete prerequisites in PingFederate

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

Create data store

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

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

Create password credential validator

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

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

Create IdP adapter instance

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

Steps

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

Create or import signing certificate

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

Steps

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

Create an SP connection in PingFederate

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

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

Choose SP connection type

Steps

1. Go to **Applications** > **Integration** > **SP Connections**.
2. Select **Create Connection**.
3. Select **Do not use a template for this connection**.

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

Import SP metadata

Steps

1. On the Import Metadata tab, select **File**.
2. Choose the SAML metadata file you downloaded from the Configure SSO page for the Admin Node.
3. Review the Metadata Summary and the information provided on the General Info tab.

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

4. Select **Next**.

Configure IdP Browser SSO

Steps

1. From the Browser SSO tab, select **Configure Browser SSO**.
2. On the SAML profiles tab, select the **SP-initiated SSO**, **SP-initial SLO**, **IdP-initiated SSO**, and **IdP-initiated SLO** options.
3. Select **Next**.
4. On the Assertion Lifetime tab, make no changes.
5. On the Assertion Creation tab, select **Configure Assertion Creation**.
   a. On the Identity Mapping tab, select **Standard**.
   b. On the Attribute Contract tab, use the **SAML_SUBJECT** as the Attribute Contract and the unspecified name format that was imported.
6. For Extend the Contract, select **Delete** to remove the `urn:oid`, which is not used.

Map adapter instance

Steps

1. On the Authentication Source Mapping tab, select **Map New Adapter Instance**.
2. On the Adapter instance tab, select the adapter instance you created.
3. On the Mapping Method tab, select **Retrieve Additional Attributes From a Data Store**.
4. On the Attribute Source & User Lookup tab, select **Add Attribute Source**.
5. On the Data Store tab, provide a description and select the data store you added.
6. On the LDAP Directory Search tab:
   - Enter the **Base DN**, which should exactly match the value you entered in StorageGRID for the LDAP server.
   - For the Search Scope, select **Subtree**.
   - For the Root Object Class, search for and add either of these attributes: **objectGUID** or **userPrincipalName**.
7. On the LDAP Binary Attribute Encoding Types tab, select **Base64** for the **objectGUID** attribute.
8. On the LDAP Filter tab, enter **sAMAccountName=${username}**.

9. On the Attribute Contract Fulfillment tab, select **LDAP (attribute)** from the Source drop-down and select either **objectGUID** or **userPrincipalName** from the Value drop-down.
10. Review and then save the attribute source.
11. On the Failsave Attribute Source tab, select **Abort the SSO Transaction**.
12. Review the summary and select **Done**.
13. Select **Done**.

Configure protocol settings

Steps

1. On the **SP Connection** > **Browser SSO** > **Protocol Settings** tab, select **Configure Protocol Settings**.
2. On the Assertion Consumer Service URL tab, accept the default values, which were imported from the StorageGRID SAML metadata (**POST** for Binding and `/api/saml-response` for Endpoint URL).
3. On the SLO Service URLs tab, accept the default values, which were imported from the StorageGRID SAML metadata (**REDIRECT** for Binding and `/api/saml-logout` for Endpoint URL.
4. On the Allowable SAML Bindings tab, clear **ARTIFACT** and **SOAP**. Only **POST** and **REDIRECT** are required.
5. On the Signature Policy tab, leave the **Require Authn Requests to be Signed** and **Always Sign Assertion** checkboxes selected.
6. On the Encryption Policy tab, select **None**.
7. Review the summary and select **Done** to save the protocol settings.
8. Review the summary and select **Done** to save the Browser SSO settings.

Configure credentials

Steps

1. From the SP Connection tab, select **Credentials**.
2. From the Credentials tab, select **Configure Credentials**.
3. Select the signing certificate you created or imported.
4. Select **Next** to go to **Manage Signature Verification Settings**.
   a. On the Trust Model tab, select **Unanchored**.
   b. On the Signature Verification Certificate tab, review the signing certificate information, which was imported from the StorageGRID SAML metadata.
5. Review the summary screens and select **Save** to save the SP connection.

Create additional SP connections

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

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

Steps

1. Select **Action** > **Copy** to create a copy of the initial SP connection for each additional Admin Node.
2. Enter the Connection ID and Connection Name for the copy, and select **Save**.
3. Choose the metadata file corresponding to the Admin Node:
    a. Select **Action** > **Update with Metadata**.
    b. Select **Choose File** and upload the metadata.
    c. Select **Next**.
    d. Select **Save**.
4. Resolve the error due to the unused attribute:
    a. Select the new connection.
    b. Select **Configure Browser SSO > Configure Assertion Creation > Attribute Contract**.
    c. Delete the entry for **urn:oid**.
    d. Select **Save**.

Copyright information

Trademark information