Set up SSO with OIDC

StorageGRID software

NetApp
July 22, 2026

This PDF was generated from https://docs.netapp.com/us-en/storagegrid/admin/learn-about-setting-up-sso-oidc.html on July 22, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Set up SSO with OIDC

Learn about setting up SSO in StorageGRID using OIDC

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 OIDC or learn about setting up SSO using SAML.

1 **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, Keycloak, Okta, 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 OIDC 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 client for each Admin Node in Keycloak
- Learn about creating an Okta application for each Admin Node
- Learn about creating a service provider connection for each Admin Node in PingFederate

2 **Configure SSO**

Select the Configure SSO wizard for OIDC. Then, configure SSO with your identity provider and enter sandbox mode to configure and test SSO before enabling it for StorageGRID users.

Learn about configuring SSO using OIDC

3 **Enable SSO**

After confirming that you can use SSO to sign in to each Admin Node, enable SSO for all StorageGRID users.

Learn about enabling SSO for StorageGRID users

Create application groups in AD FS for OIDC in StorageGRID

You must use Active Directory Federation Services (AD FS) to create an application group for each Admin Node for OpenID Connect (OIDC) in your system.

Before you begin

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

> Each Admin Node in your StorageGRID system must have an application group. This ensures that users can securely sign in to and out of any Admin Node. You can create a single application group for all Admin Nodes (recommended) or a different application group for each Admin Node.

- You have experience creating application groups 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 Windows Server 2022 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.

Step 1: Create an application group

You can use Windows PowerShell to quickly create an application group.

Steps

1. From Windows Server Manager, select **Tools** > **AD FS Management**.
2. Select **Application Groups** > **Add Application Group**
3. For **Name**, enter the relying party identifier.
4. Under Template, select **Client-Server applications** > **Server application accessing a web API**.
5. Select **Next**.
6. Record the **Client Identifier** value.
7. Under **Redirect URI**, enter the FQDN (or IP address) `callback` and `logged-out` URIs for the Admin Node:
   - `https://<FQDN>/api/v4/oidc-callback` or `https://<IP_address>/api/v4/oidc-callback`
   - `https://<FQDN>/api/v4/oidc-logged-out` or `https://<IP_address>/api/v4/oidc-logged-out`

   Enter the URIs for each Admin Node if you are using one application group for all Admin Nodes. If you are using a different application group for each Admin Node, only enter the URIs for the corresponding Admin Node.
8. Select **Add**.
9. Select **Generate a shared secret**, record the value for **Secret**, then select **Next**.
10. Enter the client identifier for **Identifier**.
11. Select **Add**, then select **Next**.
12. Select **Permit everyone**.
13. Verify that the server application is selected under **Client application (caller)**.

14. Under **Permitted scopes**, verify that only the following options are selected:
    - allatclaims
    - email
    - openid
    - profile
15. Select **Next** > **Next**.
16. Select **Close**.

Step 2: Configure issuance transform rules

Configure the issuance transform rules for each application group.

Steps

1. In the **AD FS Management** page, right-select the application group, then select **Properties**.
2. Select the previously created web API, then select **Edit**.
3. Select **Issuance Transform Rules** > **Add Rule …**.
4. Under **Claim rule template:**, select **Send LDAP Attribute as Claims**.
5. Select **Next**.
6. Enter a Claim rule name.
7. Select **Active Directory** for Attribute store.
8. Add the LDAP attribute mappings to the outgoing claim types:
    - `E-Mail Addresses - E-Mail Address`
    - `Token-Groups - Unqualified Names - Group`
9. Select **Finish**.
10. Select **Apply** > **OK** > **OK**.

What's next

After creating application groups, configure SSO using OIDC.

Create enterprise applications in Entra ID for OIDC in StorageGRID

Use Entra ID to create an enterprise application for each Admin Node for OpenID Connect (OIDC) in your system.

Before you begin

- You have the relying party identifier and fully qualified domain name (FQDN) or IP address for each Admin Node in your system.

> Each Admin Node in your StorageGRID system must have an enterprise application. This ensures that users can securely sign in to and out of any Admin Node. You can create a single enterprise application for all Admin Nodes (recommended) or a different enterprise application for each Admin Node.

- You have experience creating 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. Select Microsoft Entra ID.
3. Select App registrations.

Step 2: Register a new application

Register a new enterprise application for each Admin Node in your system.

Steps

1. In the Entra ID Enterprise applications pane, select **Application registrations** > **New registration**.
2. For **Name**, enter the relying party identifier.
3. Under **Supported account types**, select the account types that can use the application or access the API, for example, **Single tenant only - <tenant_name>**.
4. Under **Redirect URI**, select **Select a platform** > **Web**.
5. Enter the FQDN (or IP address) redirect URI for the Admin Node: `https://<FQDN>/api/v4/oidc-callback` or `https://<IP_address>/api/v4/oidc-callback`

   Enter the URI for each Admin Node if you are using one enterprise application for all Admin Nodes. If you are using a different enterprise application for each Admin Node, only enter the URI for the corresponding Admin Node.

6. Select **Register**.
7. On the Overview page for the new application registration, record the **Application (client) ID** and **Directory (tenant) ID**.

Step 3: Configure a client secret

Register a client secret for each new application.

Steps

1. On the Overview page for the new application registration, select **Manage** > **Certificates and secrets** > **New client secret**.
2. Enter the client secret and set a desired expiry date.
3. Select **Add** to create the client secret.
4. Copy the secret **Value**.

   The secret value is not visible after you refresh or navigate from the client secret page.

Step 4: Set up the API permissions

Set up the API permissions for each new application.

Steps

1. On the Overview page for the new application registration, select **Manage** > **API permissions** > **Add a permission**.
2. Select **Microsoft APIs** > **Microsoft Graph** > **Delegated permissions**.
3. Expand **OpenId permissions**, then select **email**, **offline_access**, **openid**, and **profile**.
4. Select **Add permissions**.
5. Select **Grant admin consent for <tenant>**, then select **Yes**.

Step 5: Add the logged-out redirect URI

Add the logged-out redirect URI for each new application.

Steps

1. On the Overview page for the new application registration, select **Manage** > **Authentication**.
2. Select **Add Redirect URI** > **Web**.
3. Enter the FQDN (or IP address) redirect URI for the Admin Node: `https://<FQDN>/api/v4/oidc-logged-out` or `https://<IP_address>/api/v4/oidc-logged-out`

   Enter the URI for each Admin Node if you are using one application group for all Admin Nodes. If you are using a different application group for each Admin Node, only enter the URI for the corresponding Admin Node.

4. Select **Configure**.

What's next

After creating enterprise applications, configure SSO using OIDC.

Create clients in Keycloak for OIDC in StorageGRID

Use Keycloak to create a client connection for each Admin Node for OpenID Connect (OIDC) in your StorageGRID system.

Before you begin

- You have experience creating clients in Keycloak, or you have access to the Keycloak documentation.
- You have a dedicated account (Bind DN) for directory lookups and the login credentials.
- You have Keycloak Administrator access.

About this task

Each Admin Node in your StorageGRID system must have a client connection. This ensures that users can securely sign in to and out of any Admin Node. You can create a single client connection for all Admin Nodes (recommended) or a different client connection for each Admin Node.

Use the default settings unless otherwise specified. In some cases you can use settings required by your organization.

Step 1: Optionally, create a realm

Create a Keycloak realm to configure the LDAP provider and OIDC client, or use the Keycloak default realm.

Steps

1. Select **Create Realm**.
2. Enter a name for the realm.
3. Select **Enabled**.
4. Select **Create**.

Step 2: Configure LDAP provider

Configure the LDAP provider so that Keycloak connects to the Active Directory Federation Service (AD FS) LDAP server.

Steps

1. Select **User federation** > **Add Ldap providers**.
2. Under the Settings tab:
   a. Enter the following recommended values:
      - UI display name: Enter a unique value.
      - Vendor: **Active Directory**
      - Connection URL: `ldap://<ldap_IP_address>` or `ldaps://<ldap_IP_address>`
      - Connection pooling: **ON**
      - Bind DN: Enter your Bind DN
      - Bind credentials: Enter password
      - Edit mode: **READ_ONLY**
      - Users DN: For example, `CN=Users`, `DC=saml`, `DC=sgws`
      - Username LDAP attribute: **sAMAccountName**
      - RDN LDAP attribute: **cn**
      - UUID LDAP attribute: **objectGUID**
      - User object classes: `person`, `organizationalPerson`, `user`
      - User LDAP filter: `(sAMAccountName=*)`
      - Search scope: **Subtree**
      - Pagination: **ON**
      - Import users: **ON**
      - Sync registrations: **ON**
      - Remove invalid users during searches: **ON**
   b. Select **Test connection** and **Test authentication**.

      Resolve any issues that might occur before continuing.
3. Select **Save**.

Step 3: Configure LDAP mapping

Configure LDAP mapping to map AD as an attribute to Keycloak.

Steps

1. Go to **User federation** > **LDAP**
2. Select the LDAP provider you created.
3. On the Mappers tab, select **Add mapper** > **Create new mapper**.
4. For Mapper Type, select **user-attribute-ldap-mapper**.
5. Select **Save**, then enter the following information:
   - User Model Attribute: **userPrincipalName**
   - LDAP Attribute: **userPrincipalName**
   - Read Only: **ON**
   - Always Read Value From LDAP: **ON**
   - Is mandatory in LDAP: **OFF**
   - Force a Default value: **ON**
   - Is Binary Attribute: **OFF**
6. Select **Save**.

Step 4: Create OIDC client

Create the OIDC client for your system.

Steps

1. Go to **Clients** > **Create client**.
2. For General settings, enter the following information:
   - Name: Enter a display name for the client.
   - Client type: **OIDC Connect**
   - Client ID: Enter a unique value. Save this value for use later.
3. Select **Next**.
4. For Capability config, enter the following information:
   - Client authentication: **ON**
   - Standard flow: **Enable**
   - Direct access grants: **Enable**
   - Service account roles: **Enable**
5. Select **Next**.
6. For Login settings, enter the redirect URIs:

If one or more load balancer endpoints are configured for the management interface, add the redirect URIs for each port. For example:
`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-callback` and
`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-logged-out`

- Valid redirect URIs: `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-callback` and `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`
- Valid post logout redirect URIs: `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`
- Web origins: `https://<Admin_IP_address_or_FQDN>`

7. Select **Save**.

Step 5: Generate client secret

Generate a client secret for the OIDC client you created.

Steps

1. Go to **Clients**, then select the OIDC client you created.
2. On the Credentials tab, enter the following information:
   - Client authenticator: **Client Id and Secret**
   - Client secret: **Generate or set a client secret**. Save this value for use later.

Step 6: Define scopes

Define the scopes in Keycloak.

Steps

1. Go to **Client scopes** > **Create client scope**, then enter the following information:
   - Type: **None**
   - Protocol: **OpenID Connect**
   - Display on consent screen: **Enabled**
   - Include in OpenID Provider Metadata: **Enabled**
2. Select **Save**.
3. On the Mappers tab, select **Configure a new mapper** > **User Attribute**, then enter the following information:
   - Name: Enter a unique value.
   - User Attribute: **userPrincipalName**
   - Token Claim Name: **upn**
   - Claim JSON Type: **String**
   - Add to ID token: **ON**
   - Add to access token: **ON**
   - Add to userinfo: **ON**
   - Add to token introspection: **ON**
4. Select **Save**.
5. Go to **Clients** and select the OIDC client you created.
6. Select **Client Scopes** > **Add client scope**.
7. Select the client scope you created.

8. Select **Add**.

Step 7: Prepare to configure SSO using OIDC

Save the information required to configure SSO with OIDC using Keycloak in your StorageGRID system.

Steps

1. Check that you've saved the client ID and the client secret from the OIDC client you created.
2. Save the OpenID Connect discovery endpoint for the realm. This is available in the `well-known` configuration endpoint:

   ```
   https://<keycloak_host_ip/keycloak_host_name>/realms/<realm_name>/.well-known/openid-configuration
   ```

   Optionally include the network port:

   ```
   https://<keycloak_host_ip/keycloak_host_name>:<https_port>/realms/<realm_name>/.well-known/openid-configuration
   ```

What's next

After creating OIDC clients, configure SSO using OIDC.

Create Okta application for OIDC in StorageGRID

Create an Okta application for all Admin Nodes for OpenID Connect (OIDC) in your StorageGRID system.

Before you begin

- You have experience creating Okta applications, or you have access to the Okta documentation.
- You have Okta Administrator access.

About this task

An Okta application must contain sign-in and sign-out redirect URIs for all Admin Nodes. Redirect URIs ensure that users can securely sign in to and out of any Admin Node. You can create a single Okta application for all Admin Nodes (recommended) or a different application for each Admin Node.

Use the default settings unless otherwise specified. In some cases you can use settings required by your organization.

Step 1: Create an Okta application

Create an Okta application using the Okta UI.

Steps

1. In Okta, go to **Applications** > **Applications**.
2. Select **Create App Integration**, then enter the following information:
   - Sign-in method: **OIDC - OpenID Connect**
   - Application type: **Web Application**

3. Select **Next**.
4. Enter a name for the application in the App Integration field.
5. Verify that Authorization Code is selected (default) for Core grants.
6. Add the sign-in and sign-out redirect URIs for each Admin Node:
   - Sign-in redirect URI: `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-callback`
   - Sign-out redirect URI: `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`

   > If one or more load balancer endpoints are configured for the management interface, add the redirect URIs for each port. For example: `https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-callback` and `https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-logged-out`

7. Select **Save**. Save the client ID and client secret values for use later.

Step 2: Add a federate group

Create a group or use an existing group from the Active Directory Federation Service (AD FS) server for StorageGRID.

Steps

1. In GRID Manager, select **Configuration** > **Admin groups** > **Create group** > **Federate Group**.
2. Enter the AD FS server group name.
3. Select **Read-write** for access mode and **Root access** for permissions.
4. Select **Create group**.

Step 3: Import AD FS server groups and users

Install the Okta Active Directory client in the AD FS Server. Then, import the AD FS server groups and users.

Steps

1. In Okta, go to **Directory** > **Directory Integrations** > **Add Directory** > **Add Active Directory**.
2. Select **Set Up Active Directory** > **Download Agent**.
3. Immediately follow the setup process.

   > If you delay, the setup might stall and you will need to start over.

   a. Select the Active Directory domain.
   b. Create an OktaService account instead of linking an existing user.
   c. Select the organizational units that contain the users and the organizational units that contain the groups.
   d. Select the User Principal Name (UPN) that uses the AD UPN as the Okta username. For example: user@domain.com
4. Search for the **Okta AD Agent Management Utility** application. Then, run the application and confirm that the status message `The agent is running` appears.

The Okta AD client must be running whenever you want to execute an AD FS server sync and import with Okta.

5. In Okta, go to **Directory** > **Directory Integrations**.
6. Select the directory integration that you created.
7. Select **Import** > **Import Now**.
8. Select the user that you want to import, then select **Confirm Assignments**.
9. Go to **Directory** > **People** and confirm that the user was imported successfully.

   If the user status isn't Active, select **Activate** and keep refreshing the page until the user has the Active status.

10. Go to **Directory** > **Groups** and confirm that the group for the imported user was automatically imported.
11. Select the group and verify that the imported user is part of this group.

Step 4: Set up a claim

Set up a claim to include AD FS server groups in the access token. Then, verify that the claim includes the imported group for the imported user and Okta application.

Steps

1. In Okta, go to **Directory** > **Groups**.
2. Select the imported group for the imported user.
3. Select **Applications** > **Assign applications** > **Assign**.
4. Go to **Security** > **API**.
5. Select the **default** authorization server.
6. Select **Claims** > **Add Claim**. Then, create a claim with the following credentials:
   - Name: **groups**
   - Include in token type: **ID Token - Always**
   - Value type: **Expression**
   - Value: **Groups.startsWith("active_directory","",100)**
   - Include in: **Any scope**
7. Go to **Security** > **API**.
8. Select the **default** authorization server.
9. Select the **Token Preview** tab and enter the following credentials for Request Properties:
   - OAuth/OIDC client: **<application name>**
   - Grant type: **Authorization Code**
   - User: **Imported user (e-mail address)**
   - Scopes: **email, profile, openid**
10. Select **Execute**.

    The imported group appears in the Preview id_token tab in the Payload.

What's next

After creating an Okta application, configure SSO using OIDC.

Create service provider connections in PingFederate for OIDC in StorageGRID

Use PingFederate to create a service provider (SP) connection for each Admin Node for OpenID Connect (OIDC) in your system.

Before you begin

- 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 12.1.10 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.

Use the default settings unless otherwise specified. In some cases you can use settings required by your organization, such as settings for authentication method.

Step 1: Create data store

If you haven't already, create a data store to connect PingFederate to the AD FS LDAP server.

Steps

1. Go to **System** > **Data & Credentials Stores**.
2. Select **New Data Store**.
3. For Type, select **Directory (LDAP)**.
4. Select **Next**.
5. Under LDAP Configuration:
   - Enter the values for **Hostname**, **User DN** (username), and **Password**.

     Use the values you used when configuring identity federation in StorageGRID.
   - For Active Directory, select **LDAP Type**.

Step 2: Create password credential validator

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

Steps

1. Select **Password Credential Validators** > **Create New instance**.
2. On the Type tab, enter the following information:
   a. INSTANCE NAME and INSTANCE ID: You can use the same value for both.

b. Type: Select **LDAP Username Password Credential Validator**.

3. Select **Next**.
4. On the Instance Configuration tab, enter the following information:
   - LDAP DATASTORE: Select the data store you created.
   - SEARCH BASE: Enter the information for the LDAP configuration.
   - SEARCH FILTER: Enter **sAMAccountName=${username}**.
   - SCOPE OF SEARCH: Select **Subtree**.
5. Select **Next**.
6. On the Extended Contract tab, add the following attributes: `memberOf`, `objectGUID`, `sAMAccountName`, `sn`, and `userPrincipalName`
7. Select **Next** > **Save**.

Step 3: Create IdP adapter instance

If you haven't already, create an IdP (identity provider) adapter instance.

> Each Admin Node in your StorageGRID system must have an IdP connection. This ensures that users can securely sign in to and out of any Admin Node. You can create a single IdP connection for all Admin Nodes (recommended) or a different IdP connection for each Admin Node.

Steps

1. Go to **Authentication** > **Integration** > **IdP Adapters**.
2. Select **Create New Instance**.
3. On the Type tab, enter the following information:
   - INSTANCE NAME and INSTANCE ID: You can use the same value for both.
   - TYPE: Select **HTML Form IdP Adapter**.
4. Select **Next**.
5. On the **IdP Adapter** tab, select **Add a new row to 'Credential Validators'**.
6. Select the password credential validator you created.
7. Select **Next**.
8. On the Extended Contract tab, add the attributes that you mapped for the password credential validator.
9. Select **Next**.
10. On the Adapter Attributes tab, select the **username** attribute for Pseudonym.
11. Select **Next** > **Next**.
12. Review the summary and select **Save**.

Step 4: Configure OAuth Server and Authorization Server Settings

Configure the Authorization Server to support the grant types accepted by StorageGRID.

Steps

1. Go to **System** > **Authorization Server Settings**.
2. Verify that the following options are selected for REUSE EXISTING PERSISTENT ACCESS GRANTS FOR GRANT TYPES:
   - IMPLICIT
   - AUTHORIZATION CODE
   - RESOURCE OWNER PASSWORD CREDENTIALS

   > If your company restricts the use of RESOURCE OWNER PASSWORD CREDENTIALS, you can only use AUTHORIZATION CODE.

3. For OAuth Administrative Web Services Settings, select the password credential validator you created.

Step 5: Define scopes

Define the scopes in PingFederate.

Steps

1. Go to **System** > **OAuth Settings** > **Scope Management**.
2. On the Common Scopes tab, add the values for **openid**, **email**, and **profile**, if they don't already exist.

Step 6: Configure IdP Adapter Mapping

Configure IdP Adapter Mapping to map attributes from the IdP to persistent grants that are issued to clients, such as access tokens or refresh tokens.

Steps

1. Go to **Authentication** > **Policy Contract Grant Mapping**.
2. Select **IdP Adapter Grant Mapping**.
3. From the SOURCE ADAPTER INSTANCE drop-down, select the HTML Form Adapter you created.
4. Select **Add Mapping** > **Contract Fulfillment**.
5. Under Source, select **Adapter** for USER_KEY and USER_NAME.
6. Under Value, select **sAMAccountName** for USER_KEY and **username** for USER_NAME.
7. Select **Next** > **Next** to navigate to the summary page.
8. Select **Save**.

Step 7: Set up Resource Owner Credentials Mapping

Set up Resource Owner Credentials Mapping to ensure that user credentials are validated correctly during authentication.

Steps

1. Go to **Authentication** > **Policy Contract Grant Mapping**.
2. Select **Resource Owner Credentials Grant Mapping**.
3. From the SOURCE PASSWORD VALIDATOR INSTANCE drop-down, select the password credential validator you created.

4. Select **Add Mapping** > **Contract Fulfillment**.
5. Add the mapping for for USER_KEY:
    - Under Source, select **Password Credential Validator**.
    - Under Value, select **sAMAccountName**.
6. Select **Next** > **Next** to navigate to the summary page.
7. Select **Save**.

Step 8: 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. Select **Create New**, then enter the following information:
    - Common Name (CN): This should be the fully qualified domain name (FQDN) of the server.
    - Organization (Org): Enter the name of your organization.
    - Country: Provide the two-letter country code, for example, US for the United States.
    - Key Algorithm: Select the appropriate key algorithm, such as **RSA**.
    - Key Size: Set to **2048** bits.
    - Signature Algorithm: Select **RSA with SHA256** as the signature algorithm to ensure secure cryptographic operations.

Step 9: Configure Access Token Management

StorageGRID uses access tokens to authenticate and authorize API requests in PingFederate.

Steps

1. Navigate to **Applications** > **Access Token Management**.
2. Select **Create New Instance**.
3. On the Type tab, enter the following information:
    - INSTANCE NAME and INSTANCE ID: You can use the same value for both.
    - Type: Verify that the value is **JSON Web Tokens**.
4. Select **Next**.
5. On the Instance Configuration tab, enter the following information for Certificates:
    - KEY ID: Enter a unique identifier for the key.
    - Certificate: Add the certificate you created.
    - JWS ALGORITHM: Select **RSA using SHA256**.
    - ACTIVE SIGNING CERTIFICATE KEY ID: Select the **KEY ID** you created in this step.
6. Select **Next** > **Next**.
7. On the Access Token Attribute Contract tab, select **USER_KEY** for Subject Attribute Name and **username** for Extend the Contract.
8. Select **Add**.

9. Select **Next** > **Next** > **Next** to navigate to the summary page.
10. Select **Save**.

Step 10: Configure Access Token Mapping

Configure Access Token Mapping to use the access token you created.

Steps

1. Go to **Applications** > **Access Token Mappings**.
2. Select **Access Token Mappings**.
3. Select **Add Mapping**.
4. For Context, select **Default**.
5. For Access Token Manager, select the access token you created.
6. Select **Next** > **Contract Fulfillment**:
7. Under Source, select **Persistent Grant** for username.
8. Under Value, select **USER_KEY** for username.
9. Select **Next** > **Save**.

Step 11: Set Up the OpenID Connect Policy

Define the OpenID Connect policies for client access to the attributes that are mapped according to the OpenID specifications.

Steps

1. Go to **Applications** > **OAuth Clients**.
2. Select **OpenId Connect Policy Management** > **Add Policy**.
3. On the Manage Policy tab, enter the following information:
   - POLICY ID: A unique identifier for the policy.
   - POLICY NAME: A descriptive name for the policy.
   - ACCESS TOKEN MANAGER: Select the access token that you created.
   - ID TOKEN LIFETIME: Set the desired lifetime for the ID token, for example, 60 minutes or one hour.
   - INCLUDE USER INFO IN ID TOKEN: Select the box to include user details in the ID token.
4. Select **Next**.
5. On the Attribute Contract tab, remove any existing attributes that aren't required for the data store you created. Retain only the attributes that you want to pass from Ping Authentication to StorageGRID.

   This is a critical step. It determines which attribute values are included in the ID token. StorageGRID inherits these values during the authentication process.

6. Select **Next** > **Next**.
7. On the Attribute Source & User Lookup tab, select **Add Attribute Source**. Then enter the following information:
   - ATTRIBUTE SOURCE ID and ATTRIBUTE SOURCE DESCRIPTION: You can use the same value for both.

- ACTIVE DATA STORE: Select the data store you created.

8. Select **Next**.
9. On the LDAP Directory Search tab:
   a. Enter the **Base DN**, which should exactly match the value you entered in StorageGRID for the LDAP server.
   b. From the ROOT OBJECT CLASS dropdown, select **objectClass**.
   c. From the ATTRIBUTE drop-down, add an attribute for each object class that you want to map. For example:
      - InetOrgPerson: Add displayName, givenName, or HomePhone.
      - user: Add LocalID or userPrincipalName (upn).
      - top: Add memberOf or name.
      - person: Add sn.
10. Select **Next**.
11. On the LDAP Filter tab, enter **sAMAccountName=${username}**.

    You need to customize the LDAP filter to ensure StorageGRID retrieves the user attributes based on your organization's specific Active Directory or LDAP structure. Consult with your LDAP/AD administrator to obtain the appropriate filter expression for your setup.

12. Select **Save** and review the summary.
13. On the Contract Fulfillment tab, enter the following information:
    - Source: Select the LDAP data store you created.
    - Value: Map each Attribute Contract to the respective value.
14. Select **Next** > **Next**.
15. Review the summary and select **Save**.
16. Go to **Applications** > **OAuth Clients** > **OpenID Connect Policy Management**.
17. Verify that the policy you created is set as the default policy.

Step 12: Create OAuth Client for OAuth Server

Create a new OAuth client to configure the necessary client credentials and authorize connections between PingFederate and StorageGRID.

Steps

1. Go to **Applications** > **OAuth Clients**.
2. Select **Add Client**, then enter the following information:
   - CLIENT ID: Enter a unique value.
   - CLIENT AUTHENTICATION: Select **Client Secret**.
   - CLIENT SECRET: Select **CHANGE SECRET** > **Generate Secret**.

     This generates the secret key for the client. Save this key for use later.

   - REDIRECT URIS: Provide the StorageGRID return URLs in the **Redirect URI** section. These URLs should match the URLs configured in StorageGRID for OAuth: For example:

- `https://<Admin IP or Hostname>/api/v4/oidc-callback`
- `https://<Admin IP or Hostname>/api/v4/oidc-logged-out`
- ALLOWED GRANT TYPES: Select the following options:
  - **Authorization Code**: This initiates the OAuth flow.
  - **Refresh Token**: Obtain a new token when an access token expires.
  - **Resource Owner Password Credentials**: If you need direct access to user credentials for authentication.
- OPENID CONNECT: Select **RSA using SHA-256** for ID Token Signing Algorithm.
- Logout Mode: Select **OIDC Back-Channel**.
- Front-Channel Logout URI, Back-Channel Logout URI, and Post-Logout Redirect URI: Add the StorageGRID logout URI: `https://<Admin IP or Hostname>/api/v4/oidc-logged-out`

3. Select **Save**.

What's next

After creating SP connections, configure SSO using OIDC.

Configure SSO in StorageGRID using OIDC

Follow the Configure SSO wizard for OpenID Connect (OIDC) 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 the OIDC client in the SSO identity provider for your StorageGRID system.
- You have configured identity federation for your StorageGRID system.

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 to configure SSO settings:
   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 **OIDC**.
3. Select the **SSO type** from the drop-down list.

4. 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:

     a. Browse to the location of the CA certificate.
     b. Upload the CA certificate file.
   - **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.

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

Step 2: Enter client information

Complete the fields in the Enter client information step of the wizard.

Steps

1. Specify the **Relying party identifier** for StorageGRID. This value controls the name you use for each OIDC configuration.
   - 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 OIDC configuration for each Admin Node in the grid, based on the node's hostname.

   > You must configure OIDC for the Admin Nodes in your StorageGRID system. This ensures that users can securely sign in to and out of any Admin Node. You can use the same OIDC configuration for all Admin Nodes (recommended) or set up a different OIDC configuration for each Admin Node.

2. Enter the **Client ID**, **Client secret**, and **OpenID endpoint URL** for each relying party identifier.
3. Select **Save and enter sandbox mode**.

Step 3: Test configuration

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

Sandbox mode makes it easy to perform the back-and-forth configuration and to test all of your settings before you enable SSO. StorageGRID can remain in sandbox mode as long as required. However, only federated users and local users can sign in.

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 new tab, to access your identity provider's sign-on page.
3. Enter your federated username and password.
   - If the SSO sign-in and logout operations are successful, a green banner appears.
   - If the SSO operation is unsuccessful, an error message appears. Fix the issue, clear the browser's cookies, and try again.
4. Follow the steps in the wizard to access the Test configuration page for each Admin Node in your grid.
5. Repeat Steps 2 and 3 to verify the SSO connection for each Admin Node.

Step 4: 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. StorageGRID doesn't provide an example authentication script for all supported SSO providers.

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**.

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.

Copyright information

Copyright © 2026 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.