Qumulo Nexus Configuration Guide

Table of Contents

Enabling Single Sign-On (SSO)

Enabling Single Sign-On (SSO)

Configuration Workflow for Storage Administrators who Manage a Qumulo Nexus Account

This configuration workflow explains how to enable single sign-on (SSO) for Qumulo Nexus from the perspective of a storage administrator who manages a Qumulo Nexus account and works together with a system administrator who manages your organization's identity provider (IdP).

> ⚠ Important
> Nexus IdP functionality is currently in private preview.

After the storage administrator performs the initial configuration in Nexus, the system administrator configures the IdP. Then, the storage administrator completes the SSO configuration in Nexus.

Prerequisites

- Administrative access to your organization’s Nexus account
- A subdomain for your organization

Step 1: Perform Initial Single Sign-On (SSO) Configuration in Qumulo Nexus

Before you ask a system administrator to configure the identity provider (IdP), you must perform the initial SSO configuration in Qumulo Nexus.

To Perform Initial SSO Configuration in Nexus

1. Log in to Qumulo Nexus.
2. In the upper-right corner, click your username and then click **Organization Settings**.
3. On your organization’s page, click **SAML SSO**, and then click **Configure SSO**.
4. On the **Configure SAML SSO page**, enter a **Nexus login subdomain** and then click **Save & Continue**.

   The Entity ID (your Nexus account’s unique identifier) and ACS URL (the Assertion Consumer Service URL that receives SAML responses) are displayed. For example:

   ```
   https://mysubdomain.nexus.qumulo.com
   https://mysubdomain.nexus.qumulo.com/api/v1/auth/saml/acs/
   ```

> **Note**
>
> - Record these values for the next step.
> - If the subdomain that you want to use is unavailable, choose another subdomain or contact the Qumulo Care team.

Step 2: Ask a System Administrator to Configure an Identity Provider (IdP) for Qumulo Nexus

After you perform the initial SSO configuration in Nexus, you must ask a system administrator in your organization to configure the IdP and then provide you with the IdP Metadata URL.

1. Provide your system administrator with the Entity ID (your Nexus account's unique identifier) and ACS URL (the Assertion Consumer Service URL that receives SAML responses).
2. Ask the system administrator to perform the necessary configuration (page 6).
3. Receive the IdP Metadata URL from your system administrator. For example:

   ```
   https://my-organization.idp-provider.com/app/abcd12e345fgHIJKLm678/sso/saml/metadata
   ```

> **Note**
> The format of the IdP Metadata URL depends on your organization's IdP provider.

Step 3: Perform Final Single Sign-On (SSO) Configuration in Qumulo Nexus

After your system administrator configures the identity provider (IdP), you must perform the final SSO configuration in Qumulo Nexus by using the IdP Metadata URL .

1. Log in to Qumulo Nexus.
2. In the upper-right corner, click your username and then click **Organization Settings**.
3. On your organization's page, click **SAML SSO**, and then click **Configure SSO**.
4. On the **Configure SAML SSO**, enter the the **IdP Metadata URL** and then click **Complete Configuration**.

   SAML SSO - Enabled is displayed.

Next Steps

After you perform the final SSO configuration, you can click **Users** and then add users to your Nexus account. Every user that you add has SSO enabled by default.

Configuration Workflow for System Administrators who Manage a Qumulo Nexus Account and an Identity Provider (IdP)

This configuration workflow explains how to enable single sign-on (SSO) for Qumulo Nexus from the perspective of a system administrator who manages both a Qumulo Nexus account and an Identity Provider (IdP).

> ⚠ Important
> Nexus IdP functionality is currently in private preview.

After the system administrator performs the initial configuration in Nexus, she must configure the IdP. Then, she can complete the SSO configuration in Nexus.

Prerequisites

- Administrative access to your organization's Nexus account
- A subdomain for your organization

Step 1: Perform Initial Single Sign-On (SSO) Configuration in Qumulo Nexus

Before you can configure the identity provider (IdP), you must perform the initial SSO configuration in Qumulo Nexus.

To Perform Initial SSO Configuration in Nexus

1. Log in to Qumulo Nexus.
2. In the upper-right corner, click your username and then click **Organization Settings**.
3. On your organization's page, click **SAML SSO**, and then click **Configure SSO**.
4. On the **Configure SAML SSO page**, enter a **Nexus login subdomain** and then click **Save & Continue**.

   The Entity ID (your Nexus account's unique identifier) and ACS URL (the Assertion Consumer Service URL that receives SAML responses) are displayed. For example:

   ```
   https://mysubdomain.nexus.qumulo.com
   https://mysubdomain.nexus.qumulo.com/api/v1/auth/saml/acs/
   ```

> **Note**
>
> - Record these values and provide them to the system administrator who manages your organization's IdP.
> - If the subdomain that you want to use is unavailable, choose another subdomain or contact the Qumulo Care team.

Step 2: Configure an Identity Provider (IdP) for Qumulo Nexus

After you perform the initial SSO configuration in Nexus, you must configure your IdP.

> **Tip**
> If you work together with a storage administrator who manages your organization's Nexus account, she provides you with the Entity ID and ACS URL.

To Configure Your IdP for Nexus

1. Log in to your IdP's console.
2. In the application or service configuration section, take the following steps:
    a. Add Qumulo Nexus as a service provider by using the Entity ID and ACS URL from your Nexus account.

    > **Note**
    > If your IdP is joined to Active Directory (AD), configure the IdP to send the User Principal Name (UPN) as the primary name identifier. This lets the Qumulo cluster use the information provided by the IdP to identify an authenticated user and any remote management actions that she performs on the cluster.

    b. Map the IdP attributes for user email, first name, and last name to the `email`, `firstName`, and `lastName` Nexus attributes.

For more information specific to your SAML IdP, see the following documentation:

- **Auth0:** Customize SAML Assertions in the Authenticate documentation
- **Azure Active Directory:** Customize SAML token claims in the Microsoft Entra documentation

- **Google Workspace:** Set up your own custom SAML app in the Google Workspace Admin Help documentation
- **Okta:** Define attribute statements in the Okta Identity Engine documentation
- **Ping Identity:** Editing an application - SAML in the PingOne documentation

> **Tip**
> If you work together with a storage administrator who manages your organization's Nexus account, provide her with the IdP Metadata URL.

Step 3: Perform Final Single Sign-On (SSO) Configuration in Qumulo Nexus

After you configure the identity provider (IdP), you must perform the final SSO configuration in Qumulo Nexus by using the IdP Metadata URL provided by your system administrator.

1. Log in to Qumulo Nexus.
2. In the upper-right corner, click your username and then click **Organization Settings**.
3. On your organization's page, click **SAML SSO**, and then click **Configure SSO**.
4. On the **Configure SAML SSO**, enter the the **IdP Metadata URL** provided by your system administrator and then click **Complete Configuration**.

   SAML SSO - Enabled is displayed.

Next Steps

After you perform the final SSO configuration, you can click **Users** and then add users to your Nexus account. Every user that you add has SSO enabled by default.