COHESITY

Version 2.3

March 2024

Integrate AD FS with Cohesity SSO

Enable Seamless Authentication and Security for Organizations

ABSTRACT

Your organization is dynamic; strengthening agility and flexibility without compromising on security is a balancing act. Single Sign-On (SSO) solutions help solve authentication and identity challenges while providing additional benefits. Cohesity provides seamless SSO support for entire clusters as well as organizations in multi-tenant clusters.

Table of Contents

Figures

Single Sign-On (SSO) Benefits

When you streamline your organization's infrastructure with SSO capabilities, the complex tasks of managing all its components become more efficient for administrators across systems. You also gain many other benefits in the process, including:

- Increased compliance and security
- Easier collaboration between vendors and partners
- Productivity gains
- Improved user auditing
- Improved application adoption
- Better user experience for employees
- Fewer support cases

Role-based access control (RBAC) restricts system access based on a user's role within an organization and has become one of the main methods for advanced access control. The roles in RBAC refer to the levels of access that users have to a Cohesity cluster.

Cohesity's SSO integration supports three RBAC methods: Default, Individual User-based, and User Groups-based.

Default RBAC

The default role associated with the SSO configuration is applied to all users who log in using the given identity provider (IdP).

To use default RBAC, you need to pass the "Email" or the "Login" SAML attribute to Cohesity .

Individual User-based RBAC

In our integration, you can also assign custom roles to individual users. For example, all users have Viewer roles by default, and you can create SSO users on Cohesity so that individual users have admin roles as required.

As with default RBAC, to use user-based RBAC, you need to pass the "Email" or the "Login" SAML attribute to Cohesity .

NOTE: If a custom role is provided, the default role is not used. For example, if the default role is Admin and a user is assigned the Viewer role, that user won't be able to perform admin-only operations.

User Groups-based RBAC

User groups-based RBAC is the most common use case as you can assign the same role to all users in the group in a single action.

For example, all users might have the Viewer role by default. You can then create an SSO group on Cohesity called “cohesity_admins” and give that group the Admin role. Now, every user in the “cohesity_admin” group also has the Admin role.

To use groups-based RBAC, you need to pass the “Email” or “Login” SAML attribute *and* pass the “Groups” SAML attribute to Cohesity .

NOTE: If a user is assigned a custom role, and also gets a role from the group, that user has both roles. For example, if a user in the “cohesity_admin” group is also assigned the Data Security role, the user gets both the Admin and the Data Security roles.

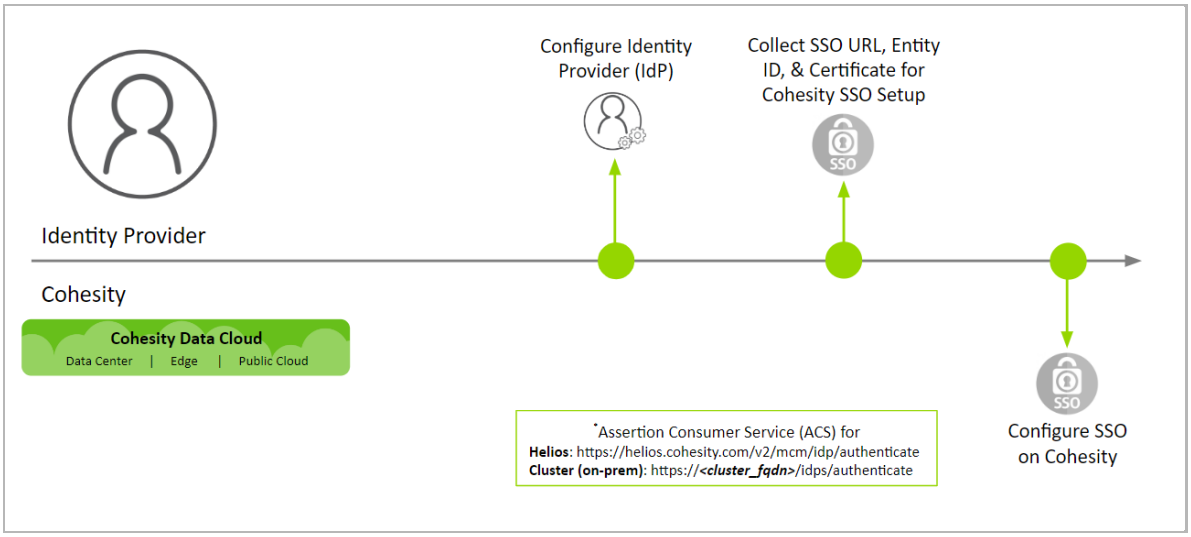
Cohesity Offers Seamless SSO Support

You can configure Cohesity to use an IdP for SSO access to both your dedicated Cohesity clusters as well as multi-tenant Cohesity clusters. On multi-tenant Cohesity clusters, you can configure SSO for each organization that is defined in Cohesity.

Integrate Cohesity with IdP

To integrate with an IdP, you need to configure details on both the IdP platform as well as the service provider (SP)—in this case, Cohesity.

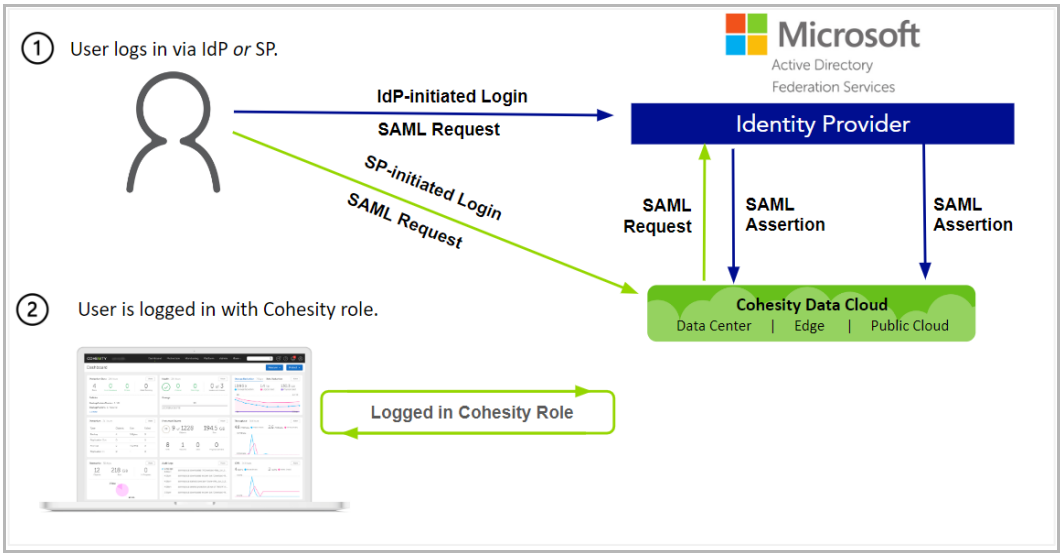
Figure 1: Integrate Cohesity with Identity Provider



The authentication workflow can start with either the IdP *or* the SP:

1. User logs in via either:
   a) **IdP**: The identity provider, AD FS, identifies and authenticates the user and sends a SAML 2.0 assertion to the service provider, Cohesity .
   b) **SP**: A user requests to log in to the service provider, Cohesity , via SSO. The SAML 2.0 request is redirected to the identity provider, AD FS. AD FS identifies and authenticates the user, then sends a SAML 2.0 assertion to Cohesity .
2. Cohesity authorizes this user with the SAML 2.0 assertion and maps the user to the appropriate role.

Figure 2: IdP authenticates Cohesity User and Assigns Cohesity Role



Map SAML Attributes for SSO setup

When an IdP sends the SAML response to Cohesity , Cohesity looks for a few SAML attributes to identify the user who is logging in and assign the correct roles.

Those attributes include the “Email” or the “Login” attribute, and the “Groups” attribute if you are using groups-based RBAC.

Pass “Email” or “Login” SAML Attribute to Cohesity

Cohesity expects *either* the “Email” or the “Login” SAML attribute in the SAML response. If both attributes are sent, the value of the “Login” attribute is read and used for role assignment and the “Email” attribute is ignored. If only the “Email” attribute is provided, then that is used for role assignment. If neither of these two attributes is provided, SSO will *not* work.

NOTE: The SAML attributes that Cohesity requires are not case-sensitive.

If Cohesity finds one of the two attributes, it lets the user into the Cohesity cluster home page and the default user role is assigned to that user unless you create an SSO user on Cohesity with a custom role.

Pass “Groups” SAML Attribute to Cohesity

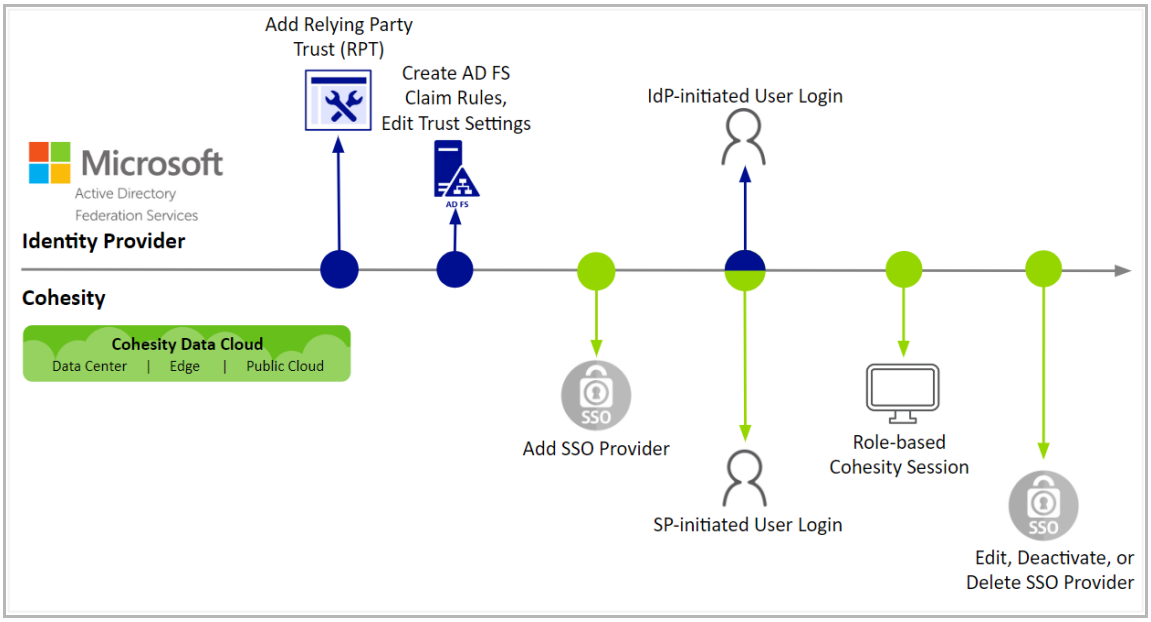
In general, it is a best practice to deploy SSO with user groups-based RBAC and assign custom roles to different user groups. To do so, you need to pass the “Groups” SAML attribute to Cohesity. The value of the “Groups” attribute is a list of groups that the user belongs to, and can include more than one group.

When Cohesity finds the “Groups” SAML attribute in the SAML response, it looks for any SSO groups that have been created on Cohesity . If the groups are found, the user is assigned the same role as the role assigned to the whole group. If no such SSO groups are present, the default role is assigned to the user. The default role is not mandatory but If the default role is not configured and there are no SSO groups created, the user cannot log in.

Configure Access Management with AD FS

To configure and use AD FS on Cohesity you need to configure certain parameters on the IdP and then use information from the IdP to configure SSO on Cohesity.

Figure 3: Cohesity Access Management with AD FS SSO Lifecycle



Configure IdP

The first step to configure SSO on Cohesity s is to supply some information to the IdP, AD FS in this case. With these details, AD FS can send the SAML response with the information about the authenticated user. The only piece of information you need from Cohesity is the SSO authenticate URL.

For SSO on:

- **Cohesity (on-prem)**, `use: https://<cluster_fqdn>/idps/authenticate`.
- **Helios**, use: `https://helios.cohesity.com/v2/mcm/idp/authenticate`.

Use this URL as the Relying Party Trust when you create the AD FS application below.

To configure the IdP:

1. Review the requirements.
2. Add a Relying Party Trust (RPT).
3. Create the AD FS claim rules and edit the trust settings.
4. Collect the SSO URL, Entity ID, and certificate from AD FS.

Review Requirements

To use AD FS to log in to Cohesity , you need:

- An Active Directory instance where all users have an email address attribute.
- A server running Microsoft Server 2016, 2012, or 2008. (This guide uses screenshots from Server 2016, but the steps are similar on other versions.)
- An SSL certificate to sign your AD FS login page and the Signing Certificate for that certificate.
- An installed certificate for hosted SSL.

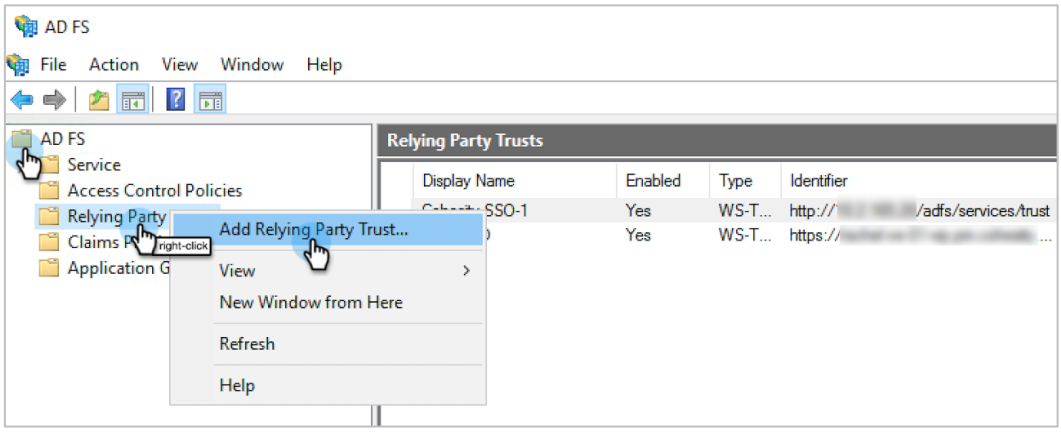
After you meet these requirements, you need to install AD FS on your server. To install and configure AD FS, see Deploy and configure AD FS from Microsoft.

Add a Relying Party Trust (RPT)

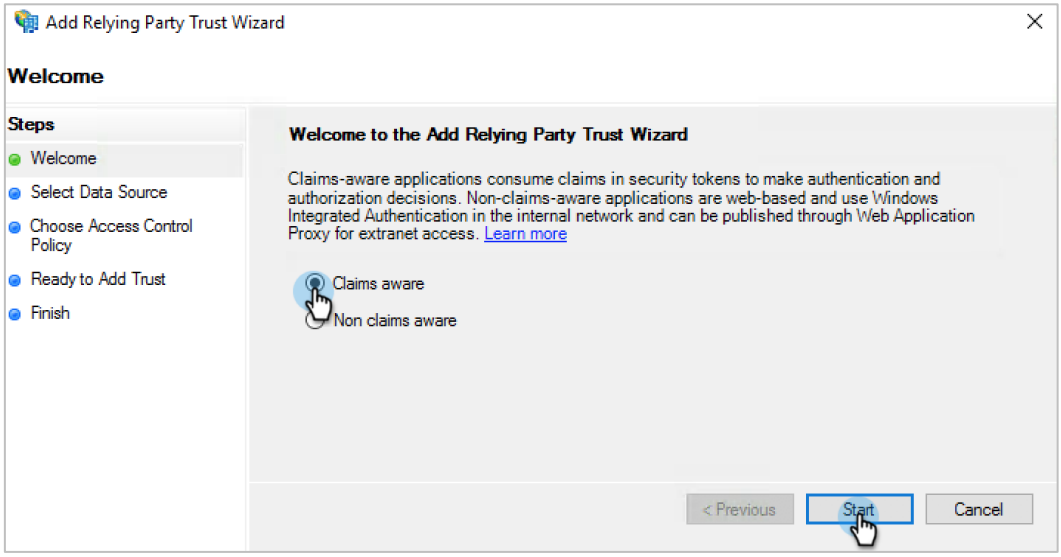
Once you have deployed AD FS, you need to add a Relying Party Trust (RPT) to enter the Cohesity SSO authenticate URL via the SAML 2.0 WebSSO protocol.

To add an RPT:

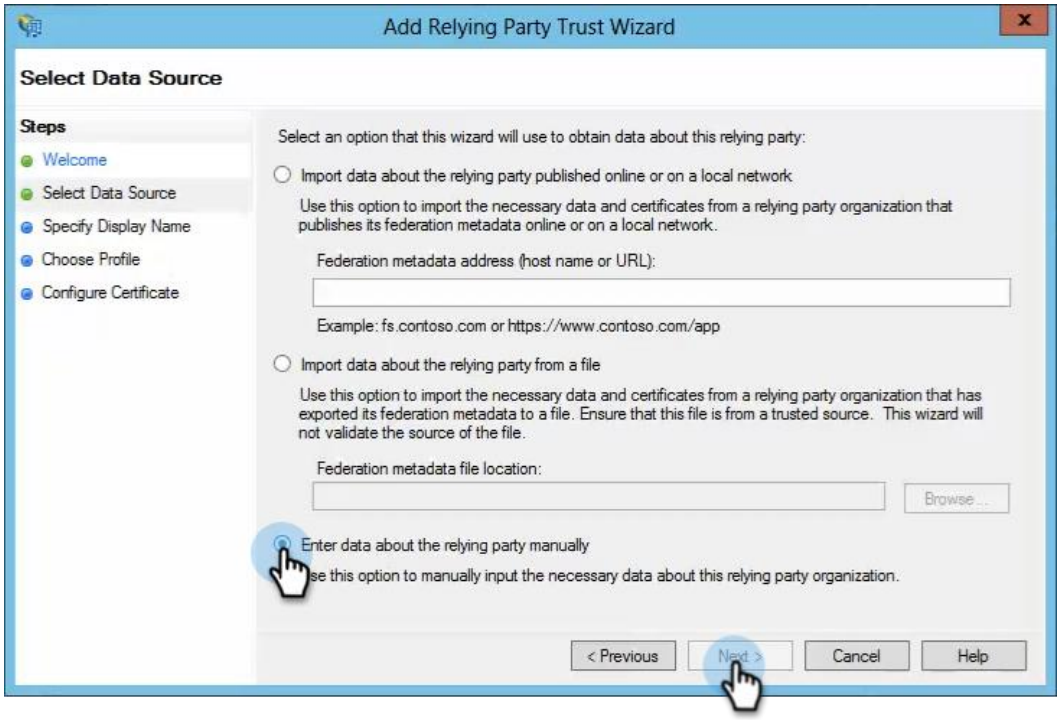
1. In the **AD FS** folder, right-click **Relying Party Trusts** and select **Add Relying Party Trust**. The **Add Relying Trust Party Wizard** opens.



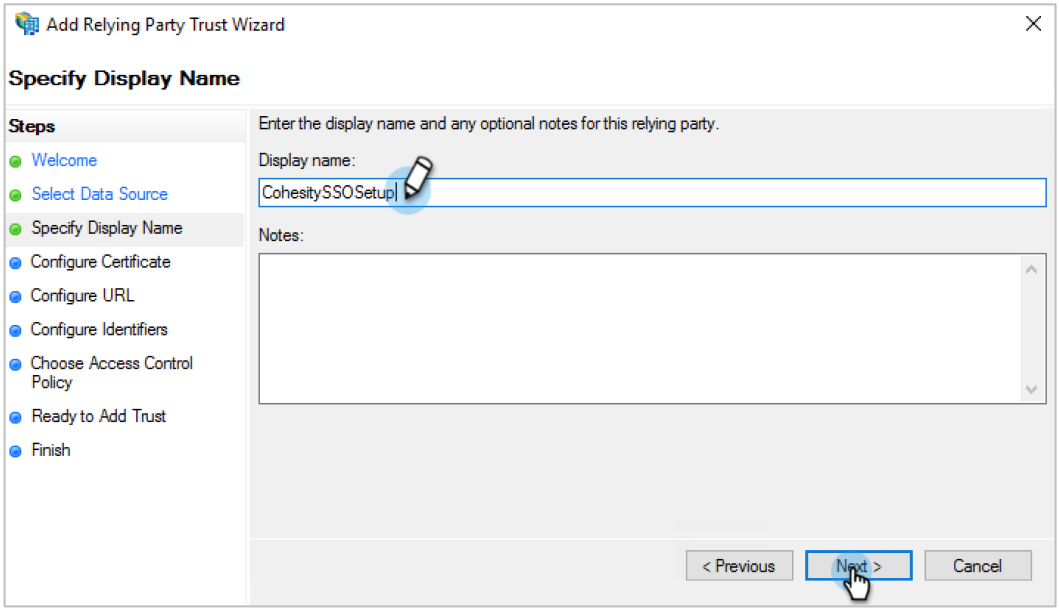
2. In the wizard's **Welcome** page, choose **Claims aware** and click **Start**.



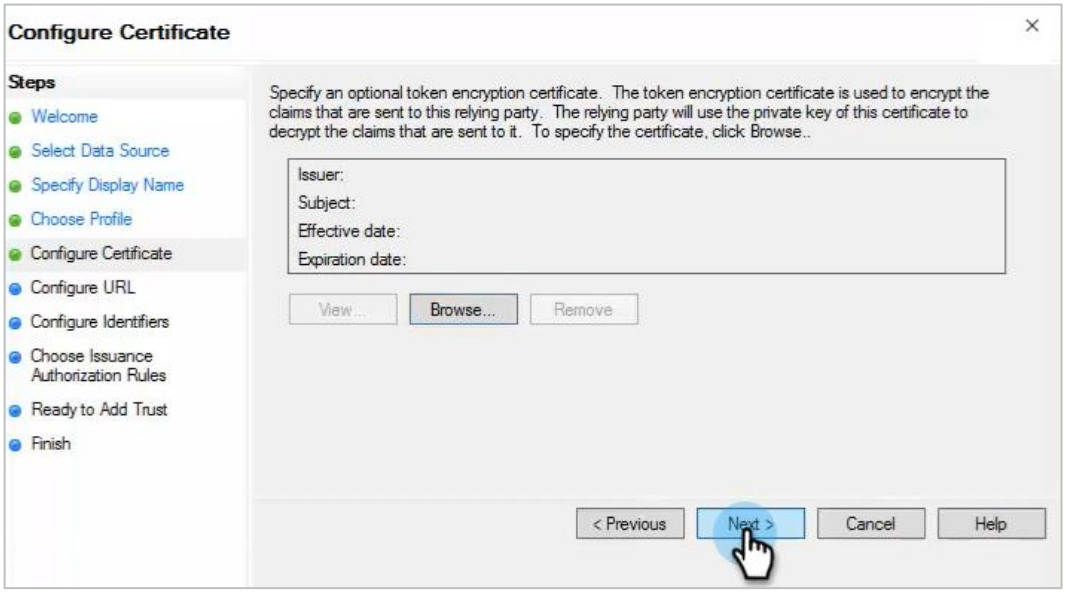
3. Under **Select Data Source**, select **Enter data about the relying party manually** and click **Next**.



4. Under **Specify Display Name**, enter a **Display name** and click **Next**.

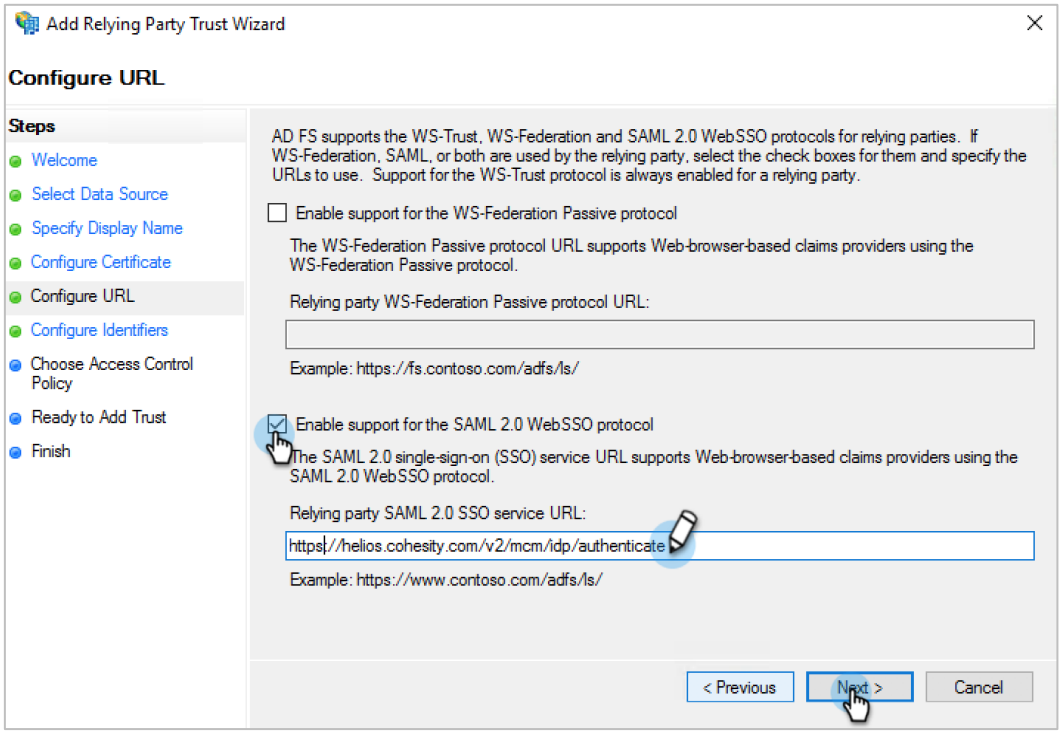


5. Under **Configure Certificate**, leave the certificate settings at their defaults and click **Next**.

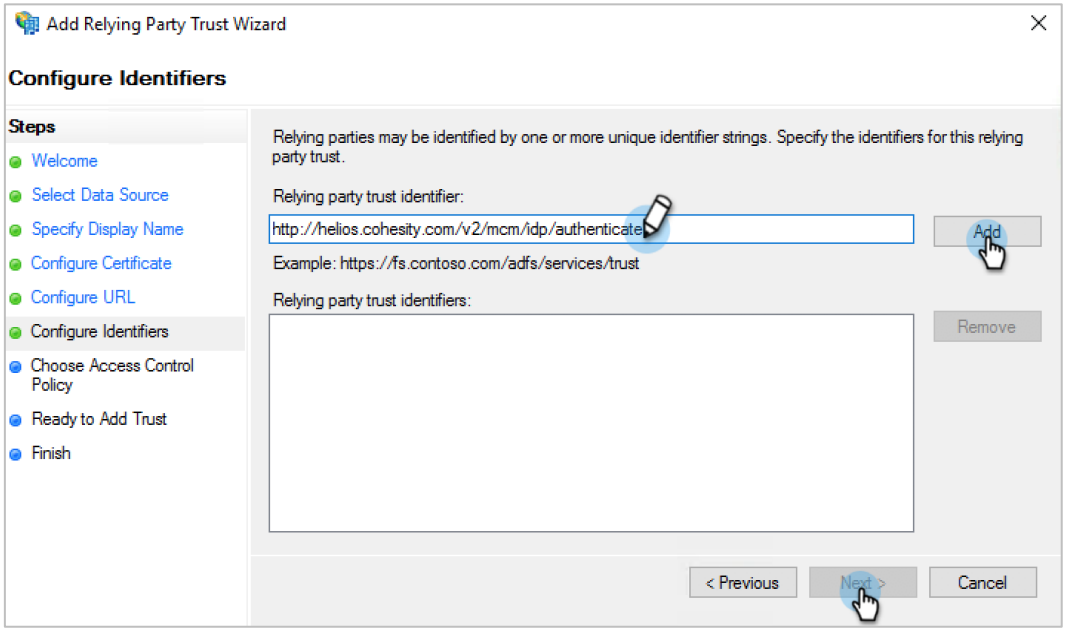


NOTE: If you wish to choose a specific certificate, click **Browse** to select the certificate file. However, if you do, you will have to provide your public key later.

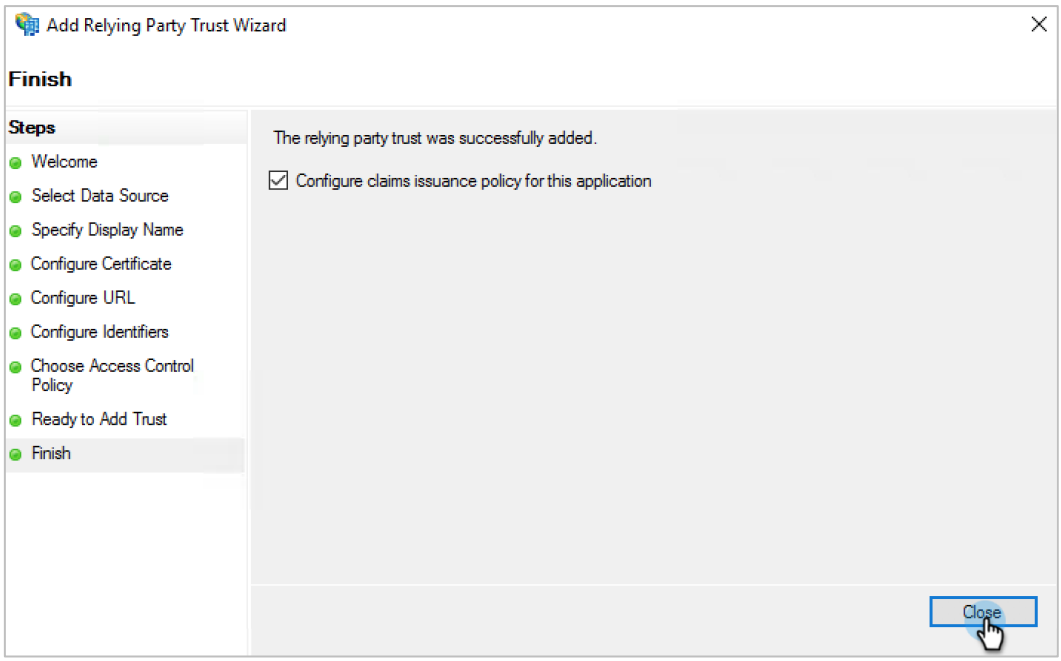
6. Under **Configure URL**, check **Enable Support for the SAML 2.0 WebSSO protocol** and enter the Cohesity SSO authenticate URL. For:
   - **Cohesity (on-prem)**, use: `https://<cluster_fqdn>/idps/authenticate`.
   - **Helios**, use: `https://helios.cohesity.com/v2/mcm/idp/authenticate`.



7. Under **Configure Identifiers**, add **Relying party trust Identifier** using the same Cohesity SSO authenticate URL that you used in the previous step and click **Add**.



8. In the next screen, you can optionally configure multi-factor authentication (MFA). For instructions, see Configure Additional Authentication Methods for AD FS from Microsoft.
9. In the next two screens, the wizard will display an overview of your settings. In the final screen, click **Close** to exit the wizard and open the Claim Rules editor.

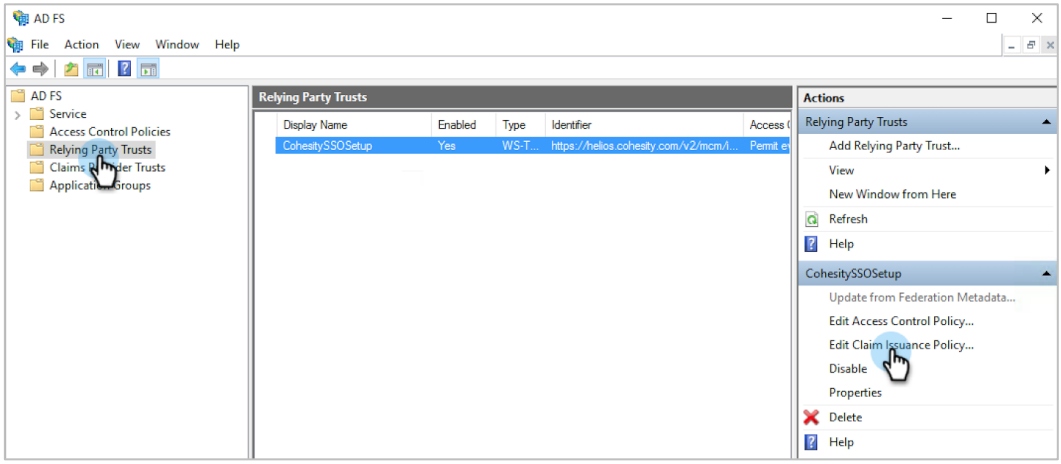


Create Claim Rules

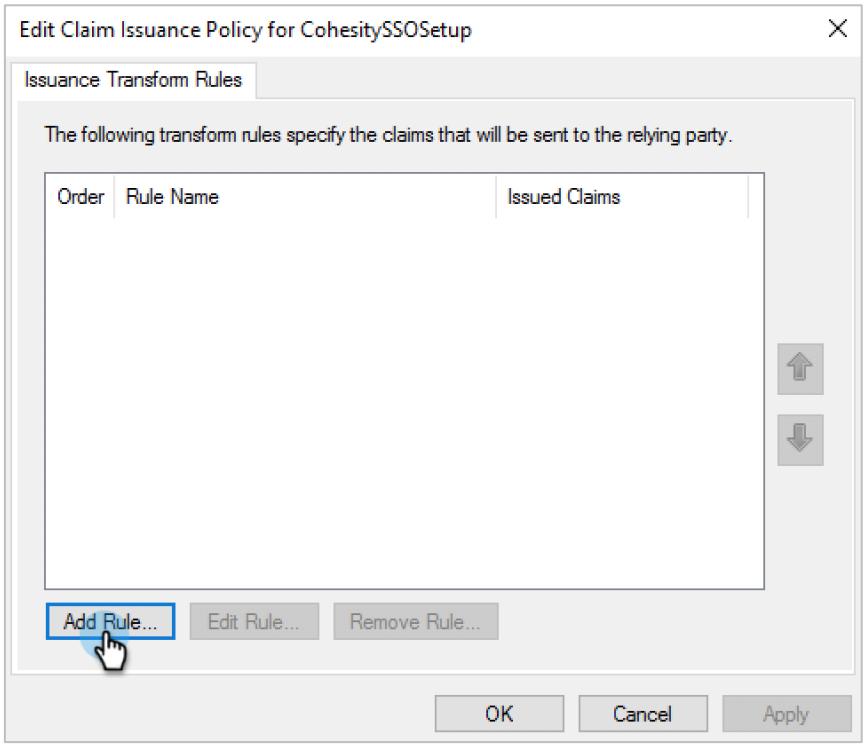
Once you have created the RPT, you need to pass two SAML attributes: "Email" or "Login" and "Groups". Cohesity looks for these attributes to identify users and assign roles.

To pass the SAML attributes:

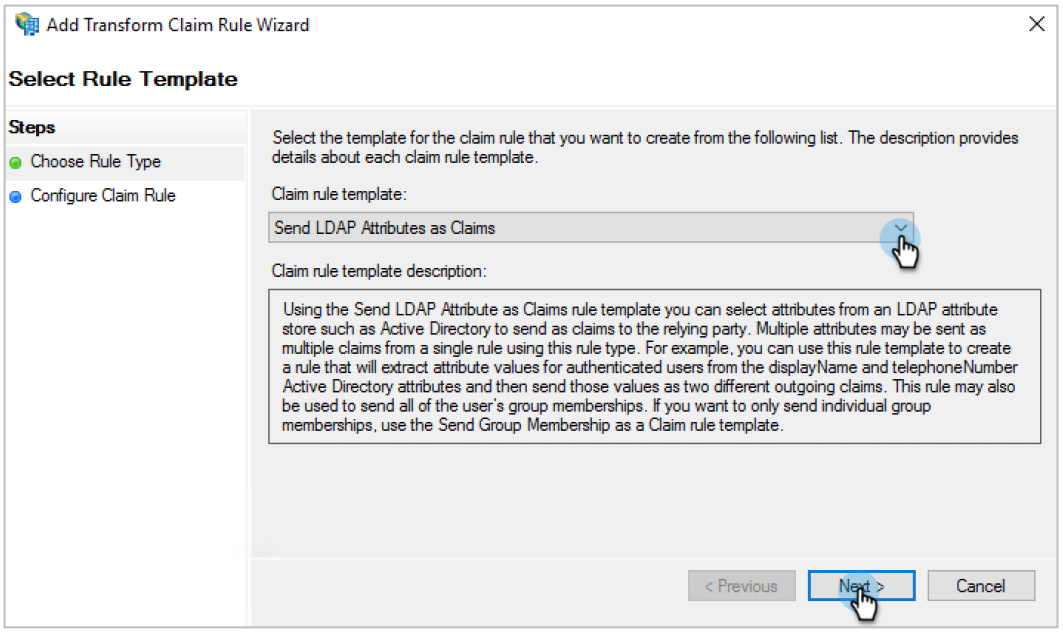
1. In the **AD FS** folder, navigate to **Relying Party Trusts** and select the RPT that you added above and click **Edit Claim Issuance Policy** on the right.



2. Click **Add Rule**.



3. Under **Select Rule Template**, select **Send LDAP Attributes as Claims** and click **Next**.

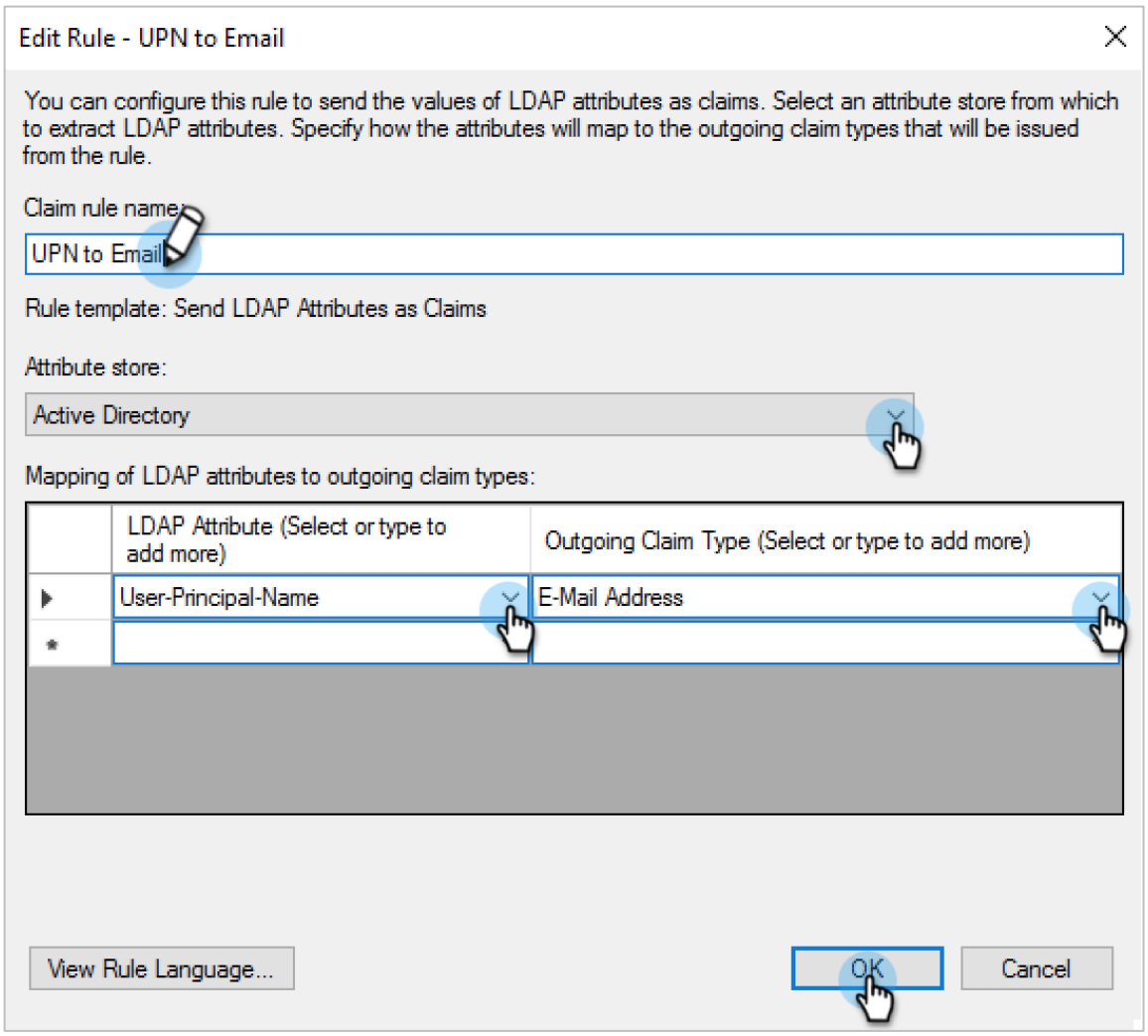


4. Under **Edit Rule** enter a **Claim rule name**, choose **Active Directory** as your **Attribute store**, and edit the mapping table:

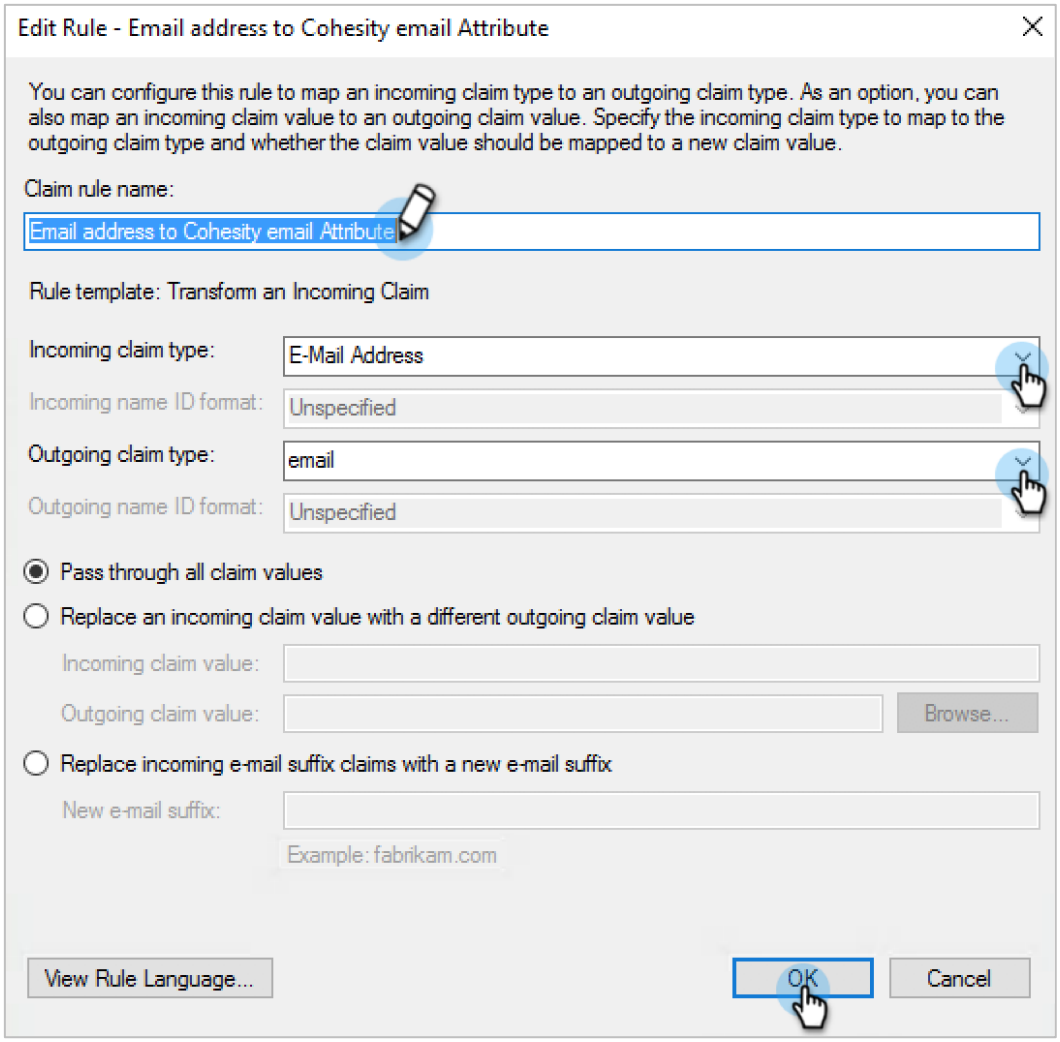
   a) Under **LDAP Attribute**, select **User-Principal-Name**.

b) Under **Outgoing Claim Type**, select **E-Mail Address**.

5. Click **OK** to save your new rule.



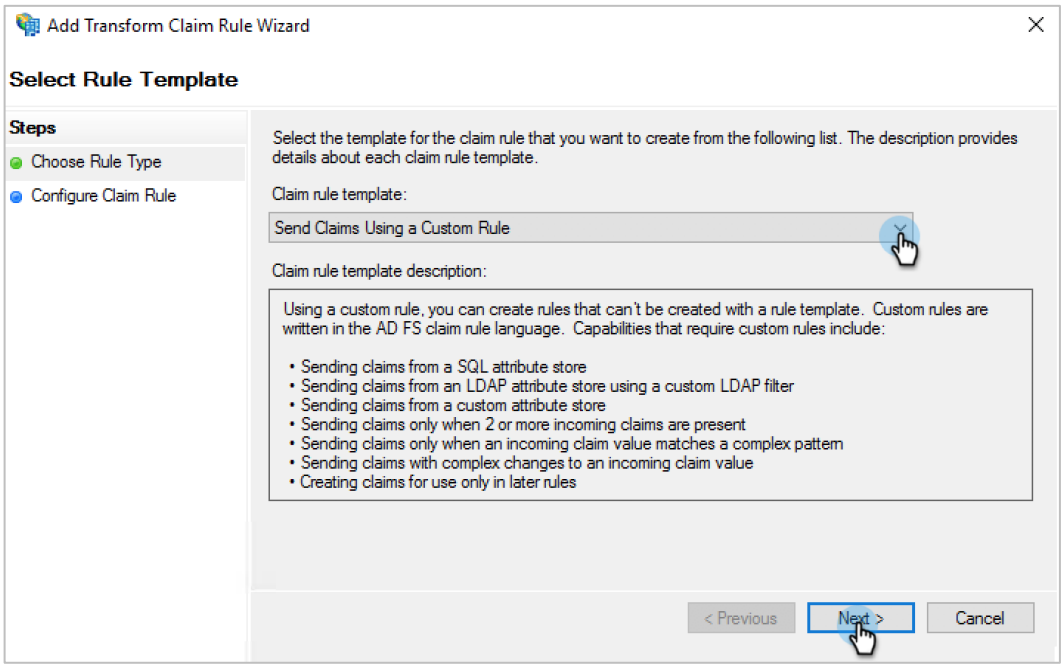
6. Click **Add Rule** to create another rule. This time, select the **Transform an Incoming Claim** rule template. Enter a **Claim rule name** and for **Incoming claim type**, choose **E-Mail Address**. For Outgoing claim type, choose **email**. Click **OK** to save the new rule.



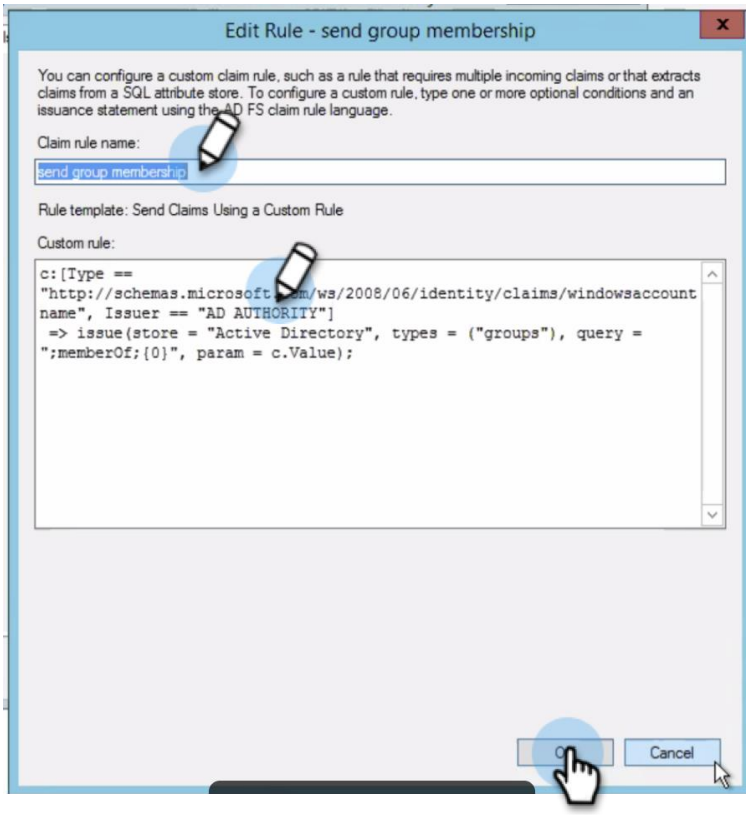
7. Click **OK** again to finish creating rules.
8. Similarly you need to send [“groups” SAML attribute] if you wish to support [User Groups-based RBAC].

9. To extract the user group name and send it to Cohesity, you will need to create a custom rule in AD FS:

   a) Click **Add Rule** and select the **Send Claims Using a Custom Rule** rule template.



b) Enter a **Claim rule name** and then use the Claim Rule Language in AD FS to create and enter a custom rule. Click **OK** to save your custom rule and exit.



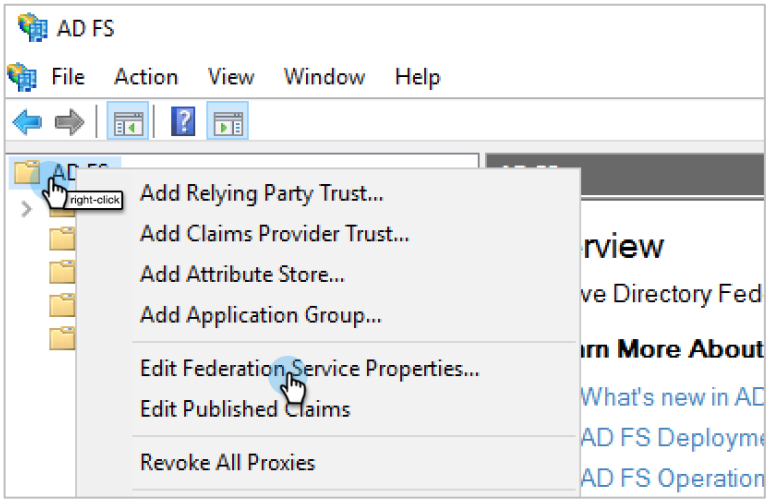
NOTE: This rule might be different for different AD FS configurations. Make sure to edit your custom rule accordingly. Read When to Use a Custom Claim Rule from Microsoft.

Collect SSO URL, Provider Issuer ID, and Certificate

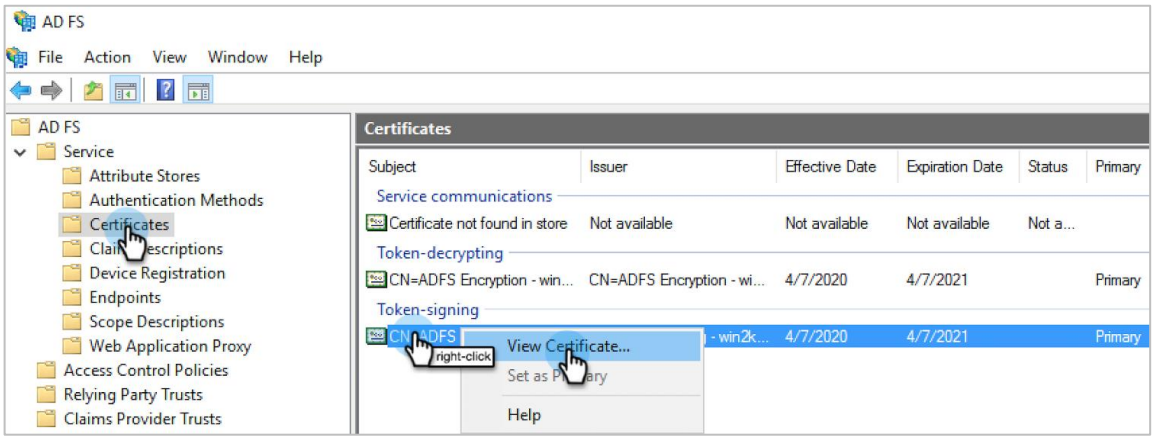
Before you can configure Cohesity for SSO from AD FS, you'll need to collect the Federation Service name that you will use to build the Cohesity SSO URL and the Federation Service Identifier that you will use as the Cohesity Provider Issuer ID when you add AD FS as an SSO provider to Cohesity below.

To collect this information:

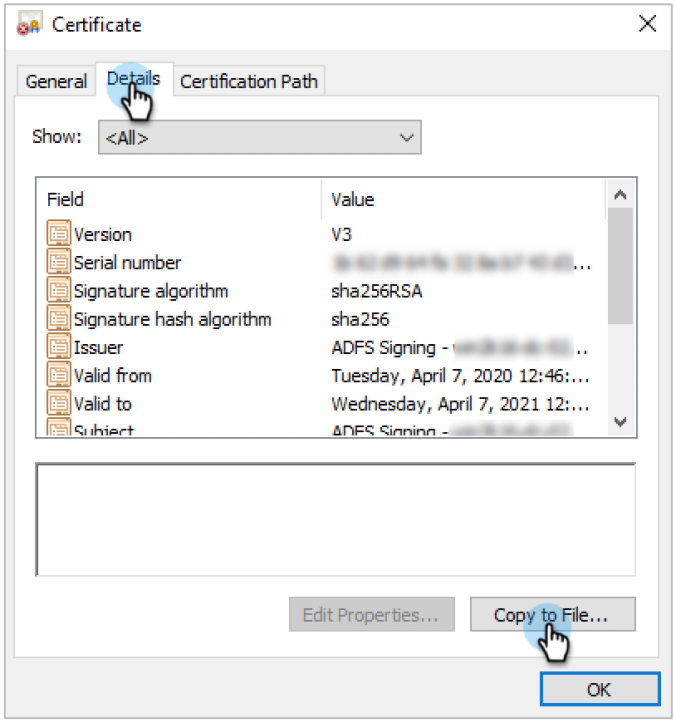
1. Right-click **AD FS** and select **Edit Federation Service Properties**.



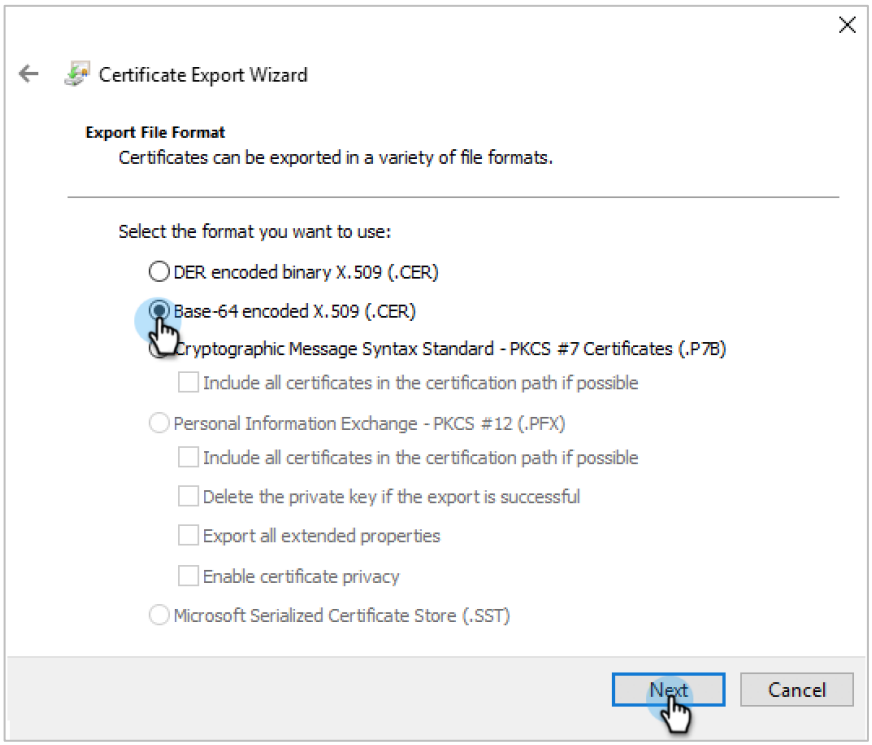
2. From the dialog that opens, copy the **Federation Service name** (to use in the SSO URL) and the **Federation Service Identifier** (to use as the Cohesity Provider Issuer ID).
3. To download the certificate, navigate to **AD FS > Service > Certificates** and in the right panel, right-click the **Token-signing** certificate and select **View Certificate**.



4. On the **Details** tab, click **Copy to File**.



5. The **Certificate Export Wizard** opens. Select **Base-64 encoded X.509 (.CER)**, click **Next**, and follow the instructions to download the certificate (.cer) file to your system.



6. Convert your certificate file from the `.cer` to the `.pem` format. To convert the file:
   - **On Mac/Linux**, simply rename the file with the .pem filename extension.
   - **On Windows**, use:

```
openssl x509 -in mycert.crt -out mycert.pem -outform PEM
```

For more, see this article from Cohesity Support.

Configure SSO Provider on Cohesity

Now that you have created your AD FS Relying Party Trust, use the SAML Signing Certificate and connection links to configure access management on Cohesity.

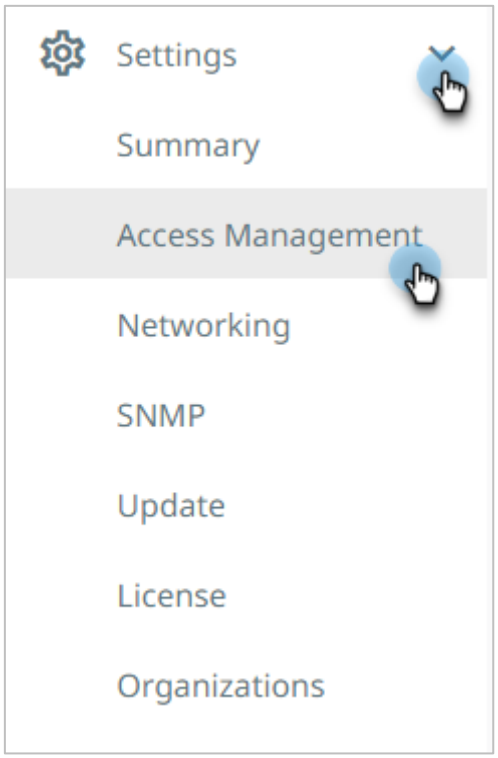
This is how you let Cohesity know where to send the user who is trying to sign in using the SSO option.

Add AD FS as SSO Provider

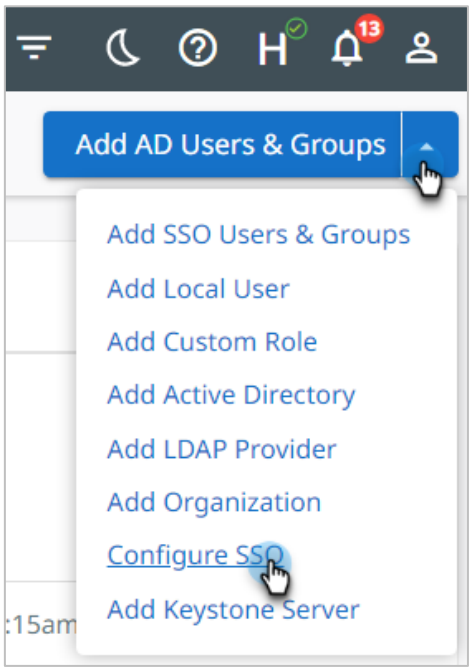
The first step is to use your AD FS details to configure access management on Cohesity .

To add an SSO provider in Cohesity:

1. Log in to Cohesity as an administrator.
2. Navigate to **Settings** > **Access Management**.



3. In the **Access Management** page**,** select **Add Users/Groups > Configure SSO**.



4. In the **Configure SSO** form, use the information you captured earlier to complete the following fields:

   a) **SSO Domain**.

   For Cohesity (on-prem): Enter **AD FS**. (Note that this name should be unique among all SSO provider domain names.

   For Helios: Unique domain name that will differentiate this IdP from others. As Helios supports multiple IdPs, this has to be a unique string (usually company domain). In order for a user to be redirected to this IdP, the user will need to log in via SSO using username@SSO_DOMAIN.

   When a user logs in to Helios using SSO and enters the email address as foo@bar.com, Helios looks for the IdP that has the SSO Domain configured as bar.com and redirects this user foo to the matching IdP. This is how Helios determines which IdP the user needs to be forwarded to.

   b) **SSO Provider**. Enter **AD FS**.

   c) **Single Sign-On URL**. Enter the **Federation Service name** that you copied earlier followed by `/adfs/ls`, as in: `https://<Federation Service name>/adfs/ls`.

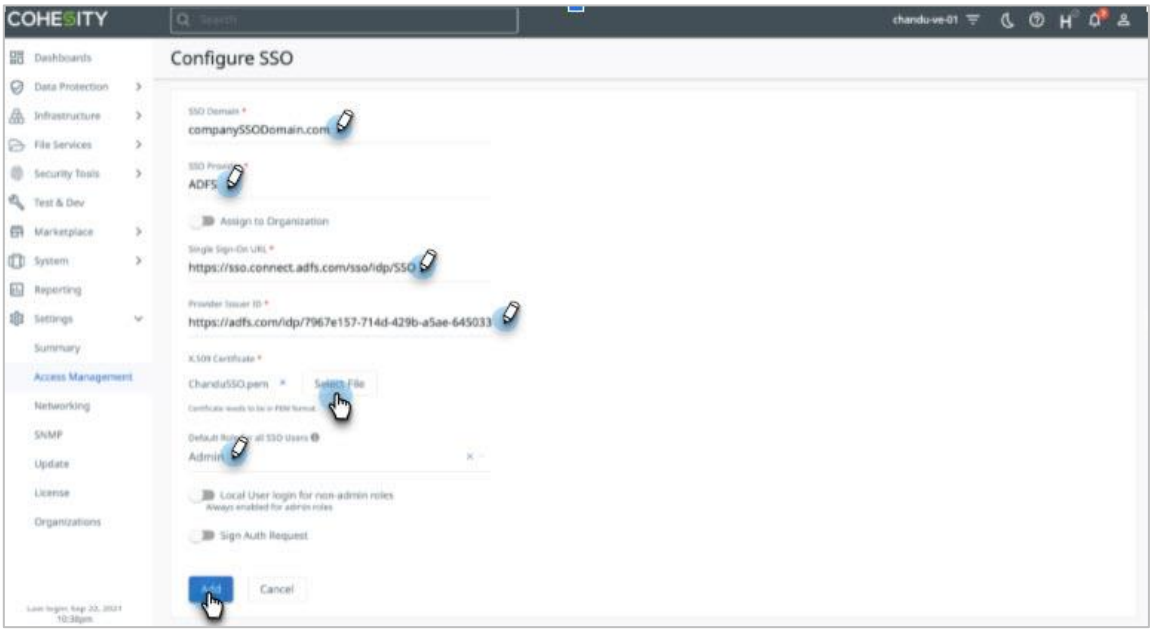
   d) **Provider Issuer ID**. Enter the **Federation Service Identifier** that you copied earlier.

   e) **X.509 Certificate**. Click **Select File** and browse to select the file that you downloaded and converted earlier.

f) **Default Role for all SSO Users**. Choose a default role for any user who logs in using Okta. If you want to specify individual roles for users and groups, see Add SSO Users and Groups below and assign the desired roles. You can change this option later.

5. Click **Add**.

> **NOTE**: To configure Helios, in the **Access Management** page, click the **SSO** tab and then click **Configure SSO**.



Cohesity validates the connection AD FS. If the connection succeeds, AD FS is added to the provider list. Users can start accessing Cohesity via AD FS or the sign-in page by clicking the **Sign in with SSO** link.

Add SSO Users and Groups

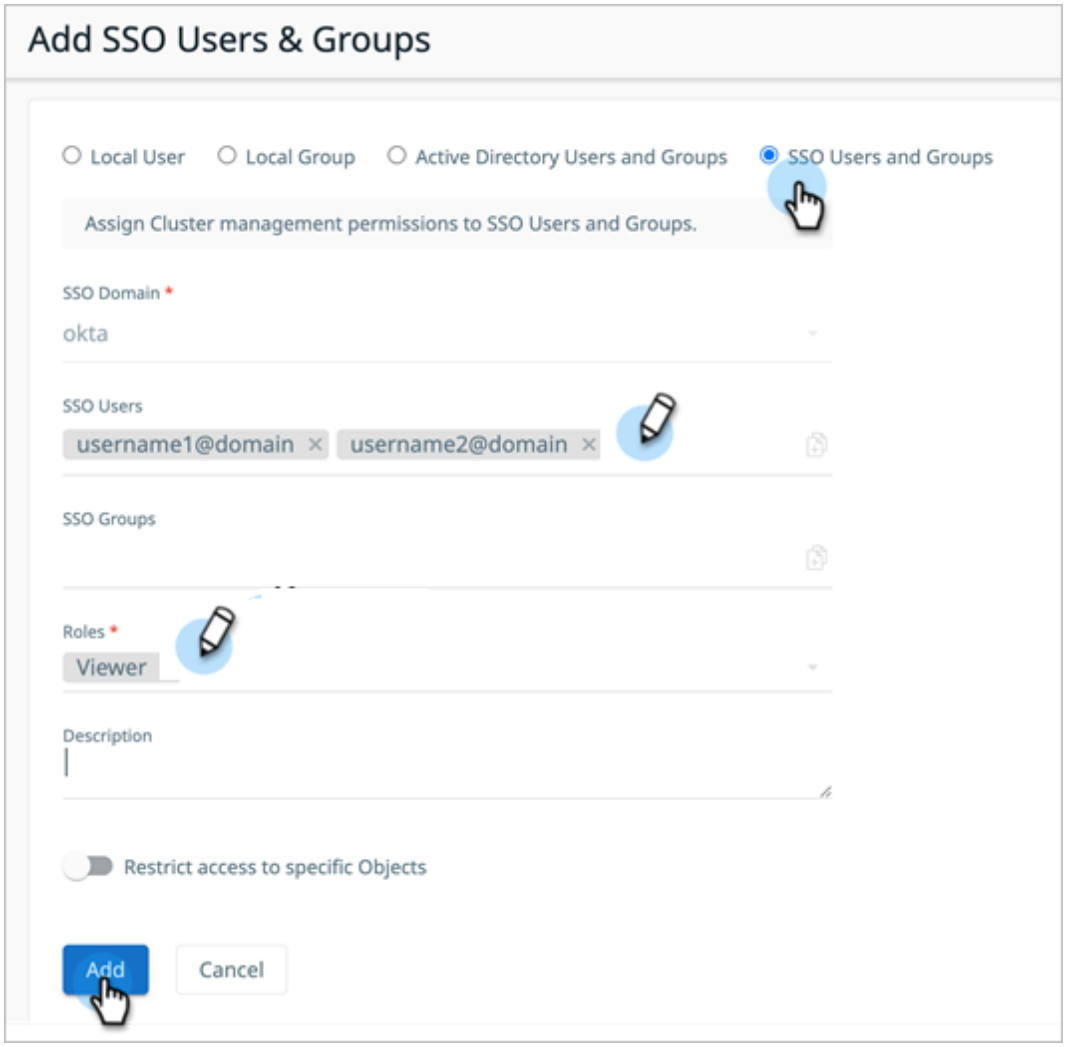
During the SSO setup step, you can optionally add a default role for all SSO users. This might not be desirable in all cases, and you might want to give different access rights to different users and/or groups. There are two ways of doing this. You can:

- Add SSO users and assign rights to them individually.
- Add an SSO group and assign it the desired role.

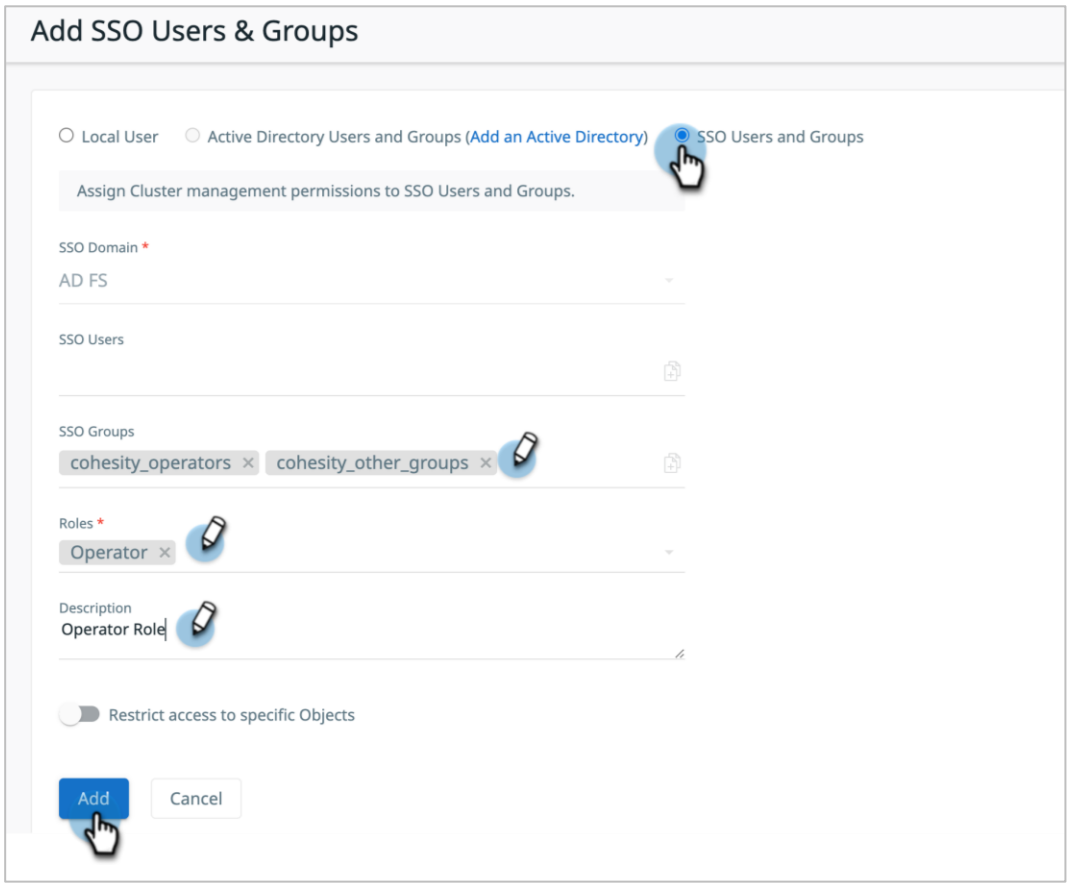
To add SSO users and groups:

1. Log in to Cohesity , select the **Settings** > **Access Management**, and click the **SSO** tab.
2. Click **Add SSO Users & Groups** in the top right corner.
3. In the **Add SSO Users & Groups** form, click **SSO Users and Groups** and then choose which you are adding:

   a) Add the **SSO Users** and assign them the desired role, and click **Add**.



b) Add the **SSO Groups** and assign them the desired role, and click **Add**.



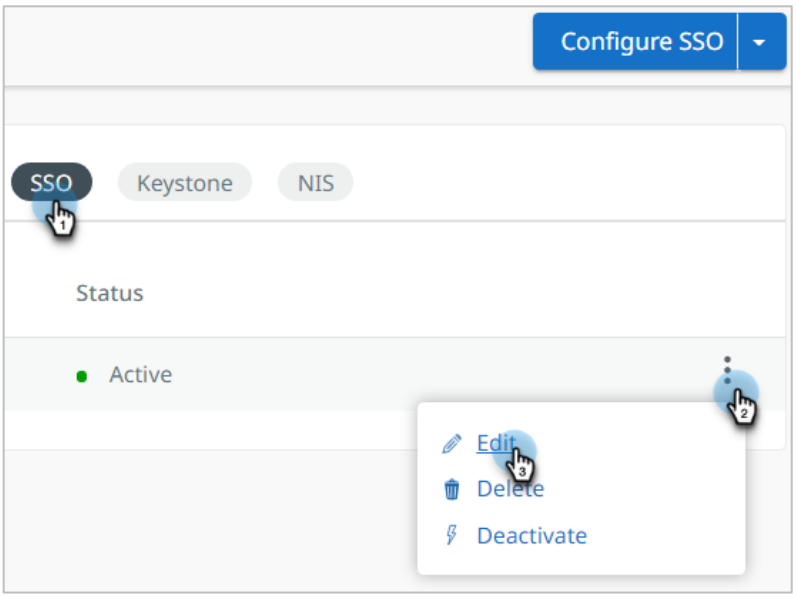
Edit SSO Provider

Once an SSO provider has been added, you can edit, delete, or deactivate it.

To edit an SSO provider:

1. In Cohesity , select **Settings** > **Access Management** and click the **SSO** tab.

2. Open the **Actions Menu** on the right and select **Edit**.



3. Change the options as needed and click **Update**.

Cohesity validates the connection to AD FS using the new information.

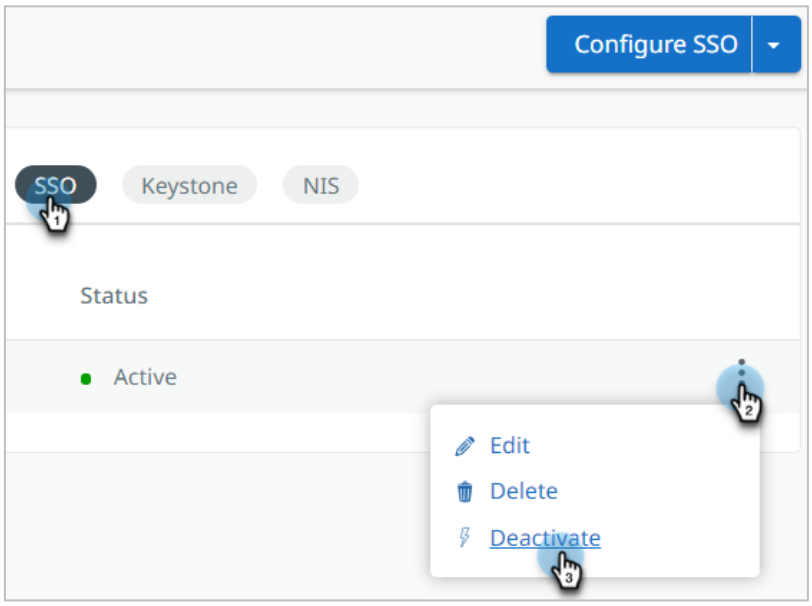
Deactivate SSO Provider

You might want to deactivate an SSO provider for testing or investigation purposes. Deactivation does not delete the provider configuration, so you can activate it later. Once deactivated, users associated with the AD FS provider will no longer bypass the Cohesity sign-in page.

To deactivate or activate an SSO provider:

1. In Cohesity , select **Admin** > **Access Management** and click the **SSO** tab.

2. Locate the SSO provider, open the **Actions Menu** on the right, and select **Deactivate** or **Activate**.

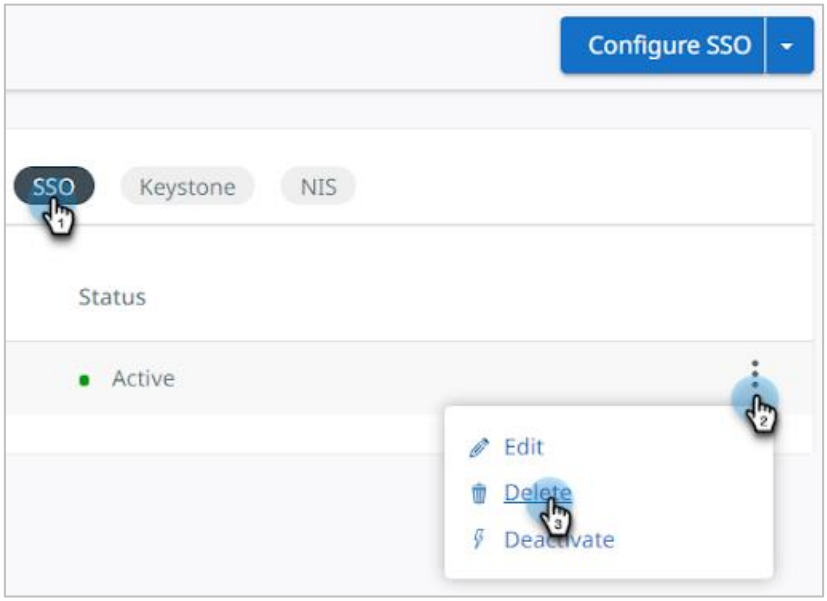


Delete SSO Provider

You can permanently delete an SSO provider if you no longer need it. Once deleted, users associated with the AD FS provider will no longer bypass the Cohesity sign-in page.

To delete an SSO provider:

1. In Cohesity , select **Admin** > **Access Management** and click the **SSO** tab.
2. Locate the SSO provider, open the **Actions Menu** on the right, and click **Delete**.



Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Sagar Sethi is a Staff Technical Solution Engineer at Cohesity. In his role, he focuses on various aspects of Cybersecurity to secure the Cohesity product design & solutions to solve the customer's current challenges for data protection & Zero Trust from advanced threats & organizational risks.

Other essential contributors included:

- Adaikkappan Arumugam, Director, Product Solutions
- Bart Abicht, Sr. Technology Writer and Editor at Cohesity
- Srini Sekaran, Product Marketing Manager at Cohesity

Document Version History

VERSION	DATE	DOCUMENT HISTORY
2.3	Mar 2024	Rebranding updates
2.2	Feb 2022	Minor update
2.1	Sept 2021	Rebranding updates
2.0	Aug 2020	Major update
1.0	June 2019	First release

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 42 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.