COHESITY

Version 2.3

March 2023

Integrate Duo with Cohesity SSO

Enable Seamless Duo Single Sign-On Authentication and Security for Cohesity

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

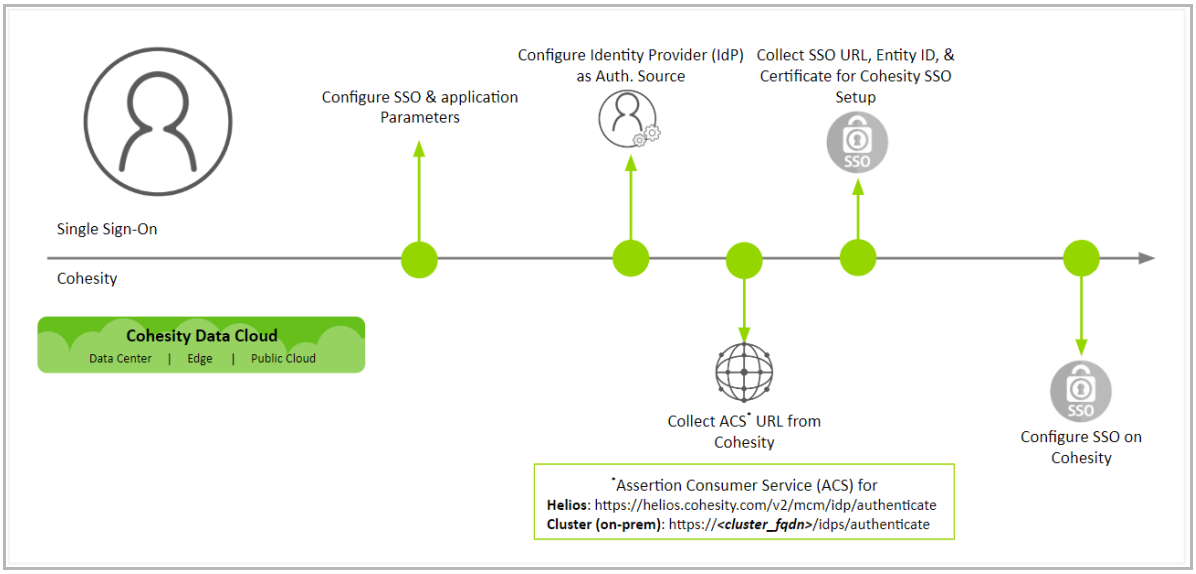
You can configure Cohesity to use a Duo SSO with IdP to access both your dedicated Cohesity clusters as well as multi-tenant Cohesity clusters. On multi-tenant Cohesity clusters, you can configure SSO for each organization that is defined in Cohesity.

NOTE: Duo has announced a deprecation timeline for Duo Access Gateway (DAG) and new integrations will be created on Duo Single Sign-On, a cloud-hosted SAML identity provider.

Integrate Cohesity with SSO

To integrate Cohesity with an SSO provider, you need to configure details on both the SSO and IdP platform, and the Service Provider (SP)—in this case, Cohesity.

Figure 1: Integrate Cohesity with SSO

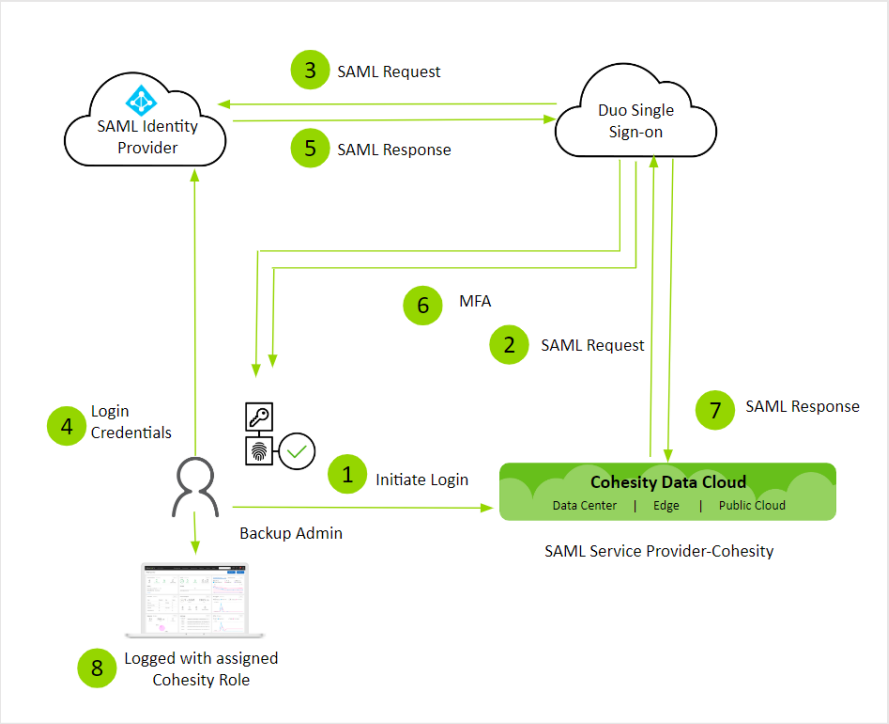


The authentication workflow can start with SSO and Service Provider as below:

1. Cohesity Backup Admin login to Cohesity cluster.
2. Cohesity cluster redirects the admin's browser to Duo Single Sign-On with a SAML request message.
3. Duo Single Sign-On redirects the admin's browser to the SAML identity provider IdP (Azure AD in this case) with a SAML request message.
4. Cohesity Backup Admin pass the login credentials.
5. SAML identity provider redirects the admin's browser to Duo Single Sign-On with a response message.
6. Duo Single Sign-On requires the admin to complete two-factor authentication (optional).
7. Duo Single Sign-On redirects the admin's browser to the Cohesity cluster with a response message.

8. Cohesity Backup Admin is successfully logged in with the assigned Cohesity role.

Figure 2: SSO Authenticates Cohesity Admin and Assigns Cohesity Role



Map SAML Attributes for SSO

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 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

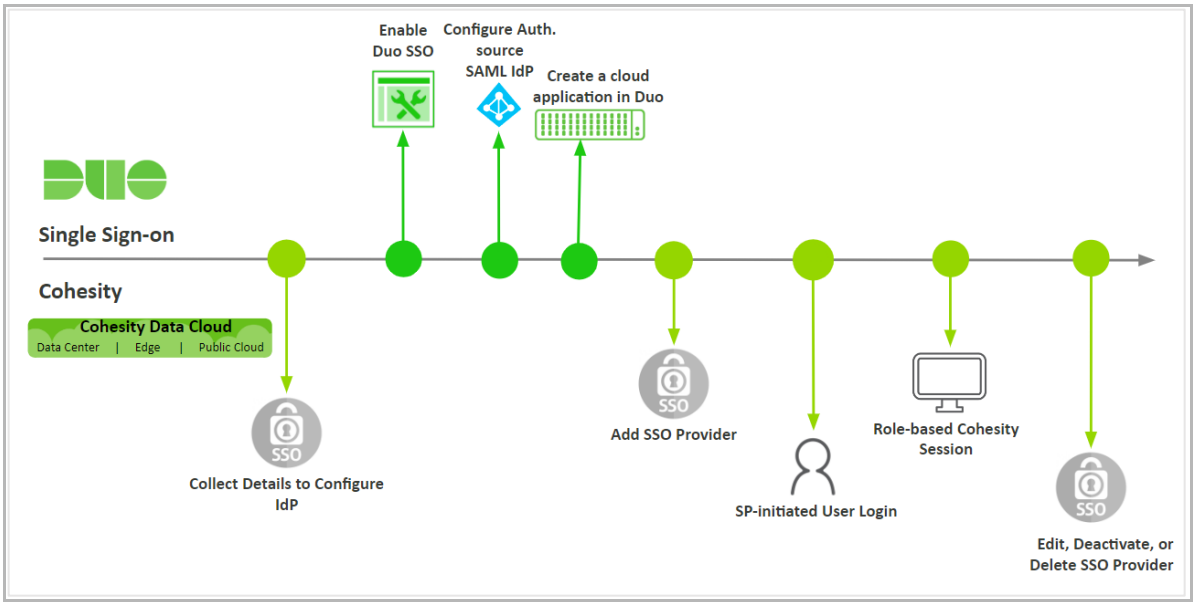
In general, it is a best practice to deploy SSO with user groups-based RBAC and assign custom roles to different user groups. To do so, you need to pass the “Groups” SAML attribute to Cohesity. The value of the “Groups” attribute is a list of groups that the user belongs to, and can include more than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

To configure and use Duo on Cohesity, you need to configure certain parameters on the Duo SSO, IdP, and then use this information to configure SSO on Cohesity.

Figure 3: Cohesity Access Management with Duo SSO Lifecycle



Configure SSO

The first step to configure Duo SSO on Cohesity is to supply some information to the IdP, Azure in this case. With these details, Duo can send the SAML response with the information about the authenticated user. The only piece of information you need from Cohesity is a 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 **Entity ID** and **Assertion Consumer Service** URL when you create the Duo application below.

To configure Duo SSO:

1. Enable Duo Single Sign-On.
2. Set up an authentication source in the Duo SSO.
3. Create a cloud application in Duo.
4. Enable the Universal Prompt.
5. Collect the SSO URL, Provider Issuer ID, and certificate from Duo.

When you complete these steps, you'll be ready to set up Duo for SSO on Cohesity.

Enable Duo Single Sign-On

The first thing you need to do is, enable Duo SSO, which will allow you to set up an authentication source. Then create the Duo SSO application and connect it to Cohesity. To set up the Duo SSO on Windows or Linux, see Enable Duo Single Sign-on page.

Set Up Authentication Source in the Duo SSO

The next step is to set Cohesity up as an authentication source for Duo SSO.

Duo Single Sign-On allows you to use either Active Directory domains and forests or a SAML Identity Provider as a first-factor authentication source.

For the purpose of writing this document, SAML Based Azure AD was used as the Authentication Source.

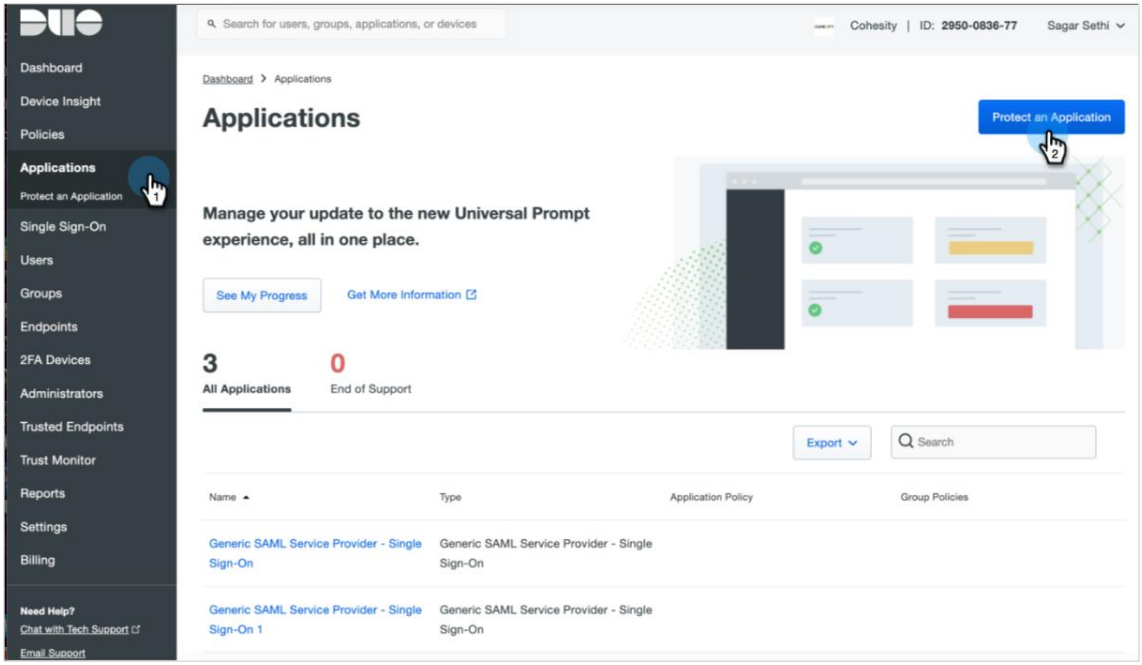
NOTE: Only one type of authentication source may be enabled for use at a time.

NOTE: For SSO to work with Cohesity, one of the two attributes ("Email" or "Login") must be passed. Note also that different authentication sources might use different attribute names (instead of "Email" or "Login") for the email address. You will have an opportunity to map them to Cohesity's SAML response attributes when you create your cloud application next.

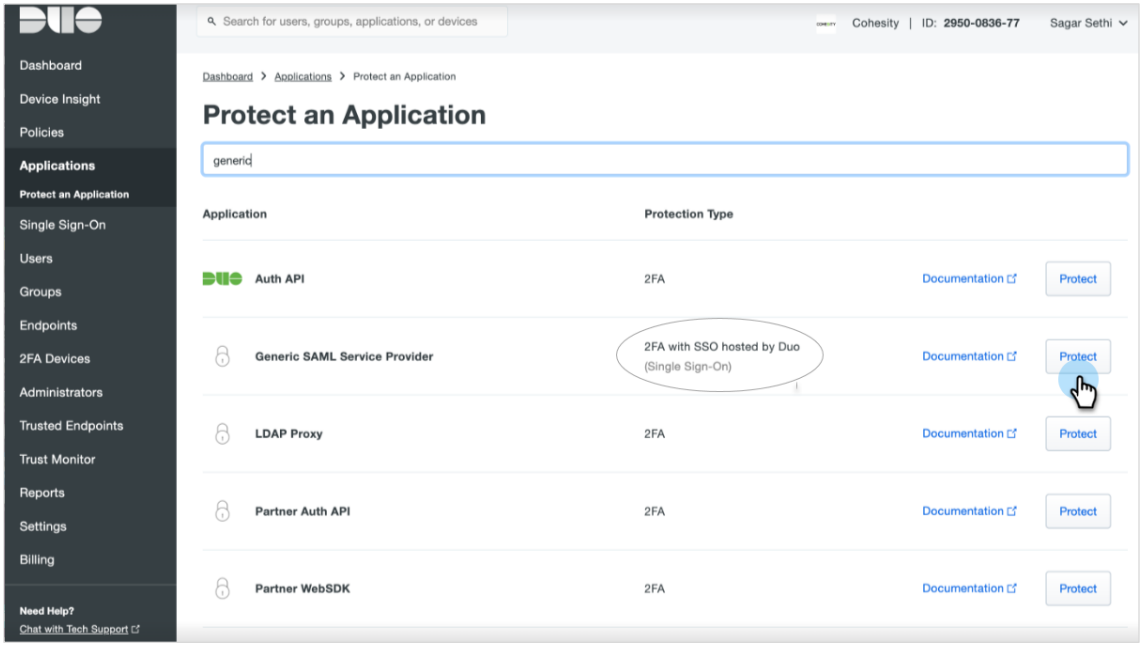
Create a Cloud Application in Duo

To configure Cohesity as a Duo Service Provider, you need to create an application in Duo:

1. Log in to the Duo Admin Panel, click **Applications** on the left, and then click **Protect an Application**.

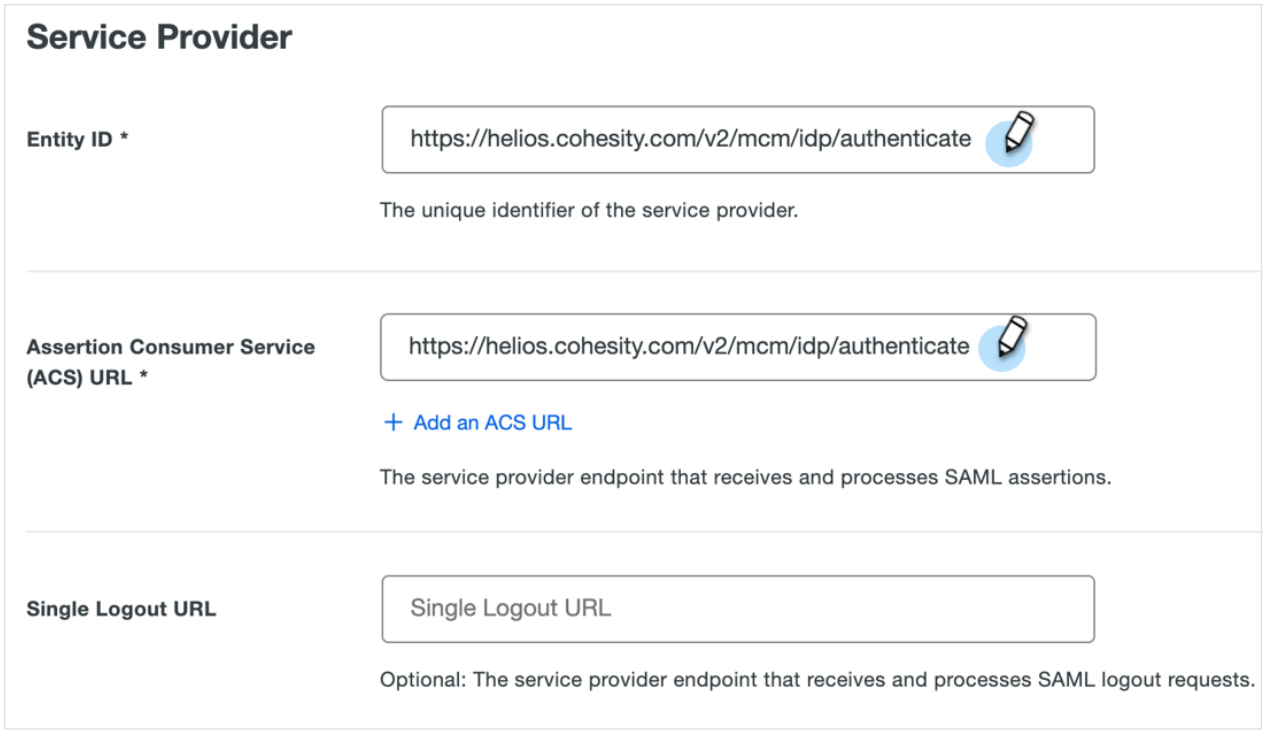


2. Under **Application**, find **Generic Service Provider** in the list. Choose the row listed as **2FA with SSO-hosted by Duo** and click **Protect**.

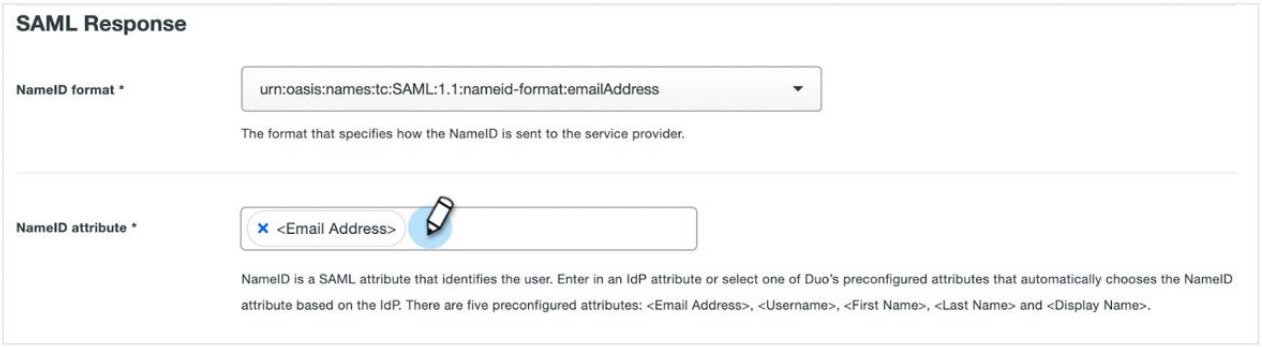


3. On the **Generic Service Provider** page, under **Service Provider**, enter:

   - **Entity ID**: Identifier for the service provider. Enter the same URL that you'll use for **Assertion Consumer Service** in the next field.
   - **Assertion Consumer Service**: The service provider endpoint that receives and processes SAML 2.0 assertions. For:
     - **Cohesity (on-prem)**, log in to Cohesity to get the cluster's FQDN and add `'/idps/authenticate'` to the URL. Use the format: `https://<cluster_fqdn>/idps/authenticate`.
     - **Cohesity Helios**, use the URL: `https://helios.cohesity.com/v2/mcm/idp/authenticate`.



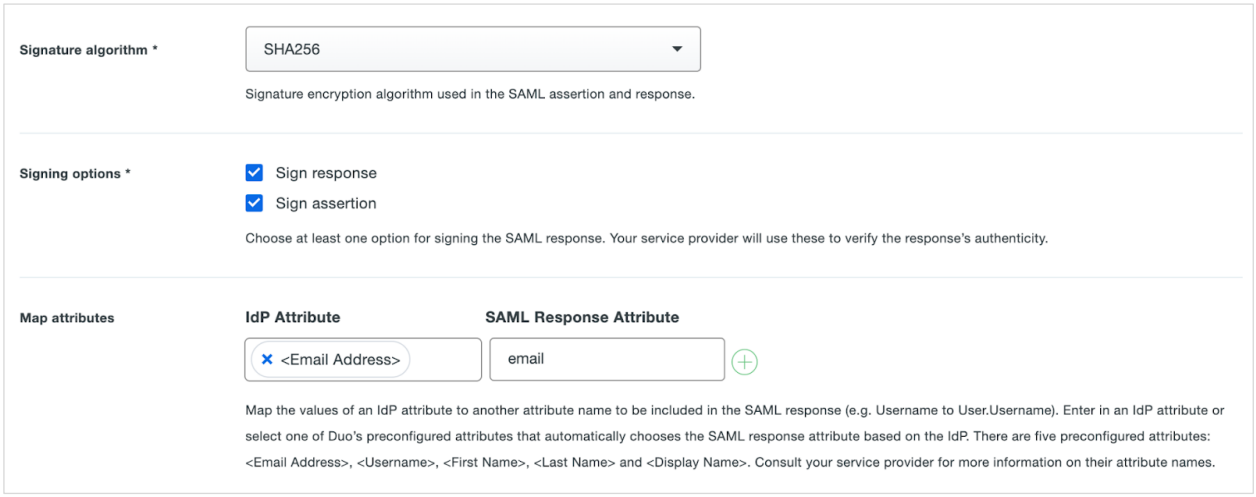
4. On the same page, under **SAML Response**, for **NameID attribute**, enter *email*.



5. Under **Map attributes,** map the attribute that will be sent by the Authentication Source to the attribute name that Cohesity expects (“Email” or “Login”). In our example using Azure AD, the **IdP Attribute** “mail” stores a user’s email address, so we will map “mail” to “Email” for the **SAML Response Attribute**.

   Optionally, if you want to give groups-based access to users, you can also map the “memberOf” AD attribute (stores the names of the groups that the user belongs to) to “Groups” SAML attribute. This enables you to add the AD groups to the Cohesity cluster as an SSO group with specific access rights.

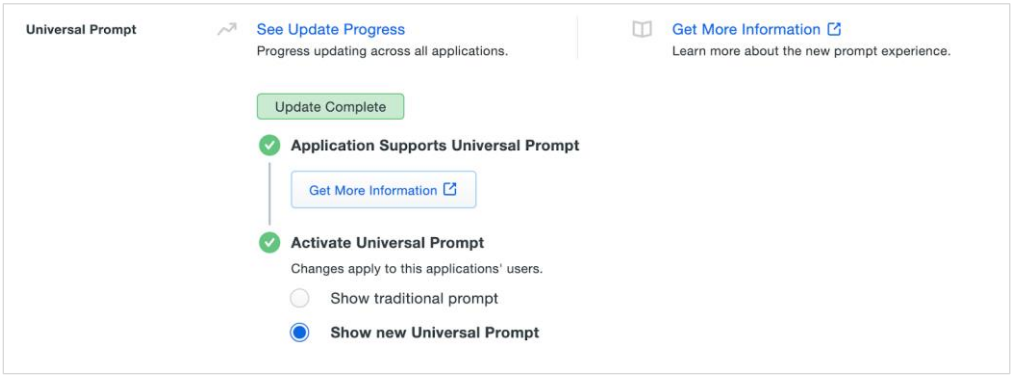
   When you complete the mappings, click **Save Configuration**.



Enable Universal prompt

Once you create the application in Duo, activate a new Universal Prompt which provides a simplified and accessible Duo login experience for web-based applications.

Enable the Universal Prompt by selecting **Show new Universal Prompt**, and then scroll to the bottom of the page and click **Save**.

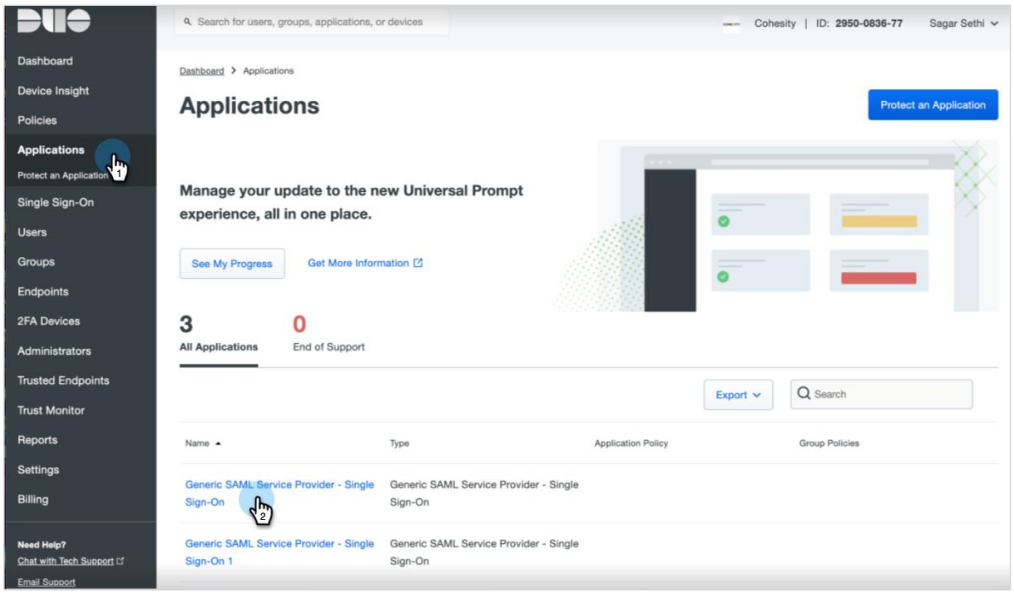


Collect SSO URL, Provider Issuer ID, and Certificate

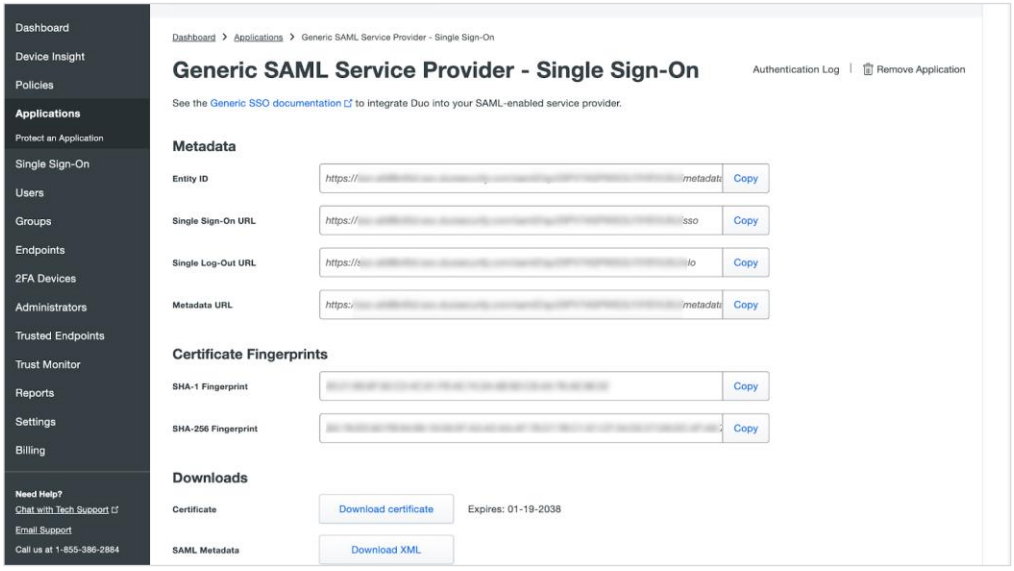
You'll need to provide some information about Duo Single Sign-On to your application Service Provider Cohesity, like URL information, a metadata file, a certificate file, or a certificate fingerprint. You can find this information in the **Metadata** section at the top of the application page in the Duo Admin Panel.

To collect the SSO URL, Provider Issuer ID, and certificate from the application:

1. In your Duo SSO, navigate to **Applications**.



2. Click **Generic SAML Service Provider- Single Sign-On**. Under **Metadata**, find and save the **SSO URL** and **Entity ID** you will enter when you add Duo as an SSO provider to Cohesity next. Download the certificate and rename it as `dag.pem`.



Configure SSO Provider on Cohesity

Now that you have created your Duo application, 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.

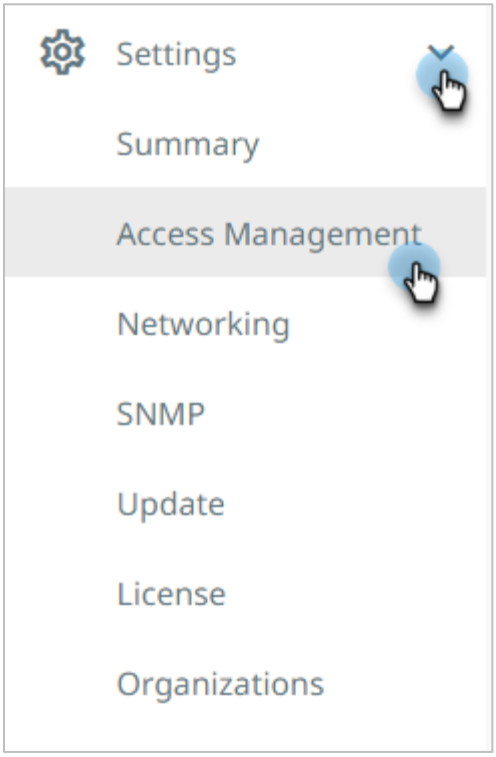
Add Duo as SSO Provider

Now that you have added the Cohesity Duo application to the gateway, use your Duo details to configure access management on Cohesity.

To add an SSO provider in Cohesity:

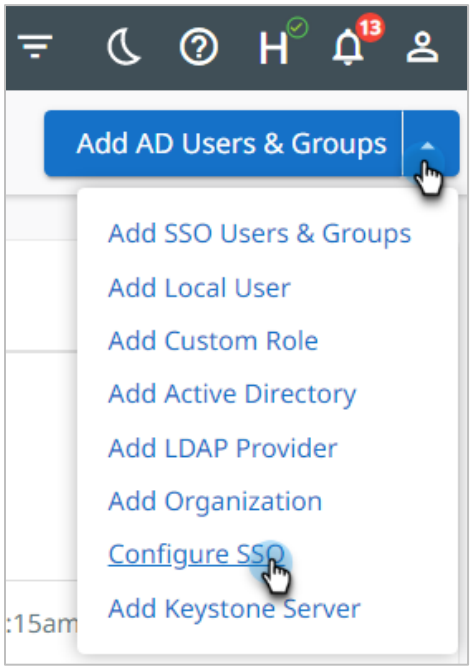
1. Log in to Cohesity as an administrator.

2. Navigate to **Settings** > **Access Management.**



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

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

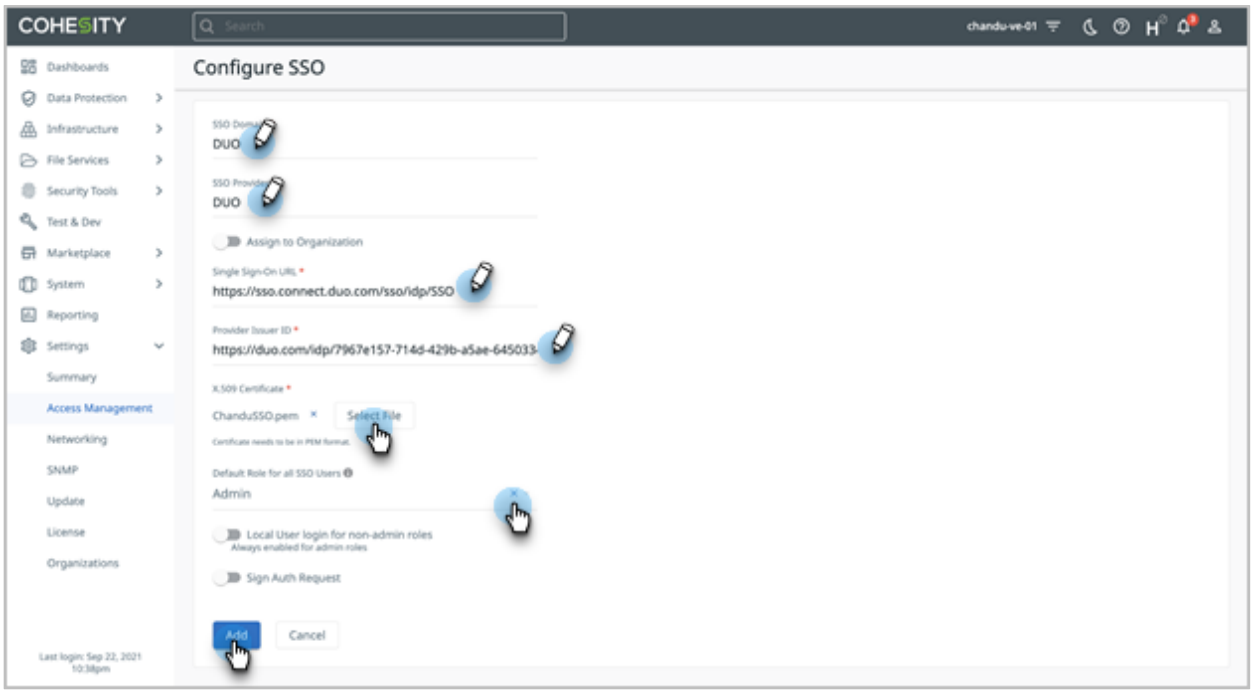
   c) **Single Sign-On URL**. Enter the **SSO URL** that you copied from Duo earlier.

   d) **Provider Issuer ID**. Enter the **Entity ID** that you copied from Duo earlier.

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

   f) **Default Role for all SSO Users**. Choose a default role for any user who logs in using Duo. 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**.



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

Add SSO Users and Groups

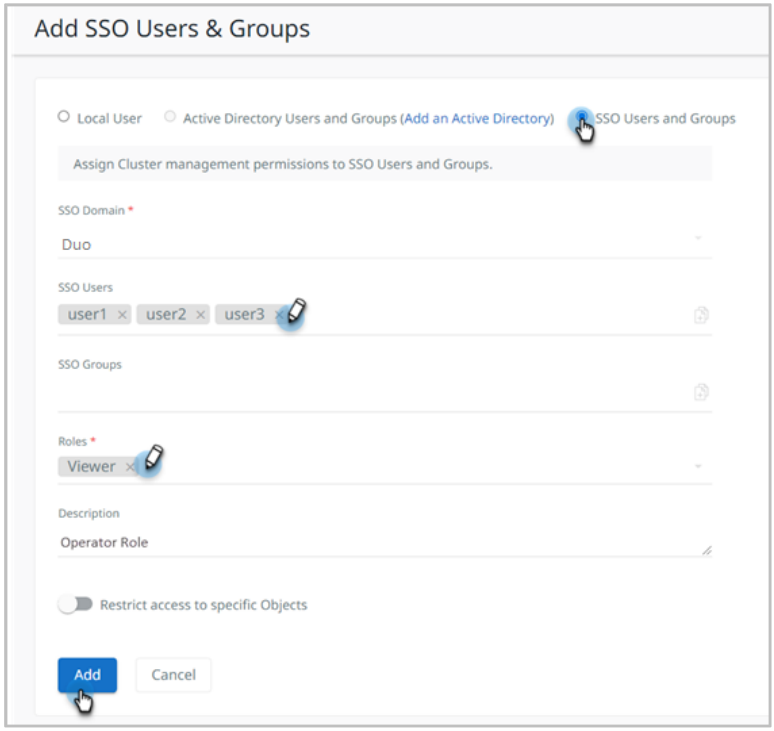
During the SSO setup step, you can optionally add a default role for all SSO users. This might not be desirable in all cases, and you might want to give different access rights to different users and/or groups. There are two ways of doing this. You can:

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

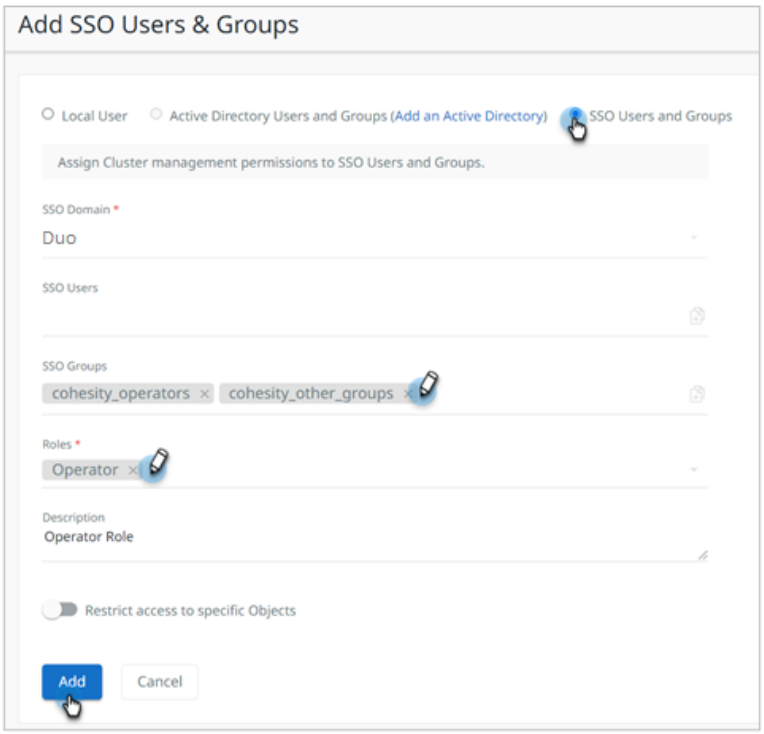
To add SSO users and groups:

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 then click **Add**.



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

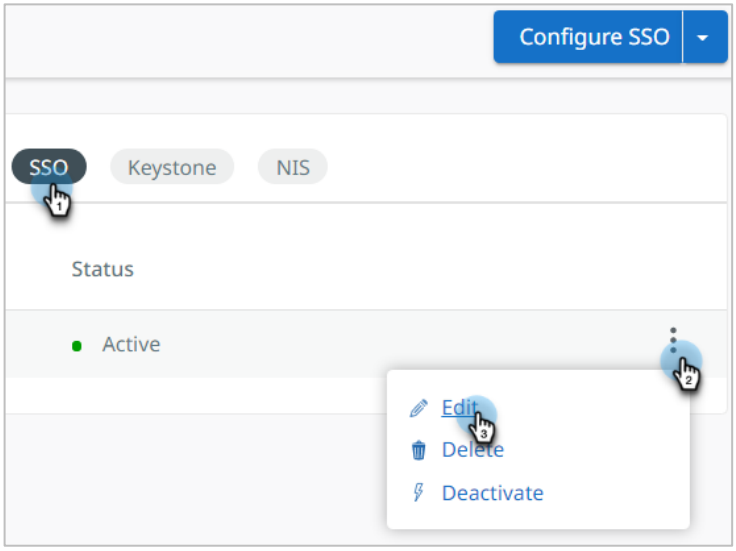


Edit SSO Provider

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**.

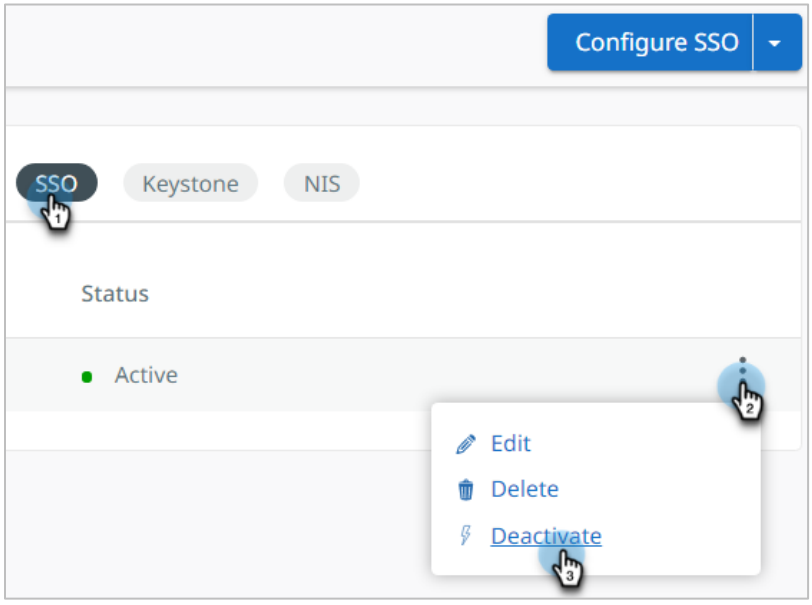
Cohesity validates the connection to Duo using the new information.

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 again later. Once deactivated, users associated with the Duo provider will no longer bypass the Cohesity sign-in page.

To deactivate or activate an SSO provider:

1. In Cohesity, select **Settings** > **Access Management** and click the **SSO** tab.
2. Locate the SSO provider, open the **Actions Menu** on the right, and select **Deactivate** or **Activate**.



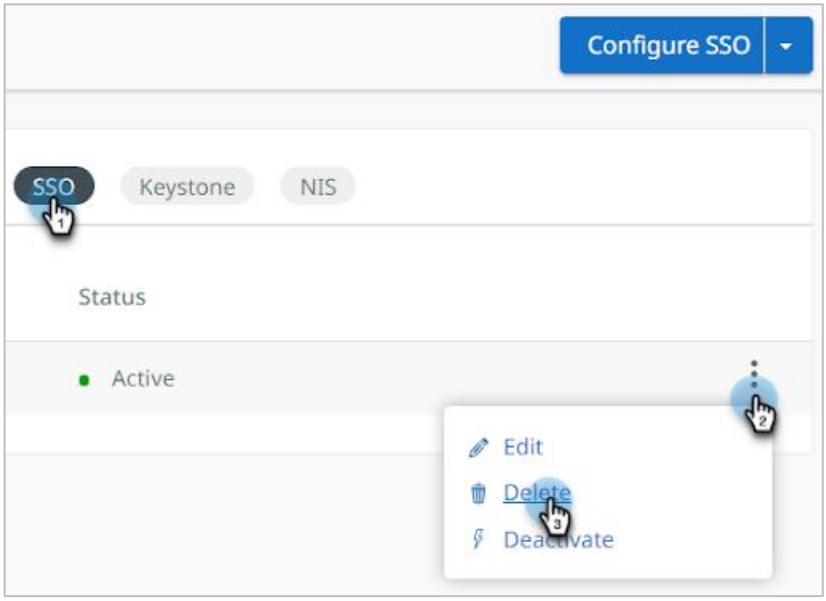
Delete SSO Provider

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

To delete an SSO provider:

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

2. Locate the SSO provider, open the **Actions Menu** on the right, and select **Delete**.



Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Karthick Radhakrishnan is Director, Technical Product Marketing. In his role, Karthick focuses on managing the technical marketing of Cohesity products and solutions.

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 2023	Rebranding updates
2.2	Sept 2022	Content update
2.1	Sept 2021	Rebranding updates
2.0	Aug 2020	Major update
1.0	June 2019	First release

ABOUT COHESITY

Cohesity radically simplifies data management. We make it easy to protect, manage, and derive value from data -- across the data center, edge, and cloud. We offer a full suite of services consolidated on one multicloud data platform: backup and recovery, disaster recovery, file and object services, dev/test, and data compliance, security, and analytics -- reducing complexity and eliminating mass data fragmentation. Cohesity can be delivered as a service, self-managed, or provided by a Cohesity-powered partner.

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