COHESITY

Version 2.2

September 2021

Integrate Azure AD with Cohesity SSO

Enable Seamless Azure AD 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

Single Sign-On (SSO) Benefits 3

Default RBAC 3

Individual User-based RBAC 3

User Groups-based RBAC........ 4

Cohesity Offers Seamless SSO Support........ 5

Integrate Cohesity with IdP 5

Map SAML Attributes for SSO setup........ 7

Pass “Email” or “Login” SAML Attribute to Cohesity 7

Pass “Groups” SAML Attribute to Cohesity........ 7

Configure Access Management with Azure AD 8

Configure IdP........ 8

Create an Azure Active Directory Application 9

Collect SSO URL, Provider Issuer ID, and Certificate........ 14

Configure SSO Provider on Cohesity........ 16

Add Azure AD as SSO Provider 16

Add SSO Users and Groups 18

Edit SSO Provider........ 21

Deactivate SSO Provider........ 21

Delete SSO Provider 22

Your Feedback 23

About the Authors........ 23

Document Version History........ 23

Figures

Figure 1: Integrate Cohesity with Identity Provider........ 5

Figure 2: IdP authenticates Cohesity User and Assigns Cohesity Role 6

Figure 3: Cohesity Access Management with Azure AD SSO Lifecycle........ 8

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.

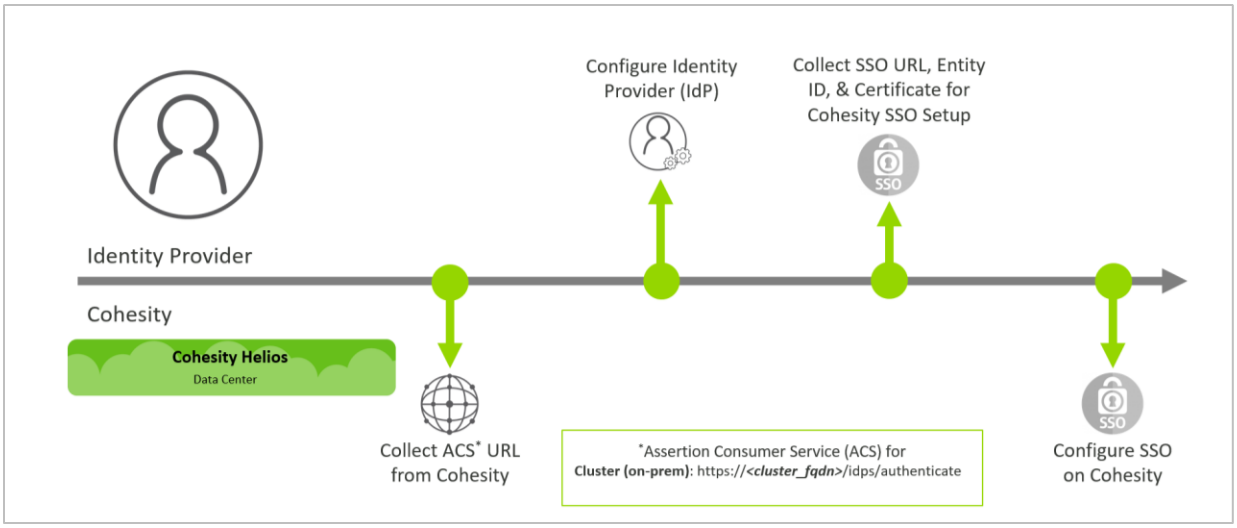
Cohesity Offers Seamless SSO Support

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

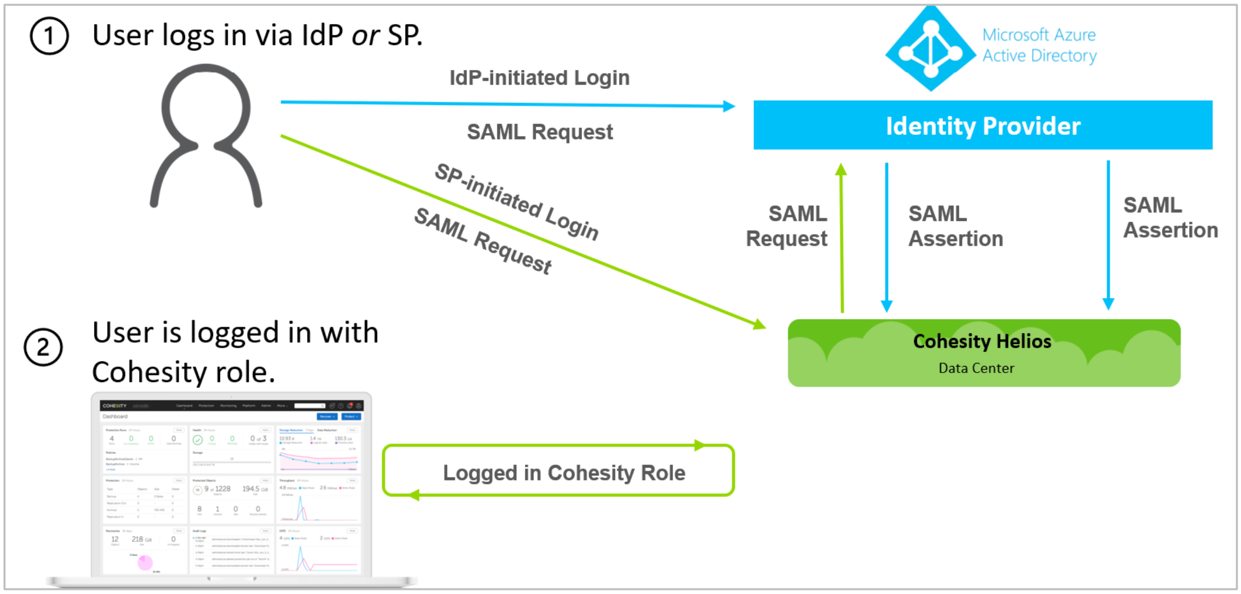
Figure 1: Integrate Cohesity with Identity Provider


Configure Identity Provider (IdP)
Collect SSO URL, Entity ID, & Certificate for Cohesity SSO Setup
SSO
Identity Provider
Cohesity
Cohesity Helios
Data Center
Collect ACS* URL from Cohesity
*Assertion Consumer Service (ACS) for
Cluster (on-prem): https://<cluster_fqdn>/idps/authenticate
SSO
Configure SSO on Cohesity

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

1. User logs in via either:
   a) **IdP**: The identity provider, Azure AD, 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, Azure AD. Azure AD 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

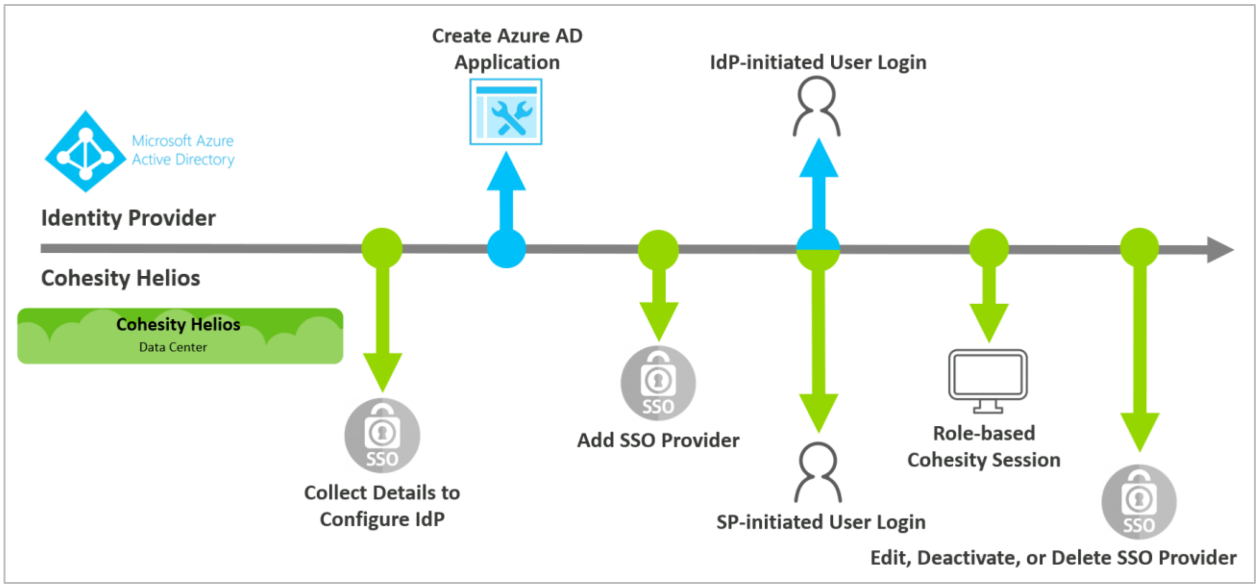
In general, it is a best practice to deploy SSO with user groups-based RBAC and assign custom roles to different user groups. To do so, you need to pass the “Groups” SAML attribute to Cohesity. The value of the “Groups” attribute is a list of groups that the user belongs to, and can include more than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

To configure and use Single Sign-on with Azure Active Directory 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 Azure AD SSO Lifecycle


Create Azure AD Application
IdP-initiated User Login
Microsoft Azure Active Directory
Identity Provider
Cohesity Helios
Cohesity Helios
Data Center
SSO
Collect Details to Configure IdP
SSO
Add SSO Provider
SP-initiated User Login
Role-based Cohesity Session
SSO
Edit, Deactivate, or Delete SSO Provider

Configure IdP

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

- `https://`***`<cluster_fqdn>`***`/idps/authenticate`

Use this URL as the Entity ID and Reply URL when you create the Azure AD application below.

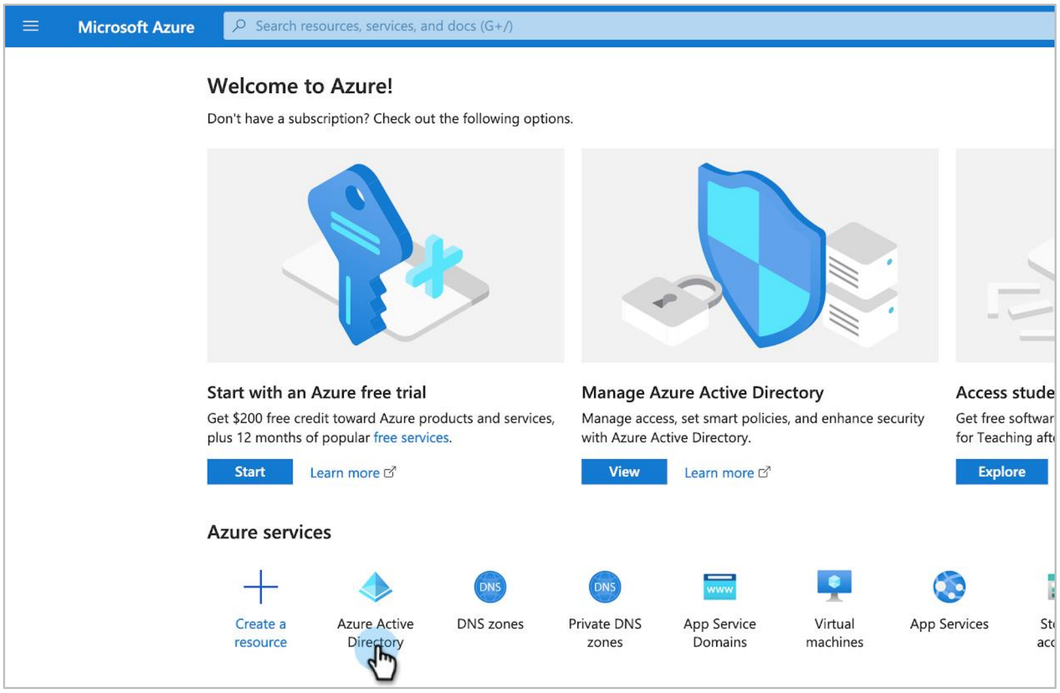
To configure the IdP:

1. Create a Azure Active Directoryapplication.
2. Collect the SSO URL, Entity ID, and certificate from Azure AD.

Create an Azure Active Directory Application

To configure Cohesity as an Azure AD service provider, you need to create an Azure AD SSO application:

1. Log in to https://portal.azure.com. under **Azure services**, click **Azure Active Directory**.



Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

Manage Azure Active Directory

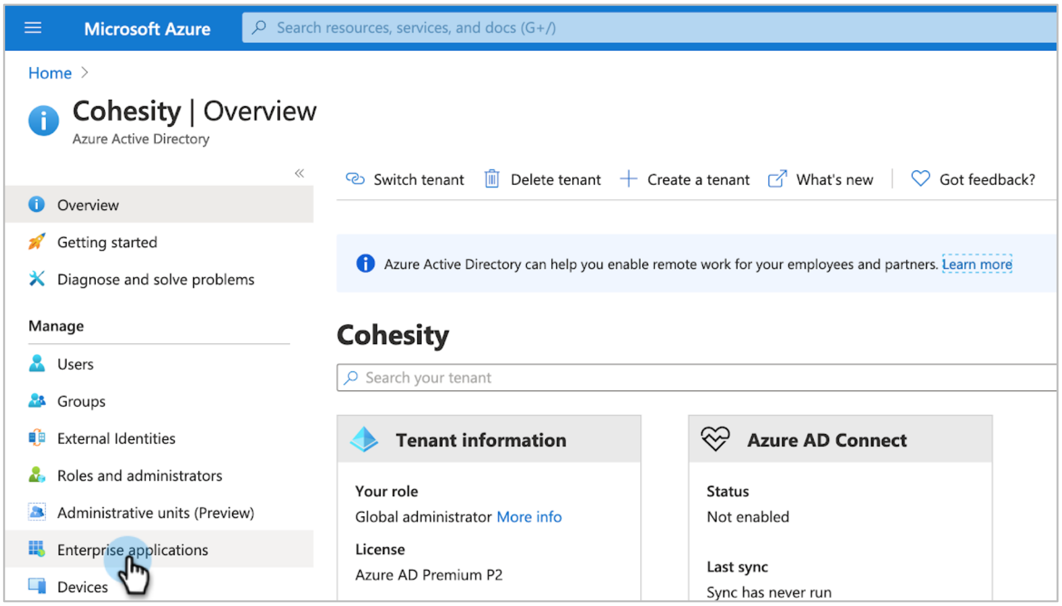
Manage access, set smart policies, and enhance security with Azure Active Directory.

Access stude

Get free softwar for Teaching aft

Azure services

2. On the left, click **Enterprise applications**.



Cohesity | Overview

Azure Active Directory

Azure Active Directory can help you enable remote work for your employees and partners. Learn more

Cohesity

Tenant information

Your role: Global administrator More info

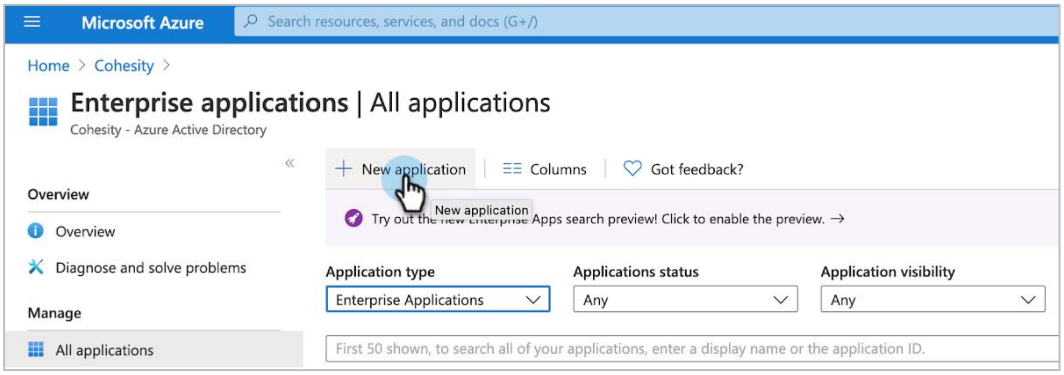
License: Azure AD Premium P2

Azure AD Connect

Status: Not enabled

Last sync: Sync has never run

3. Under **All applications**, click **New application**.



Enterprise applications | All applications

Cohesity - Azure Active Directory

Try out the new Enterprise Apps search preview! Click to enable the preview. →

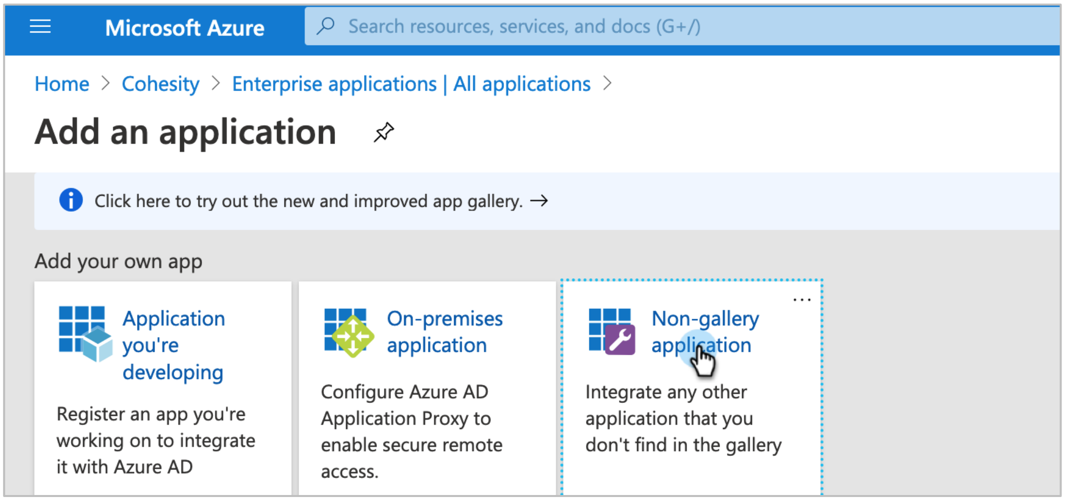
Application type: Enterprise Applications

Applications status: Any

Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

4. On the **Add an application** page, click **Non-gallery application**.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Cohesity > Enterprise applications | All applications >
...

Add an application

Click here to try out the new and improved app gallery. →

Add your own app

Application you're developing

Register an app you're working on to integrate it with Azure AD

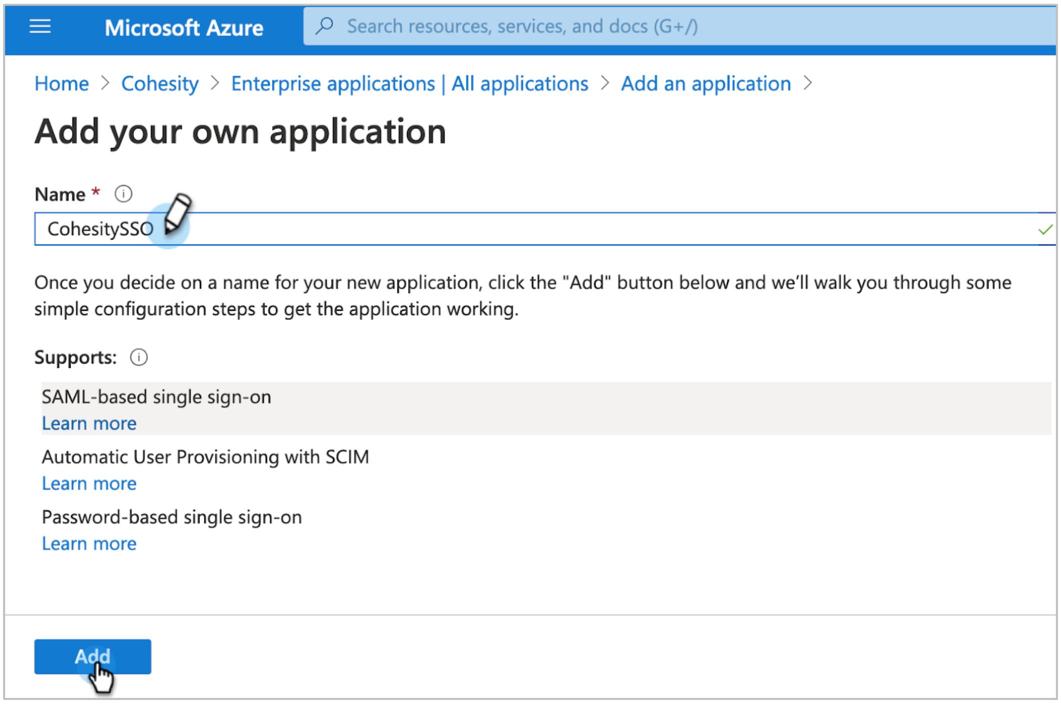
On-premises application

Configure Azure AD Application Proxy to enable secure remote access.

Non-gallery application

Integrate any other application that you don't find in the gallery

5. Enter a display name for your application and click **Add**.



Home > Cohesity > Enterprise applications | All applications > Add an application >

Add your own application

Name *

CohesitySSO

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

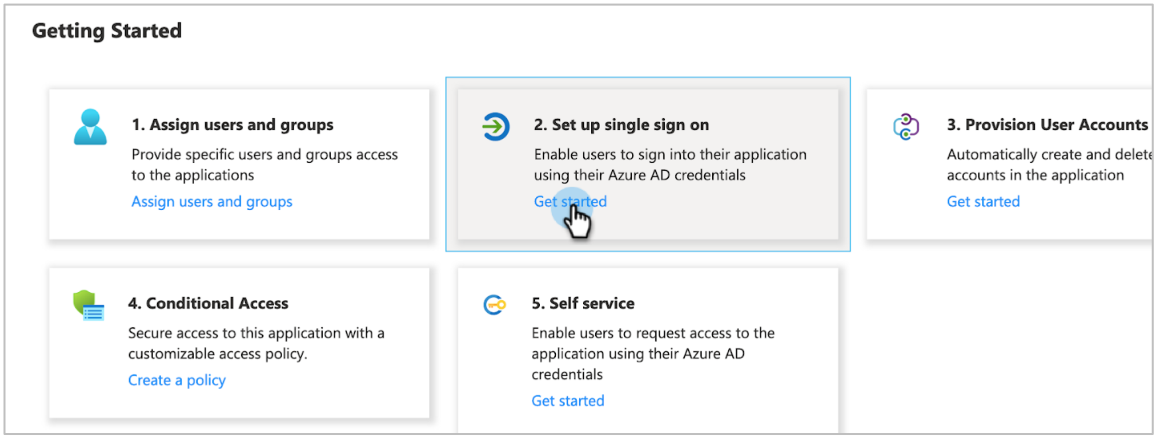
Supports:

SAML-based single sign-on
Learn more

Automatic User Provisioning with SCIM
Learn more

Password-based single sign-on
Learn more

6. On the **Set up single sign on** tile, click **Get started**.



Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

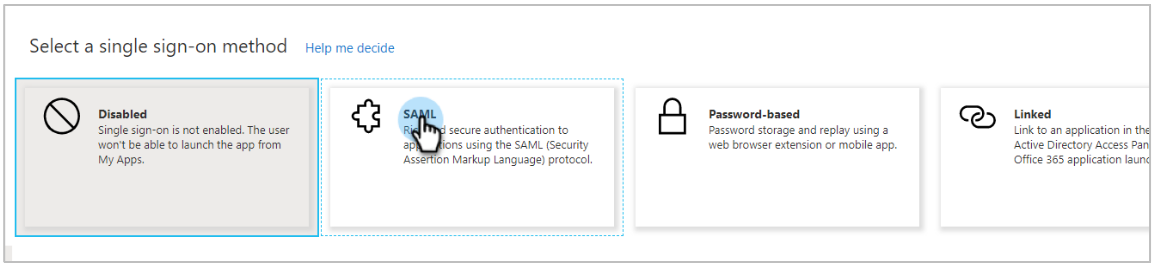
2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
Automatically create and delete accounts in the application
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

7. Under **Select a single sign-on method**, choose **SAML**.



Select a single sign-on method Help me decide

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

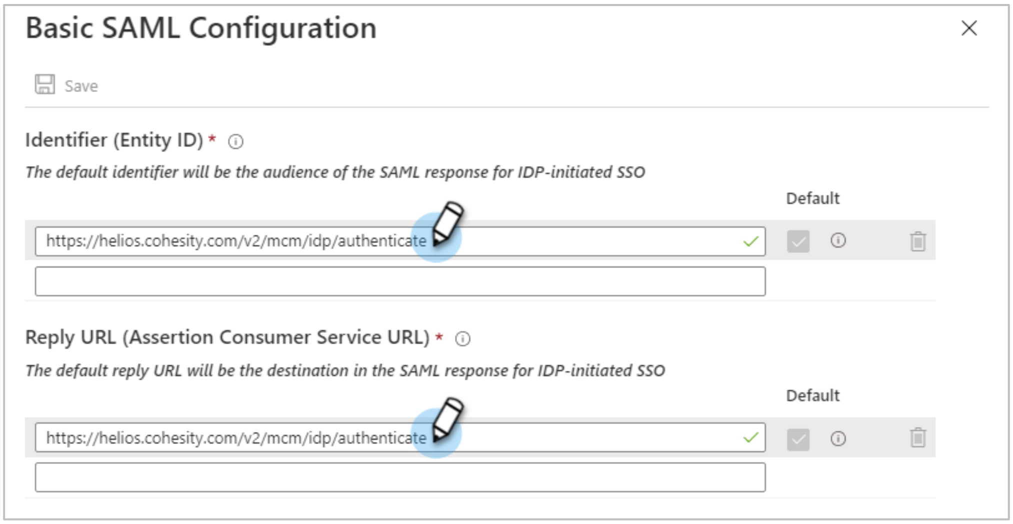
Linked
Link to an application in the Active Directory Access Pan
Office 365 application launc

8. Under **Basic SAML Configuration**, enter:

   a) **Identifier (Entity ID)**: `https://`***`<cluster_fqdn>`***`/idps/authenticate`.

   b) **Reply URL (Assertion Consumer Service URL)**: Use the same value as for **Identifier**.

> **TIP**: If you have multiple Cohesity clusters and you want to use this Azure AD application for all of them, you can use the additional cluster FQDNs to enter multiple **Identifiers** and **Reply URLs** in this step.



Basic SAML Configuration

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

https://helios.cohesity.com/v2/mcm/idp/authenticate

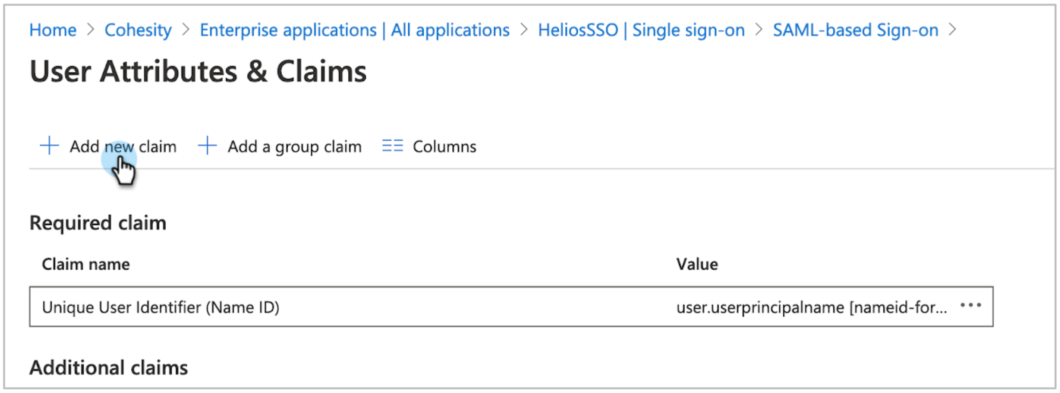
Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://helios.cohesity.com/v2/mcm/idp/authenticate

9. Under **User Attributes & Claims**, click **Add new claim**.



Home > Cohesity > Enterprise applications | All applications > HeliosSSO | Single sign-on > SAML-based Sign-on >

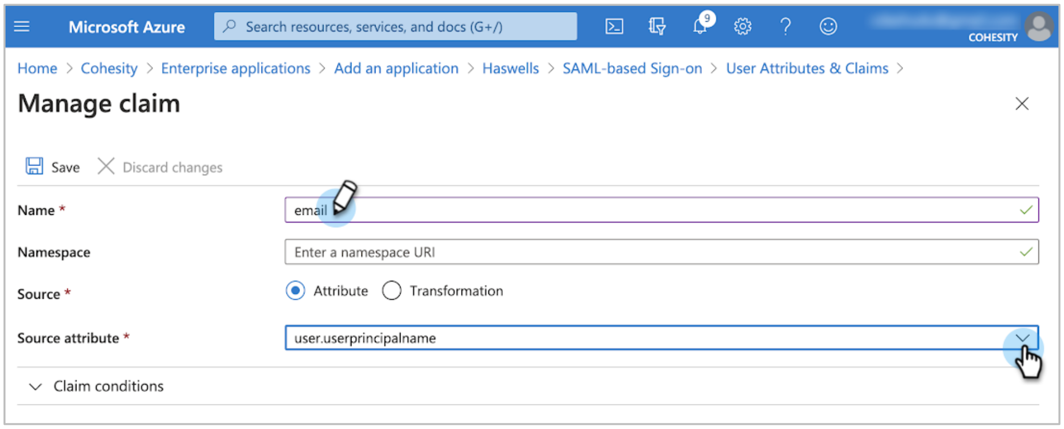
User Attributes & Claims

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ···

Additional claims

10. Enter a **Name** and select a **Source attribute**.



Home > Cohesity > Enterprise applications > Add an application > Haswells > SAML-based Sign-on > User Attributes & Claims >

Manage claim

Save Discard changes

Name *: email

Namespace: Enter a namespace URI

Source *: ● Attribute ○ Transformation

Source attribute *: user.userprincipalname

Claim conditions

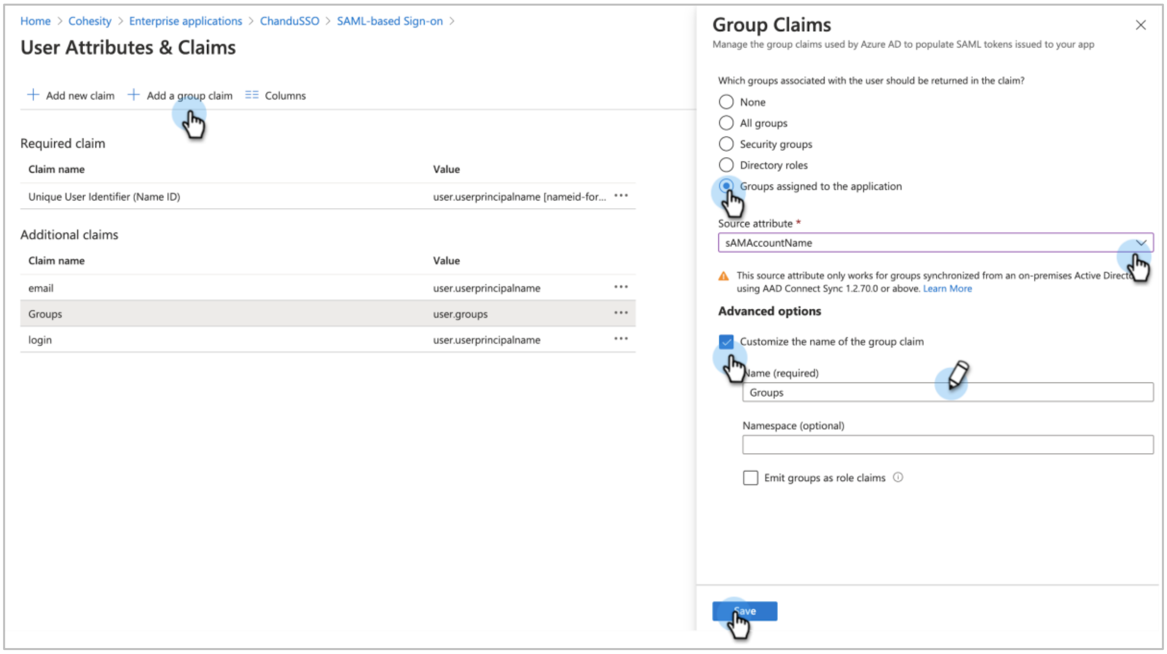
11. If you plan to use user groups-based RBAC, you need to pass the “Groups” SAML attribute to Cohesity. To do so:

    a) Under **User Attributes & Claims**, click **Add a group claim**.

    b) Select the groups that you want to send in the claim.

    c) Select the **Source attribute** that you want to send in the value.

    d) Under the **Advanced options**, check the **Customize the name of the group claim**, enter “Groups” under **Name,** and click **Save**.



Home > Cohesity > Enterprise applications > ChanduSSO > SAML-based Sign-on >

User Attributes & Claims

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...

Additional claims

Claim name	Value
email	user.userprincipalname
Groups	user.groups
login	user.userprincipalname

Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None
○ All groups
○ Security groups
○ Directory roles
● Groups assigned to the application

Source attribute *: sAMAccountName

This source attribute only works for groups synchronized from an on-premises Active Directo using AAD Connect Sync 1.2.70.0 or above. Learn More

Advanced options

☑ Customize the name of the group claim

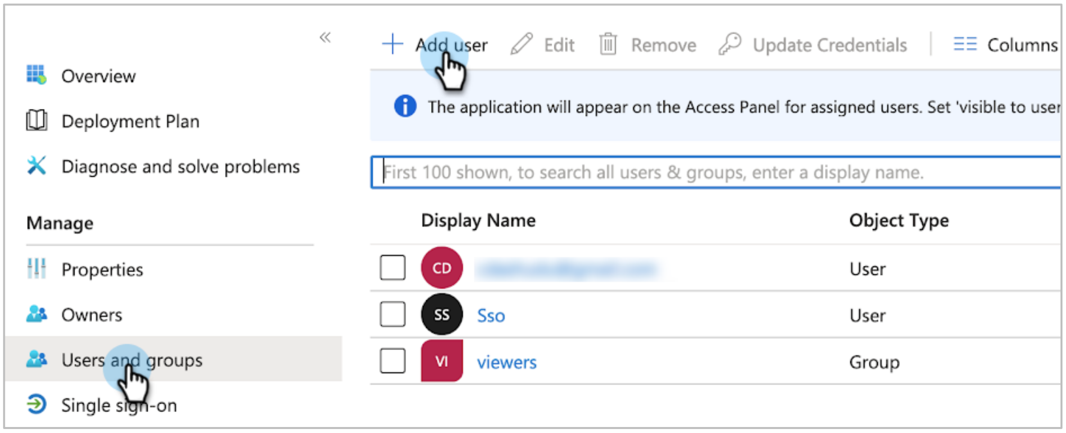
Name (required): Groups

Namespace (optional):

☐ Emit groups as role claims

NOTE: To use source attributes like **SAMAccountName** to pass the user group name in the “Groups” SAML attribute make sure that Azure AD groups are synchronized from an on-premises Active Directory using Azure AD Connect Sync 1.2.70.0 or above. For more information, see Azure AD Connect: Upgrade from a previous version to the latest in the Microsoft documentation.

12. Under **Users and groups**, click **Add user** to assign the users and/or groups who should be able to access Cohesity.



The application will appear on the Access Panel for assigned users. Set 'visible to user

First 100 shown, to search all users & groups, enter a display name.

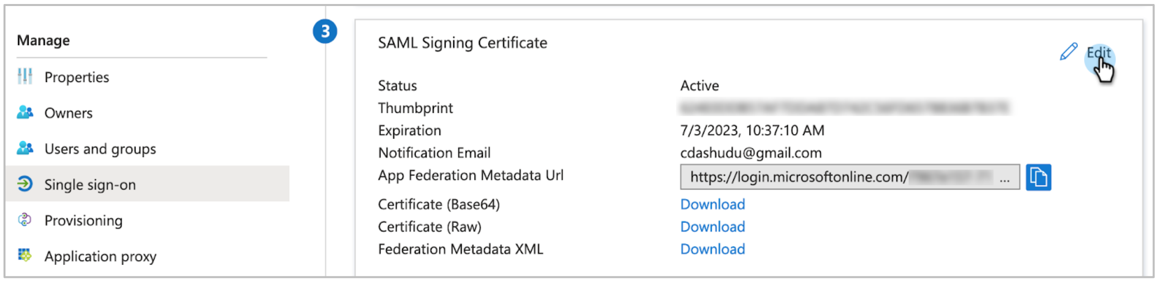
	Display Name	Object Type
□	CD [redacted]	User
□	SS Sso	User
□	VI viewers	Group

Collect SSO URL, Provider Issuer ID, and Certificate

Now, on the next page in the form, you'll need to retrieve Azure AD information to configure SSO on the 'service provider' (Cohesity) for the IdP (Azure AD).

To collect the SSO URL, Entity ID, and certificate from the Azure AD application:

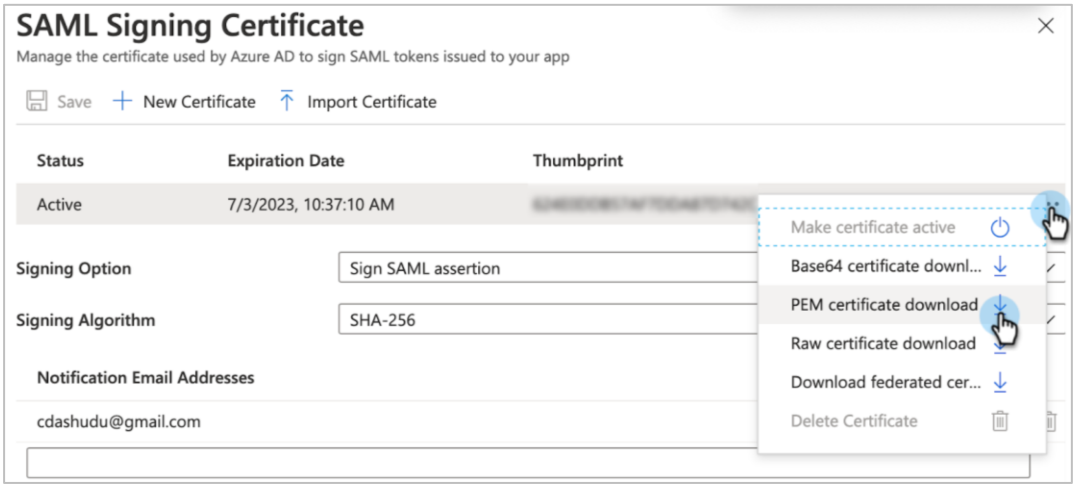
1. Log in to the Azure AD admin panel and navigate to **Azure Active Directory > Enterprise applications > *[your application]* > Single sign-on**.
2. Scroll down to **SAML Signing Certificate** and click **Edit**.



SAML Signing Certificate

Status	Active
Thumbprint	[redacted]
Expiration	7/3/2023, 10:37:10 AM
Notification Email	cdashudu@gmail.com
App Federation Metadata Url	https://login.microsoftonline.com/[redacted] ...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

3. Download the PEM certificate.



SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

Status	Expiration Date	Thumbprint
Active	7/3/2023, 10:37:10 AM	[redacted]

Signing Option: Sign SAML assertion

Signing Algorithm: SHA-256

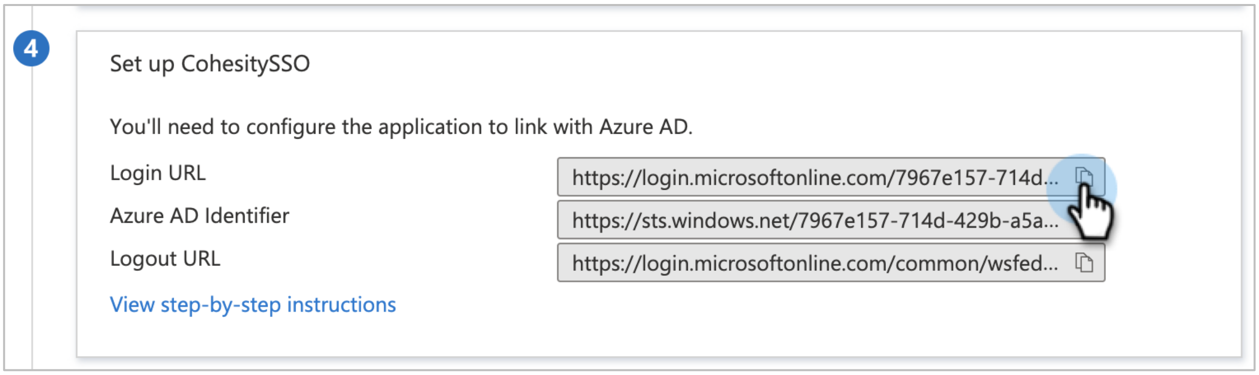
Notification Email Addresses

cdashudu@gmail.com

NOTE: Cohesity SSO only accepts `*.pem` format certificate.

To collect the URL for Cohesity Cluster,

1. Scroll down to **Set up CohesitySSO** and copy the **Login URL**. You will use the **Login URL** value to enter the Single Sign-On URL when you add Azure AD as an SSO provider to Cohesity in the next section.

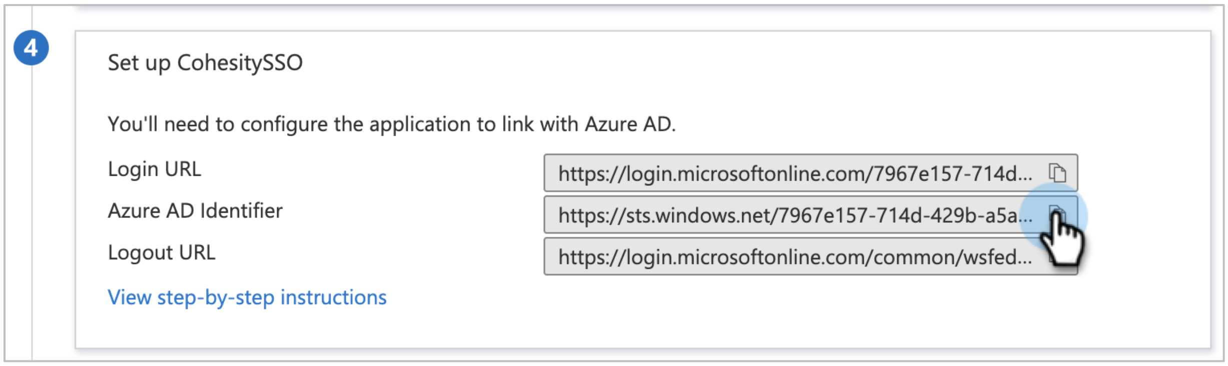


Set up CohesitySSO

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/7967e157-714d...
Azure AD Identifier	https://sts.windows.net/7967e157-714d-429b-a5a...
Logout URL	https://login.microsoftonline.com/common/wsfed...

2. Copy the **Azure AD Identifier**. You will use the Azure AD Identifier value to enter the Cohesity Provider Issuer ID when you add Azure AD as an SSO provider to Cohesity in the next section.



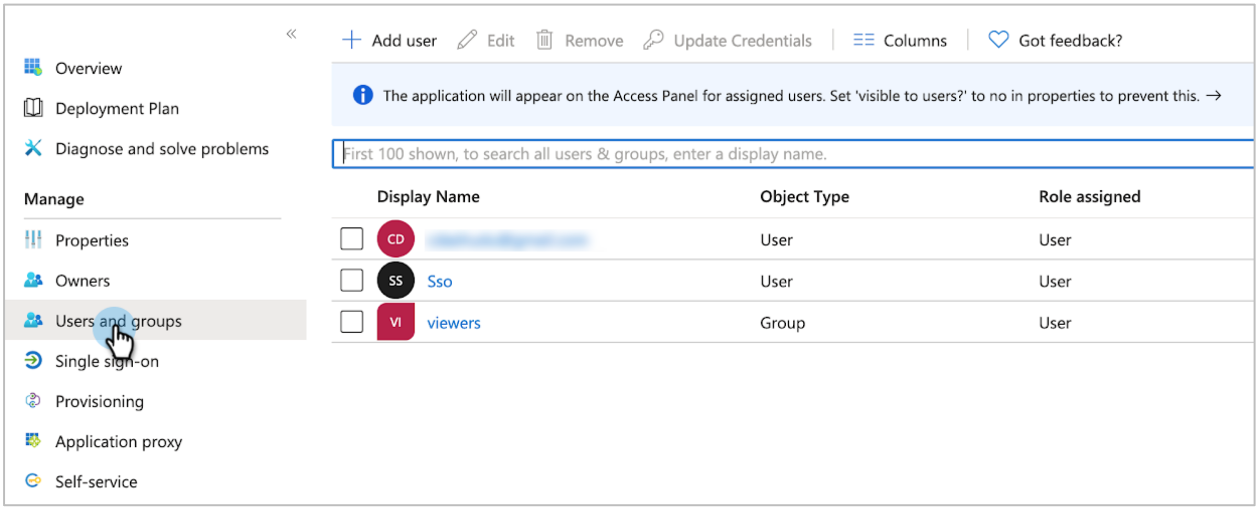
Set up CohesitySSO

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/7967e157-714d...
Azure AD Identifier	https://sts.windows.net/7967e157-714d-429b-a5a...
Logout URL	https://login.microsoftonline.com/common/wsfed...

View step-by-step instructions

3. Click **Users and groups** on the left to assign the users and/or groups who should be able to access Cohesity to your Azure AD application.



The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this. →

First 100 shown, to search all users & groups, enter a display name.

	Display Name	Object Type	Role assigned
□	CD [redacted]	User	User
□	SS Sso	User	User
□	VI viewers	Group	User

You now have the Azure AD details you'll need to configure it as your SSO provider in Cohesity in the next step.

Configure SSO Provider on Cohesity

Now that you have created your Azure AD application, use the SAML Signing Certificate and connection links to configure access management on Cohesity.

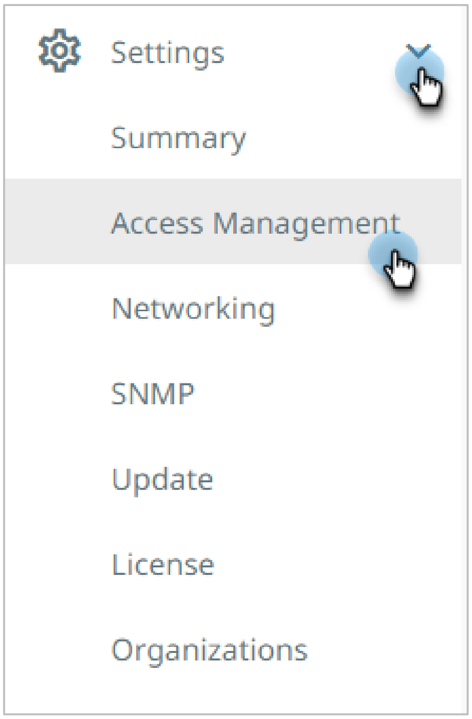
This is how you let Cohesity know where to send the user who is trying to sign in using the SSO option.

Add Azure AD as SSO Provider

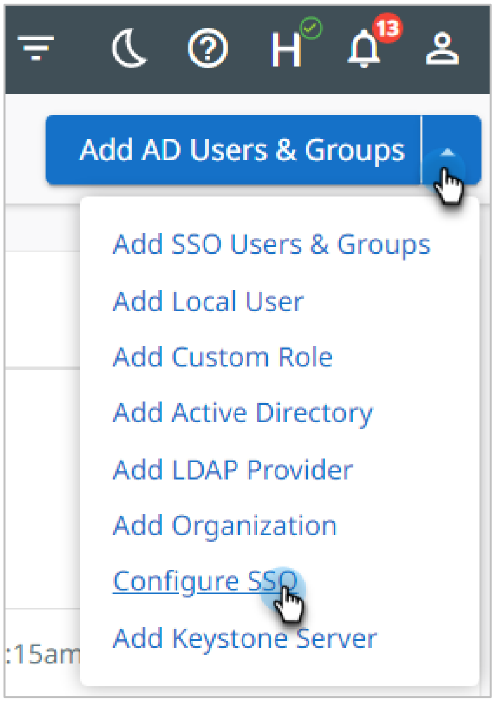
The first step is to use your Azure AD details to configure access management on Cohesity.

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**.



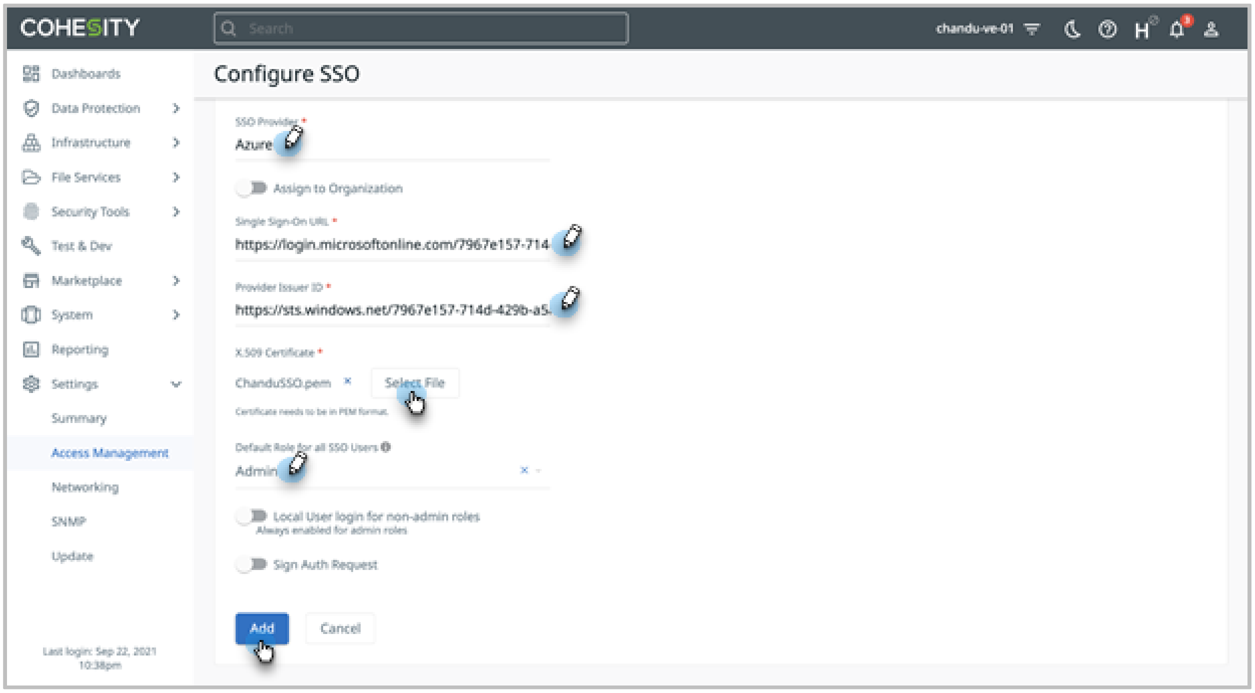
4. In the **Configure SSO** form, use the information you captured earlier to complete the following fields:
   a) **SSO Domain**. Enter **Azure AD**. (Note that this name should be unique among all SSO provider domain names.)
   b) **SSO Provider**. Enter **Azure AD**.

c) **Single Sign-On URL**. Enter the Login URL that you copied earlier for Cohesity Cluster.
   a. **Provider Issuer ID**. Enter the **Azure AD Identifier** that you copied earlier.

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

e) **Default Role for all SSO Users**. Choose a default role for any user who logs in using Azure AD. 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**.



Configure SSO

SSO Provider *
Azure

Assign to Organization

Single Sign-On URL *
https://login.microsoftonline.com/7967e157-714

Provider Issuer ID *
https://sts.windows.net/7967e157-714d-429b-a5

X.509 Certificate *
ChanduSSO.pem ×
Select File
Certificate needs to be in PEM format.

Default Role for all SSO Users
Admin

Local User login for non-admin roles
Always enabled for admin roles

Sign Auth Request

Add Cancel

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

Add SSO Users and Groups

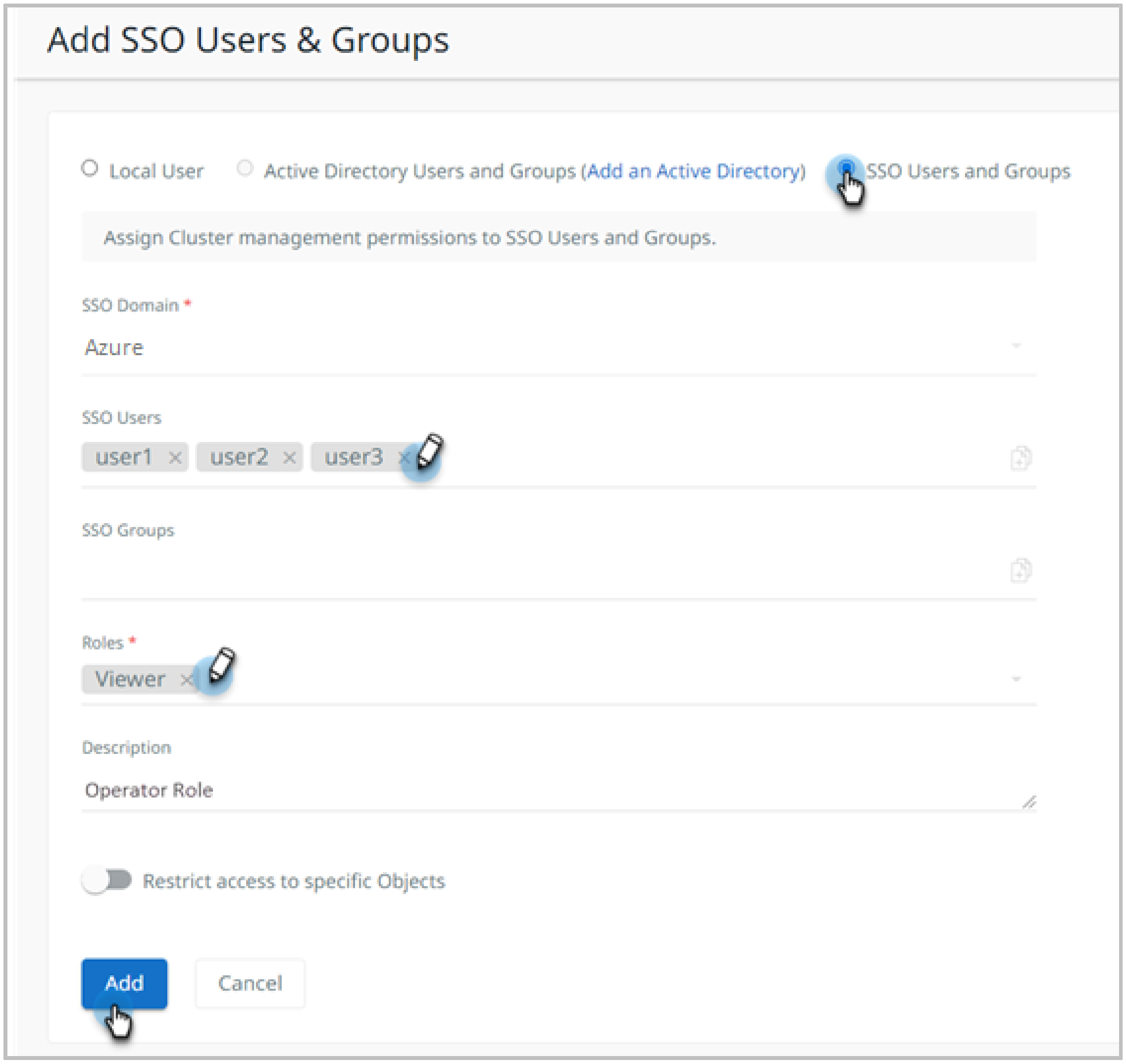
During the SSO setup step, you can optionally add a default role for all SSO users. This might not be desirable in all cases, and you might want to give different access rights to different users and/or groups. There are two ways of doing this. You can:

- 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**.



Add SSO Users & Groups

○ Local User ○ Active Directory Users and Groups (Add an Active Directory) ● SSO Users and Groups

Assign Cluster management permissions to SSO Users and Groups.

SSO Domain *: Azure

SSO Users: user1 × user2 × user3 ×

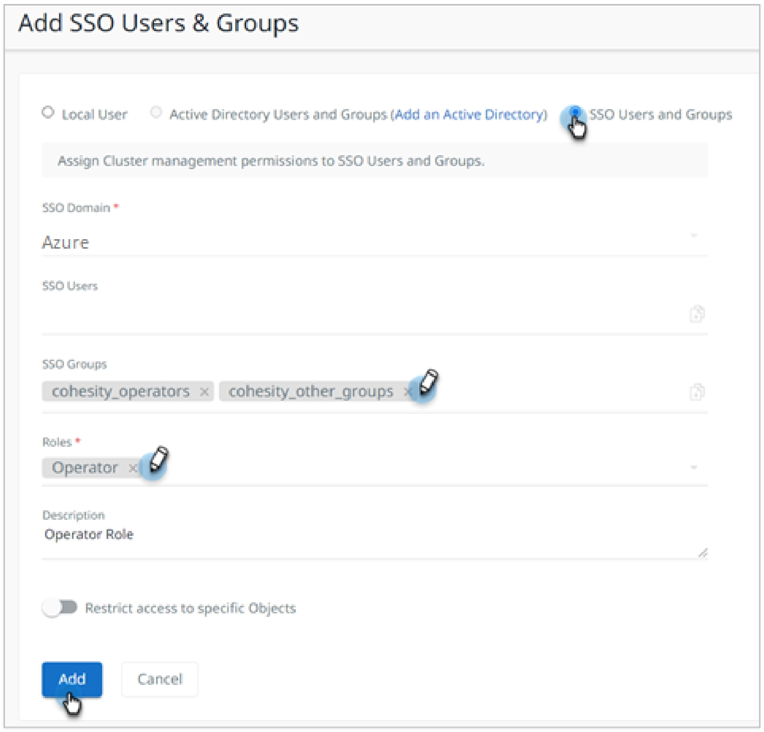
SSO Groups:

Roles *: Viewer ×

Description: Operator Role

Restrict access to specific Objects

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



Add SSO Users & Groups

○ Local User ○ Active Directory Users and Groups (Add an Active Directory) ● SSO Users and Groups

Assign Cluster management permissions to SSO Users and Groups.

SSO Domain *
Azure

SSO Users

SSO Groups
cohesity_operators × cohesity_other_groups ×

Roles *
Operator ×

Description
Operator Role

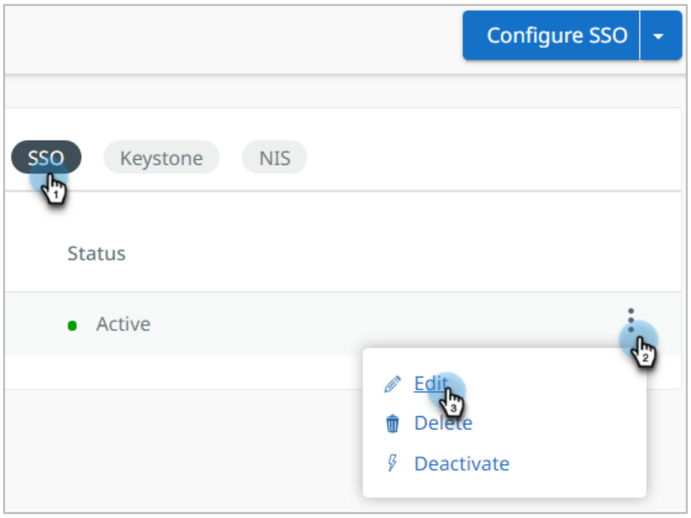
Restrict access to specific Objects

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 Azure Active Directory using the new information.

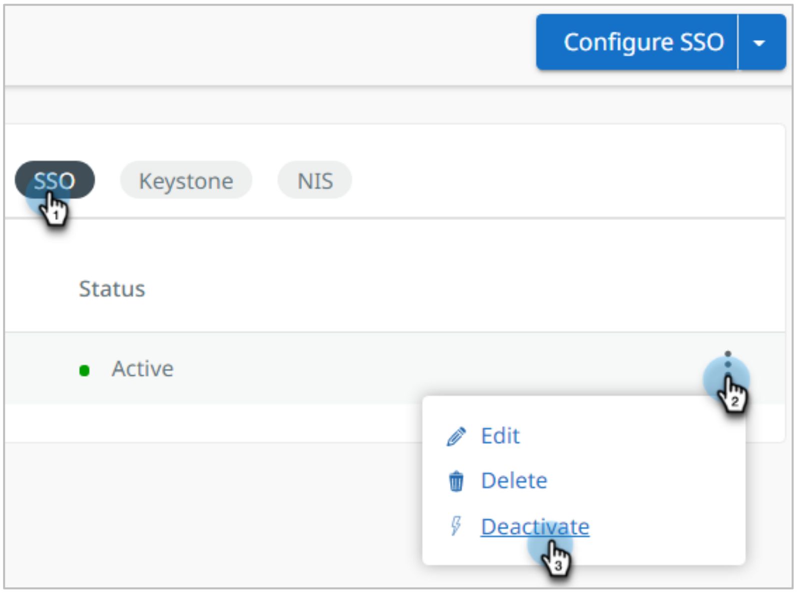
Deactivate SSO Provider

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 Azure AD provider will no longer bypass the Cohesity sign-in page.

To deactivate or activate an SSO provider:

1. Log in to Cohesity and, 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**.

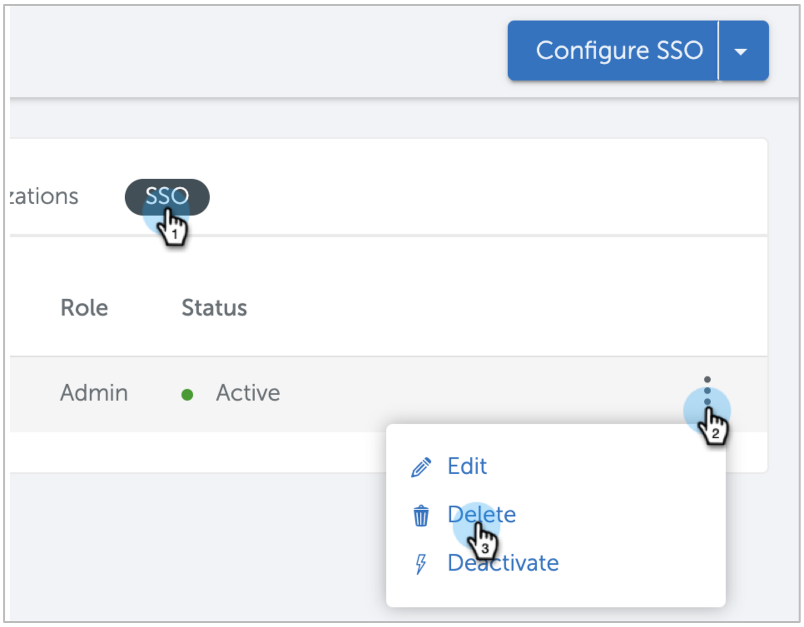


Delete SSO Provider

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

To delete an SSO provider:

1. Log in to Cohesity, select **Admin** > **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

Chandrashekar Dashudu is a Technical Marketing Engineer at Cohesity, focusing on API integrations and Apps.

Other essential contributors included:

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

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.0	June 2019	First release
2.0	Aug 2020	Major update
2.1	April 2021	Minor update
2.2	Sept 2021	Rebranding updates

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.