



Version 1.1

September 2021

Integration with Okta for Single Sign-On Capabilities

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

Single Sign-On (SSO) Benefits	3
Cohesity Offers Seamless SSO Support.....	4
Integrating with SSO Identity Providers	5
Configure Access Management with Okta on Cohesity	6
Prepare Required Information for Integration.....	6
Create Okta Application	7
Add Okta as SSO Provider on Cohesity	13
Add SSO Users and Groups.....	16
Manage Cohesity SSO Providers	18
<i>Edit SSO Provider</i>	18
<i>Deactivate SSO Provider</i>	19
<i>Delete SSO Provider</i>	20
Your Feedback	21
About the Authors.....	21
Document Version History.....	21

Figures

Figure 1: IdP Authenticates Cohesity User and Assigns Appropriate Cohesity Role	5
Figure 2: Access Management with Okta Lifecycle	6

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

Cohesity Offers Seamless SSO Support

You can configure Cohesity to use an Identity Provider (IdP) for enabling SSO access to your Cohesity cluster. For a multi-tenant cluster, you can configure SSO for each organization defined in Cohesity.

After the integration is configured, users can sign in to the Cohesity cluster by one of two paths, via the IdP or the Service Provider (SP), which is Cohesity in this case:

- **IdP-initiated login.** Click the application tile for your Cohesity cluster on the IdP sign-in page.
- **SP-initiated login.** Click the Sign in with SSO link at the bottom of the Cohesity login page.

When integrating with SSO providers, note these requirements. Cohesity currently:

- Supports SSO with solutions that support SAML (Security Assertion Markup Language) 2.0.
- Uses the **user.userType** attribute in SAML 2.0 SSO for user roles.

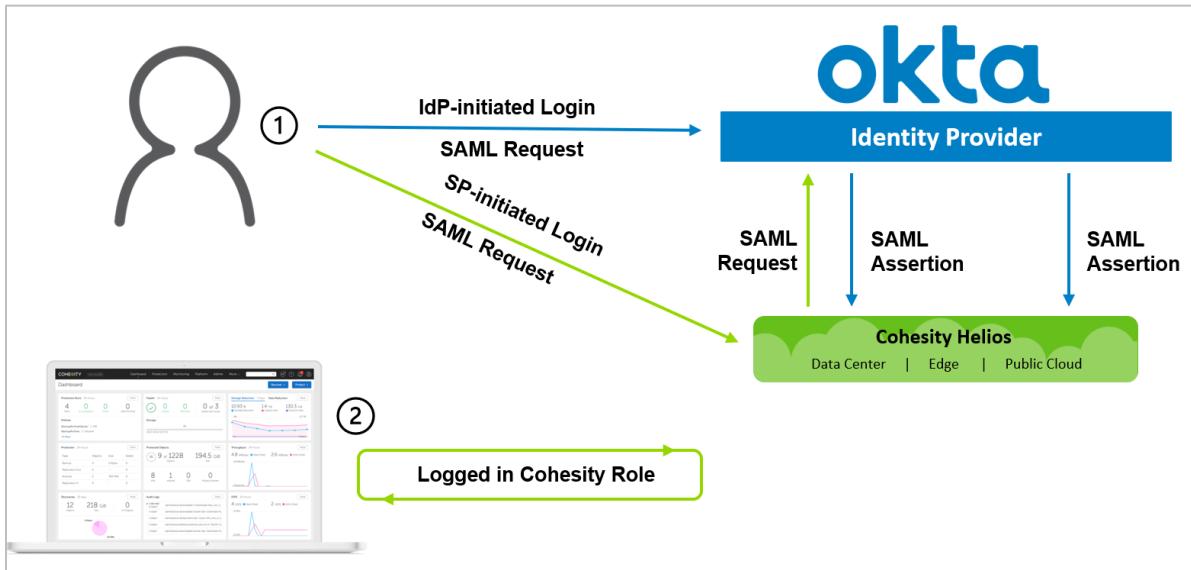
Integrating with SSO Identity Providers

To integrate with an IdP, users need to configure details on both the IdP and the SP, Cohesity. SSO support is delivered through the [Cohesity REST API](#), providing extensibility and reliability.

The authentication workflow starts with the IdP or the SP:

1. The user logs in:
 - **Via IdP:** The IdP, Okta, identifies and authenticates the user and sends a SAML 2.0 assertion to the SP, Cohesity.
 - **Via SP:** A user requests to log in to the SP, Cohesity, via SSO. The SAML 2.0 request is redirected to the IdP, Okta. Okta 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 1: IdP Authenticates Cohesity User and Assigns Appropriate Cohesity Role

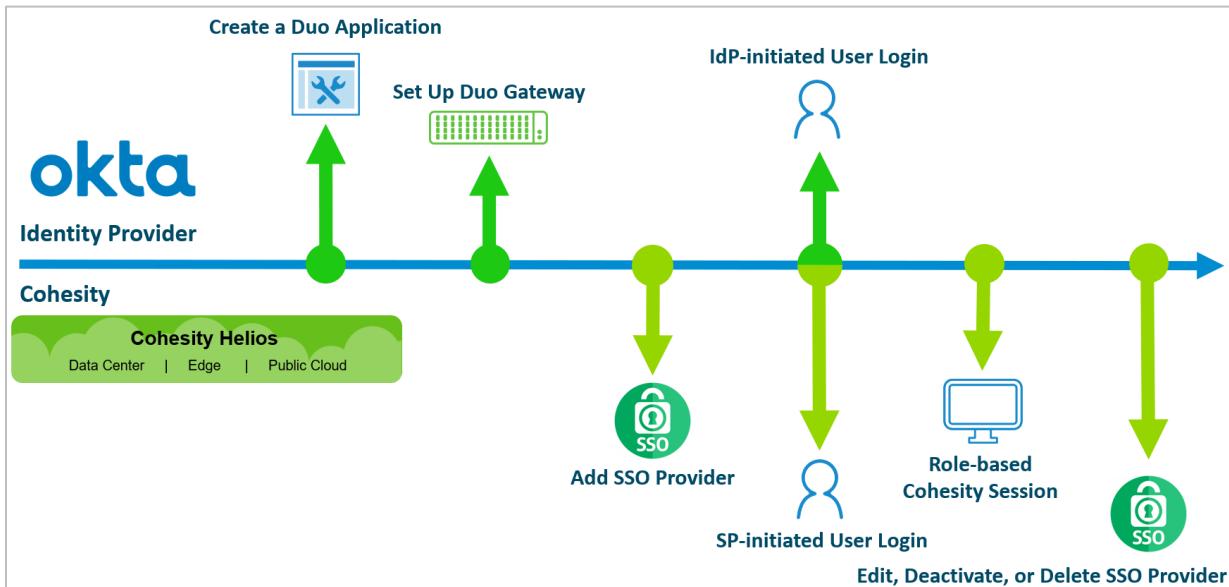


Configure Access Management with Okta on Cohesity

To configure and use Okta on Cohesity:

1. [Create Okta SSO application](#). Create Okta application for Cohesity.
2. [Assign users to your Okta application](#). Assigns users to the application in Okta.
3. [Add your SSO provider](#). Use your Okta details to configure access management on Cohesity.
4. Role-based Cohesity session. Users log in to Cohesity via Okta (*IdP-initiated*) or Cohesity SSO login (*SP-initiated*).
5. [Manage SSOs](#). Edit, deactivate, or delete your SSO provider.

Figure 2: Access Management with Okta Lifecycle



Prepare Required Information for Integration

Before you use Okta as your SSO provider for Cohesity, you will need to collect several pieces of information from each platform.

To [create the Okta application](#) that will integrate with Cohesity, you will need:

- **Single Sign-On URL.** The URL where SAML assertions are sent once a user is authenticated.

To [build the Single Sign-On URL in the SAML settings for your Okta app](#):

- **For Cohesity (on-prem):** Log in to Cohesity to get the cluster's FQDN and add '/idps/authenticate'. Use the format: `https://<cluster_fqdn>/idps/authenticate`.
- **For Cohesity Helios:** Use the URL:
`https://helios.cohesity.com/v2/mcm/idp/authenticate`.

- **Audience URI (SP Entity ID)**. Same as the above. Use this in your [Okta SAML configuration](#) to identify Cohesity as the SP that will use Okta as the IdP.
- **Attributes Mapping**. Maps the parameters sent by the IdP (Okta) to the service provider (Cohesity).

To [configure Cohesity to use Okta SSO](#), you will need the following from Okta:

- **Single Sign-On URL**. The URL where the user is redirected for authentication. Enter the value of the 'Identity Single Sign-On URL' field that [you copy from Okta](#).
- **Provider Issuer ID**. Identifies the Cohesity cluster sending the SAML request and enter the value of the 'Identity Provider Issuer' field that [you copy from Okta](#).
- **X.509 Certificate**. Verifies the SAML assertions received by the IdP, Okta. Upload the `okta.pem` file that you will [download](#) from Okta and [rename](#).

Now you're ready to start setting up Okta SSO for Cohesity, starting with creating an Okta app in the next section.

Create Okta Application

The first step is to create an application in your Okta account that connects to your Cohesity cluster.

To create an Okta application for Cohesity:

1. Log in to the Okta admin panel and go to **Applications** under **Applications**.

Preview Sandbox: This is a preview of next week's release. See a problem? [File a case](#) or visit our [support site](#).

okta

Search...

RRajaraman@cohesity.com Cohesity-dev-3325...

Dashboard

Directory

Applications (selected)

Self Service

Security

Workflow

Reports

Overview

Users 53 (last 7 days) Groups 16 (last 7 days) SSO Apps 28

Updated at 24 Sep, 07:25

Status

Okta service • Operational Agents No agents added

Tasks

Type ▾ Items ▾ Description

To-do 34 Application accounts need deprovisioning

Org changes

No org changes in last 7 days

Security Monitoring

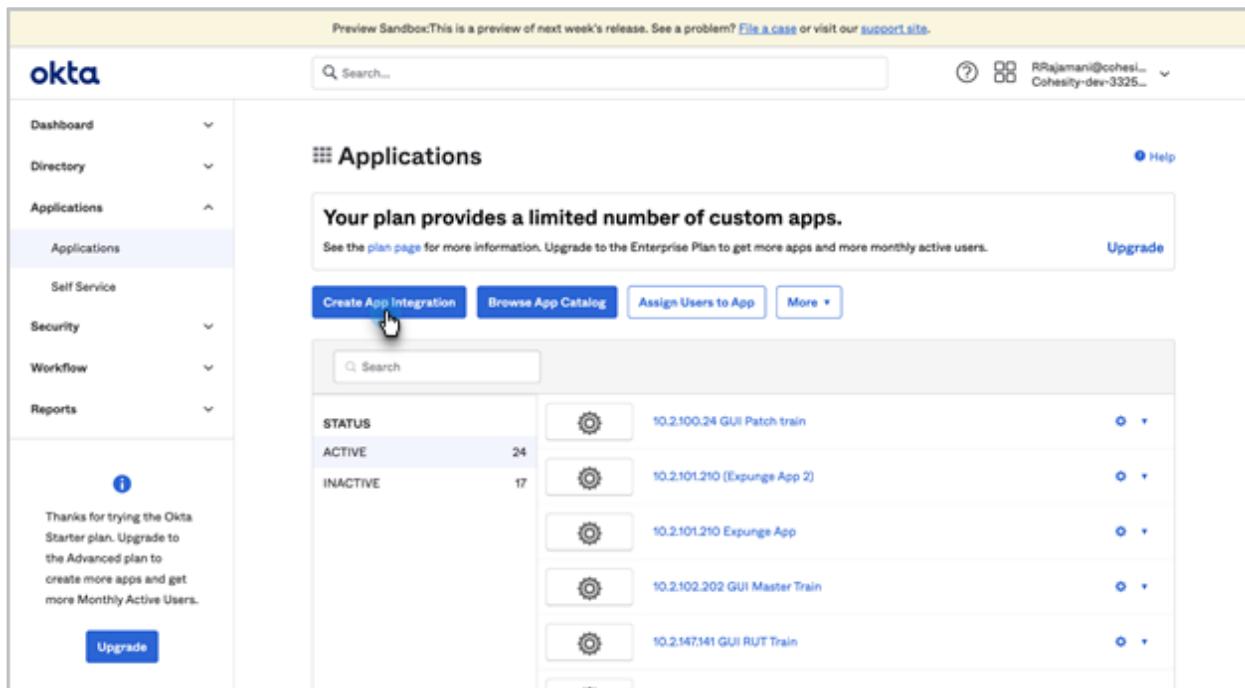
36% 5 of 14 tasks completed

View HealthInsight

Thanks for trying the Okta Starter plan. Upgrade to the Advanced plan to create more apps and get more Monthly Active Users.

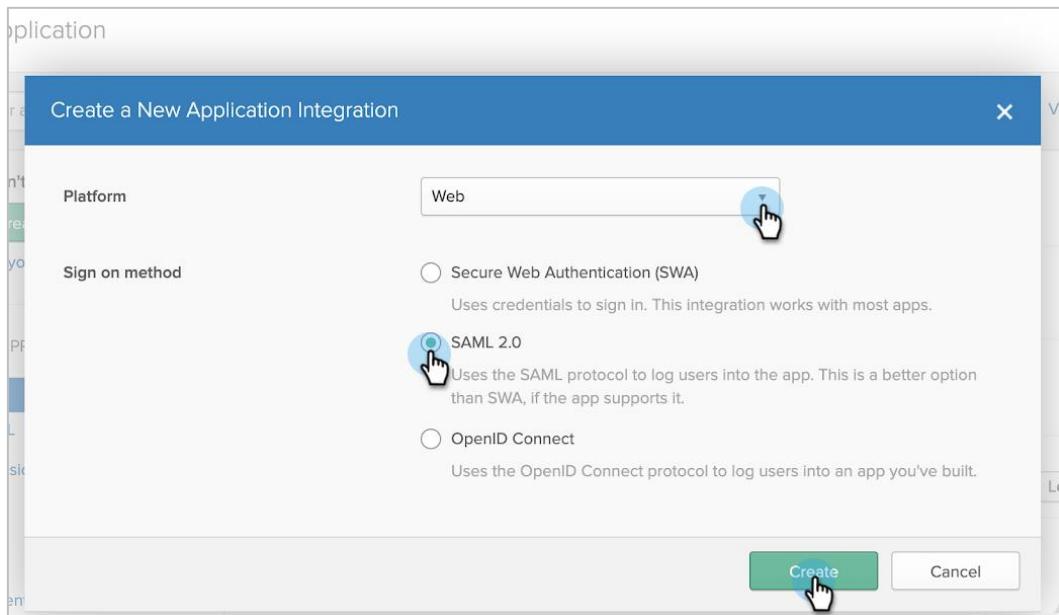
Upgrade

2. Click **Create App Integration**.



The screenshot shows the Okta Applications interface. On the left, there's a sidebar with navigation links: Dashboard, Directory, Applications (which is expanded), Applications, Self Service, Security, Workflow, and Reports. A message box on the left says: "Thanks for trying the Okta Starter plan. Upgrade to the Advanced plan to create more apps and get more Monthly Active Users." It has a blue "Upgrade" button. The main area is titled "Applications" and displays a message: "Your plan provides a limited number of custom apps. See the [plan page](#) for more information. Upgrade to the Enterprise Plan to get more apps and more monthly active users." Below this is a search bar and a row of buttons: "Create App Integration" (highlighted with a cursor), "Browse App Catalog", "Assign Users to App", and "More". The main table lists applications by status: ACTIVE (24) and INACTIVE (17). Each entry includes a gear icon, the application name, and a dropdown menu.

3. In the dialog that opens, under **Platform**, select **Web**. Under **Sign on method**, select **SAML 2.0**. Then click **Create**.



The screenshot shows the "Create a New Application Integration" dialog. At the top, it says "Create a New Application Integration". The "Platform" section has a dropdown menu set to "Web", with a cursor pointing at it. The "Sign on method" section contains three options: "Secure Web Authentication (SWA)" (unchecked), "SAML 2.0" (checked with a cursor pointing at it), and "OpenID Connect" (unchecked). Below each option is a brief description. At the bottom right are "Create" and "Cancel" buttons.

4. Enter **App name** (to display in the Cohesity cluster tile on the SSO page), upload an **App logo** (optional), and click **Next**.

The screenshot shows the Okta interface for creating a SAML integration. The top navigation bar includes 'Classic UI ▾', a search bar ('Search people, apps'), and tabs for 'Get Started', 'Dashboard', 'Directory', 'Applications', 'Security', 'Workflow', 'Reports', 'Settings', and 'Upgrade'. The main title is 'Create SAML Integration'. A progress bar at the top indicates three steps: 1 General Settings (selected), 2 Configure SAML, and 3 Advanced Options. The 'General Settings' step contains fields for 'App name' (set to 'CohesitySSO'), 'App logo (optional)' (a thumbnail of 'cohesity.png' is shown), and an 'Upload Logo' button with a cursor icon. Below these are two checkboxes for 'App visibility': 'Do not display application icon to users' and 'Do not display application icon in the Okta Mobile app'. At the bottom are 'Cancel' and 'Next' buttons, with the 'Next' button being highlighted by a cursor icon.

5. Configure your **SAML Settings** by entering:

- **Single sign on URL.** Add the Cohesity cluster FQDN or VIP address, followed by `/idps/authenticate`. For example: `https://<cluster_fqdn>/idps/authenticate`.

NOTE: To find the FQDN and VIP address, log in to Cohesity and select **Settings > Cluster > Networking > VIPs**.

For Cohesity Helios, use: `http://helios.cohesity.com/v2/mcm/idp/authenticate`.

- **Audience URI (SP Entity ID).** Use the same URL as above.
- **Application username.** Select your preference.

Create SAML Integration

SAML Settings

GENERAL

Single sign on URL:

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID):

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format:

Application username:

Update application username on:

Show Advanced Settings

- In the same form, under **ATTRIBUTE STATEMENTS**, map the **Email** and/or **Login** SAML attributes to the Okta user profile attributes. If the value is not available in the drop-down list, type it as shown in the table. You can map either or both attributes.

SAML ATTRIBUTE	OKTA USER PROFILE ATTRIBUTE VALUE
Email	user.email
Login	user.login

ATTRIBUTE STATEMENTS (OPTIONAL)

LEARN MORE

Name	Name format (optional)	Value
Email	Unspecified	user.email
Login	Unspecified	user.login

Add Another



7. Under **GROUP ATTRIBUTE STATEMENTS**, map the **groups** attribute to the Okta **Filter** attribute. (For example, select **Starts with** and enter **cohesity_** to pass any group name that starts with 'cohesity_' to Cohesity, which enables you to add it to the Cohesity cluster as an [SSO group](#) with specific access rights.) Then click **Next**.

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter
groups	Unspecified	Starts with cohesity

Add Another

B Preview the SAML assertion generated from the information above

< > Preview the SAML Assertion

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

Previous Cancel **Next**



8. Click **Finish** to add the application.

9. On your Okta application's **Sign On** tab, click **View Setup Instructions**.

The screenshot shows the Okta application configuration interface. The top navigation bar has tabs: General, Sign On (which is highlighted with a blue background and a mouse cursor), Mobile, Import, and Assignments. Below the tabs is a 'Settings' section with an 'Edit' button. The main content area is titled 'SIGN ON METHODS'. It says, 'The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.' Below this, it says, 'Application username is determined by the user profile mapping. [Configure profile mapping](#)'. A radio button is selected for 'SAML 2.0'. Underneath is a 'Default Relay State' section. A yellow callout box points to a message: 'SAML 2.0 is not configured until you complete the setup instructions.' At the bottom of this section is a button labeled 'View Setup Instructions' with a mouse cursor hovering over it.

10. Copy and keep the **Identity Provider Single Sign-On URL** and the **Identity Provider Issuer URL**, and click **Download certificate** to save the *okta.cert* file.

The screenshot shows the Okta application configuration interface. The top navigation bar has tabs: General, Sign On (highlighted with a blue background and a mouse cursor), Mobile, Import, and Assignments. Below the tabs is a 'Settings' section with an 'Edit' button. The main content area is titled 'SIGN ON METHODS'. It says, 'The following is needed to configure CohesitySSO'. Step 1: 'Identity Provider Single Sign-On URL:' shows a URL: 'https://[REDACTED].oktapreview.com/app/[REDACTED]/sso/saml'. A mouse cursor with a 'right-click' annotation is positioned over the URL. Step 2: 'Identity Provider Issuer:' shows a URL: 'http://www.okta.com/[REDACTED]'. A mouse cursor with a 'right-click' annotation is positioned over the URL. Step 3: 'X.509 Certificate:' shows a large block of redacted certificate text starting with '-----BEGIN CERTIFICATE-----' and ending with '-----END CERTIFICATE-----'. At the bottom of this section is a 'Download certificate' button with a mouse cursor hovering over it.

11. Rename the downloaded `okta.cert` file to `okta.pem`. You'll upload this file to the cluster later.
12. Click **Assign > Assign to People** to assign users to your Cohesity Okta application. Click **Assign > Assign to Groups** to assign groups to the app. (You'll assign roles to those users and groups in Cohesity later.)

The screenshot shows the Okta application management interface. At the top, there's a navigation bar with 'Classic UI ▾', a search bar ('Search people, apps'), and tabs for 'Dashboard', 'Directory', 'Applications', 'Security', 'Workflow', 'Reports', 'Settings', and 'Upgrade'. Below the navigation is a card for the 'CohesitySSO' application, which is listed as 'Active'. There's a note: 'Once you have a working SAML integration, submit it for Okta review to publish in the OAN.' Below the card, there are tabs for 'General', 'Sign On', 'Mobile', 'Import', and 'Assignments'. The 'Assignments' tab is selected and highlighted with a green underline. Under this tab, there's a section with a 'Assign' dropdown menu. The 'Assign to Groups' option is highlighted with a blue callout and a hand cursor icon, indicating it's the target of the next step. To the right, there's a sidebar labeled 'SELF' with some truncated text: 'Yo for yo ap Go'.

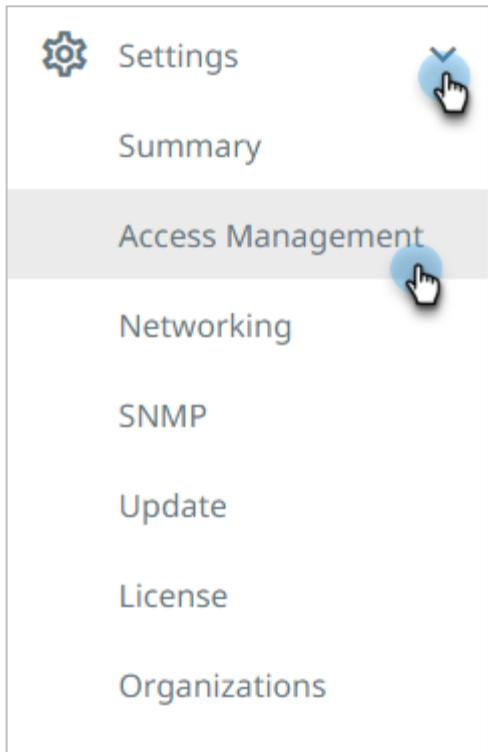
Now that you have the Okta application for Cohesity, you're ready to add it to your Cohesity cluster, as described next.

Add Okta as SSO Provider on Cohesity

Now that you have created the Cohesity Okta application, use your Okta details to configure access management on Cohesity.

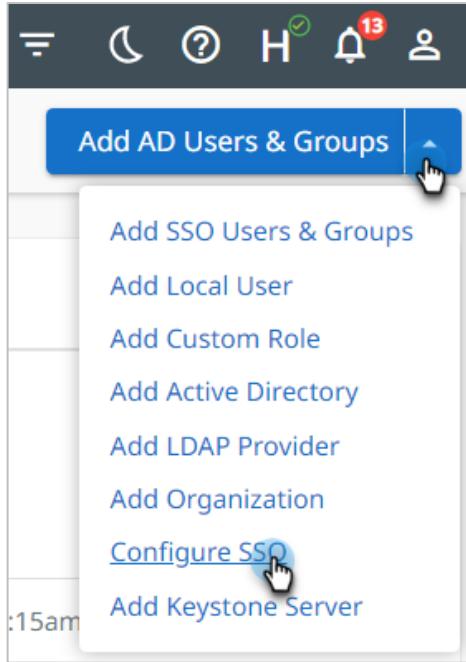
1. Log in to Cohesity as an administrator.

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



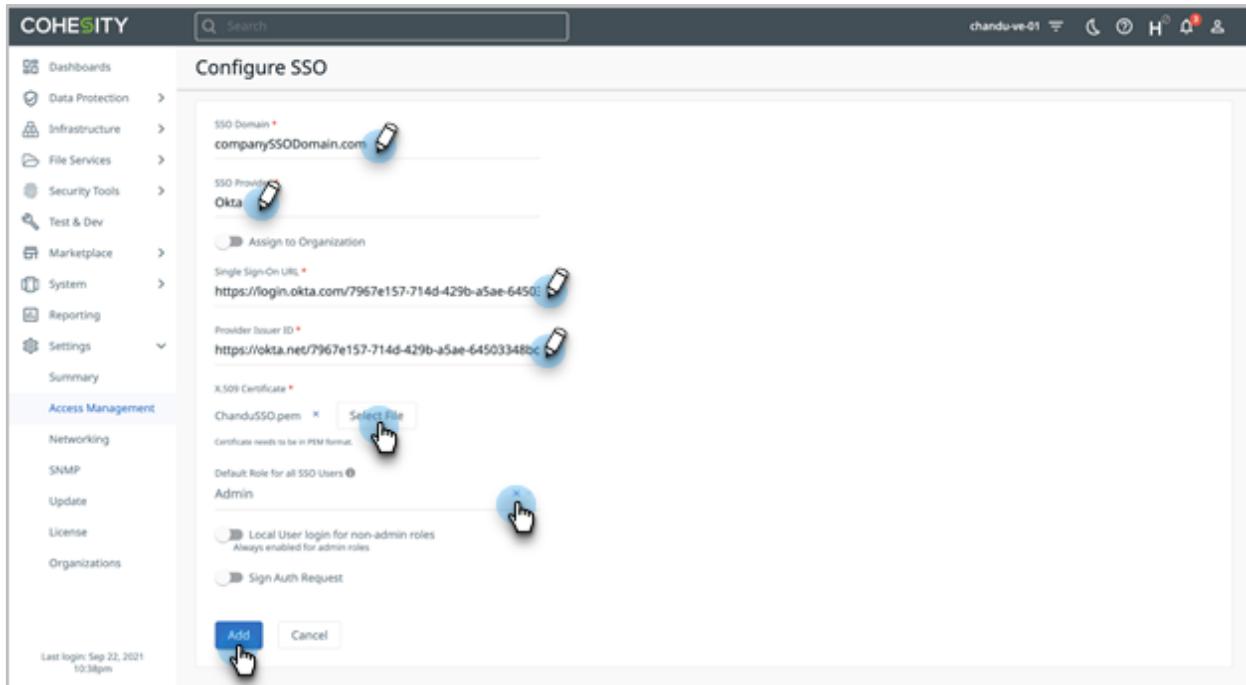
3. In the **Access Management** page, select **Add AD Users & Groups > Configure SSO**.

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 **Okta**. (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). 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 **Okta**.
 - c) **Single Sign-On URL.** Enter the **Identity Single Sign-On URL** that you copied from Okta earlier.
 - d) **Provider Issuer ID.** Enter the **Identity Provider Issuer** that you copied from Okta earlier.
 - e) **X.509 Certificate.** Click **Select File** and browse to select the `okta.pem` file that you downloaded and renamed 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.

NOTE: In Helios the SSO form is a dialog, but the fields are the same.



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

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 **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**.

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 *

Okta

SSO Users

[user1](#) [user2](#) [user3](#)

SSO Groups

Roles *

[Viewer](#)

Description

Operator Role

Restrict access to specific Objects

Add  **Cancel**

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

The screenshot shows the 'Add SSO Users & Groups' dialog box. At the top, there are three radio buttons: 'Local User', 'Active Directory Users and Groups (Add an Active Directory)', and 'SSO Users and Groups'. The 'SSO Users and Groups' option is selected and highlighted with a blue circle and a cursor. Below this, a note says 'Assign Cluster management permissions to SSO Users and Groups.' A dropdown menu for 'SSO Domain' is set to 'Okta'. Under 'SSO Users', there is a list box with a single entry 'SSO Groups'. Inside this list box are two entries: 'cohesity_operators' and 'cohesity_other_groups', each with a delete icon. Below the list box is a 'Roles' section with a dropdown menu containing 'Operator' and a delete icon. A 'Description' field is set to 'Operator Role'. A checkbox for 'Restrict access to specific Objects' is unchecked. At the bottom are 'Add' and 'Cancel' buttons, with 'Add' being highlighted by a mouse cursor.

Manage Cohesity SSO Providers

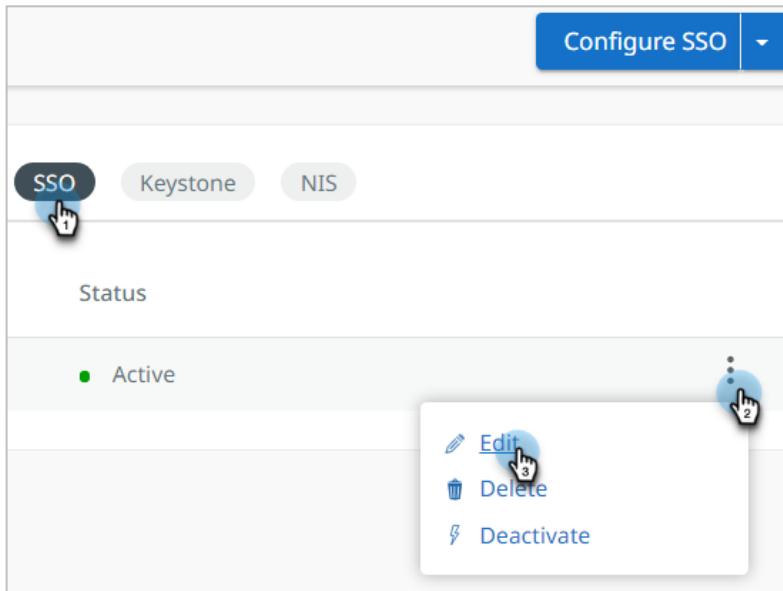
Once you've [added an SSO provider](#) to Cohesity, you can edit, delete, or deactivate it.

Edit SSO Provider

To edit SSO provider:

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

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



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

Cohesity validates the connection to Okta using the new information.

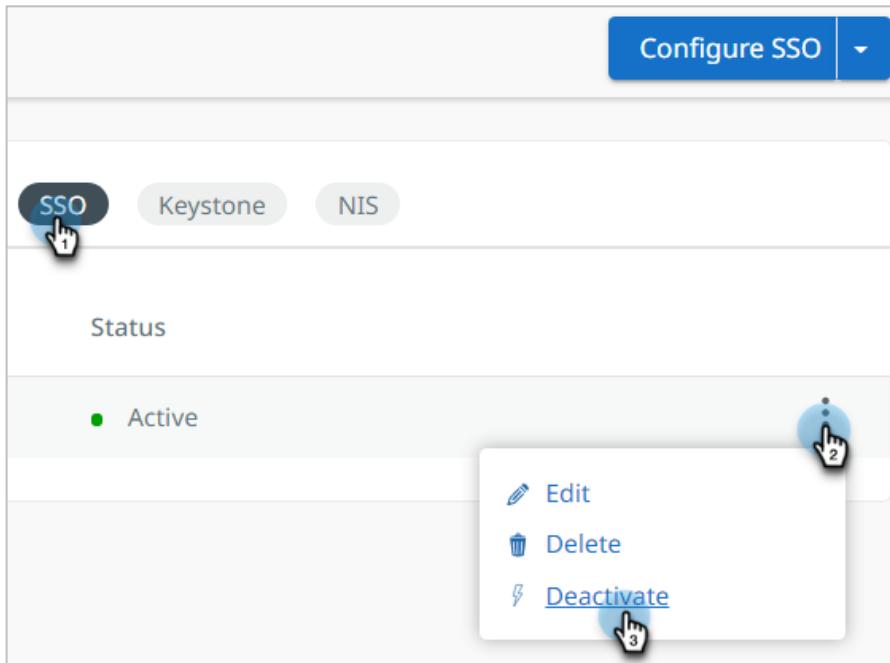
Deactivate SSO Provider

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 Okta 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 click **Deactivate** or **Activate**.

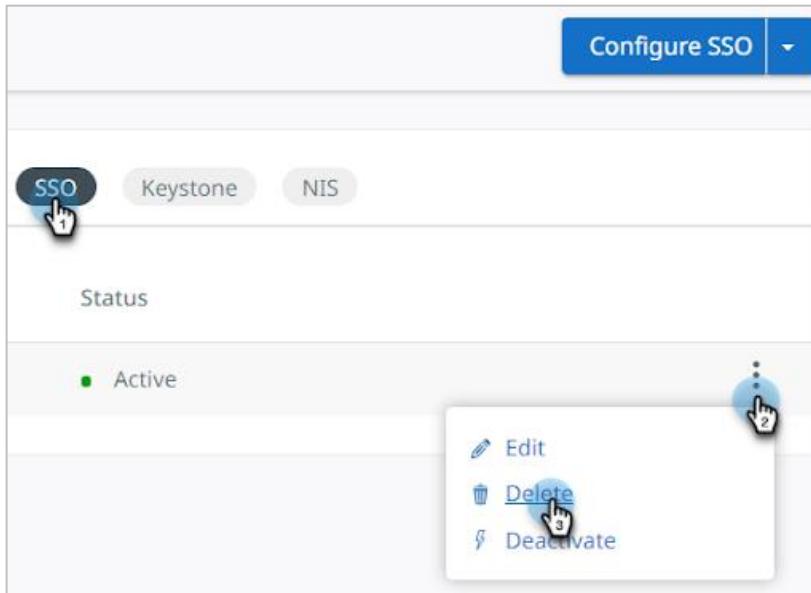


Delete SSO Provider

You can permanently delete an SSO provider if you no longer need it. Once deleted, users associated with the Okta 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 click **Delete**.



Your Feedback

Was this document helpful? [Send us your feedback!](#)

About the Authors

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

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.0	July 2020	First release
1.1	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](#).

© 2021. Cohesity, Inc. All Rights Reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

2000032-002-EN