COHESITY

Cohesity Gaia Security Whitepaper

Version 1.2

November 2025

ABSTRACT

*Cohesity Gaia is a **secure enterprise-grade RAG AI solution** that makes generative AI safe for business-critical data. Gaia gives insights into the enterprise data already protected by Cohesity — with no extra copies, no new silos. Security, governance, and compliance are embedded at every layer, ensuring enterprises can adopt AI confidently. This document outlines Gaia's security architecture and the controls that make it a **trusted, enterprise-ready foundation for unlocking insights with generative AI** in a **secure** way.*

Table of Contents

Figures

About Cohesity Gaia

Cohesity Gaia is an **enterprise-grade RAG (Retrieval Augmented Generation) AI Solution** that brings generative AI **securely** to the data already protected in Cohesity Data Cloud. Security, governance, and compliance are foundational to Gaia's design, making it safe for enterprises to adopt AI at scale.

The goal of Gaia is to help organizations unlock **actionable insights from stored data** — spanning SaaS, and on-premises workloads — without creating new data silos or pipelines. By applying advanced RAG techniques directly on enterprise data, Gaia empowers users to make **smarter, faster decisions** based on high-quality, trusted information.

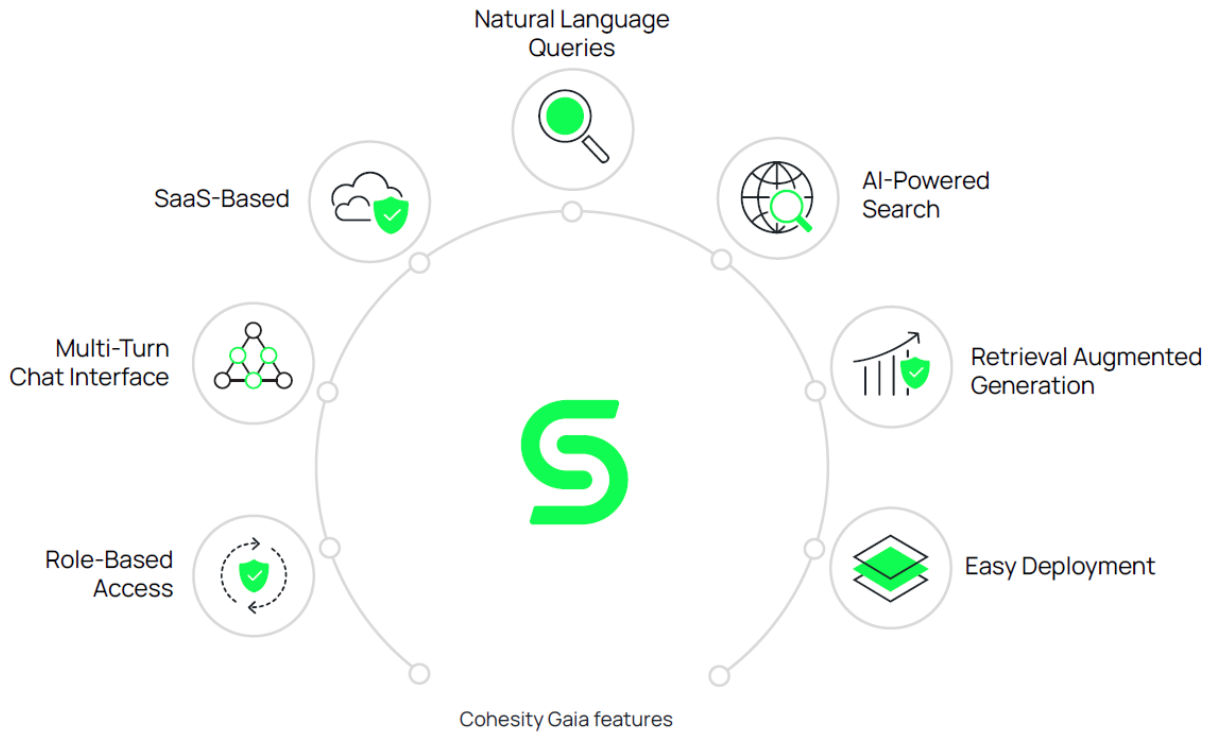
Unlike generic AI solutions, Gaia works directly on Cohesity-protected data, eliminating the need for replication or risky shadow pipelines. This ensures **AI adoption is secure, governed, and enterprise-ready from day one**.

Gaia is part of Cohesity's **AI-powered data security and management portfolio**, which protects the world's most critical workloads and provides a unified platform to secure and manage data across on-premises, cloud, and SaaS environments.

This document outlines Gaia's **security posture and enterprise controls** that enable safe adoption of generative AI in regulated, large-scale environments.

The figure below illustrates the key capabilities of Cohesity Gaia:

Figure 1: Cohesity Gaia Features



Security Challenges of Generative AI Applications

Security is a top priority for enterprises, and providing access to and securing the data becomes critical. Generative AI Applications, while powerful and innovative, present a range of security challenges and concerns. A recent Malwarebytes survey revealed that 81% of respondents are concerned about the security concerns of Generative AI applications. Below are some of the security challenges of generative AI Applications, and we will look at how Cohesity Gaia addresses these.

1. Data Privacy and Confidentiality
2. Unauthorized Access
3. Compliance and Regulatory Risks

Security by Design: User-Driven Configurations and Platform-Integrated Protections

This Security Whitepaper is organized into two main sections. The first part delves into the built-in security mechanisms inherent to the Cohesity platform, which work automatically to safeguard data stored within it. These foundational security features ensure that your data remains protected, providing an essential baseline of security.

The second part, we will explore how users can actively secure their data by configuring a variety of security measures available on the Cohesity platform. This section highlights the various security options that empower users to strengthen their data protection based on their unique needs.

Cohesity Gaia Architecture

Figure 2: Cohesity Gaia Architecture

Cohesity Gaia offers a comprehensive solution that caters to the unique requirements of enterprises. Our data security and management platform, the Cohesity Data Cloud, provides the necessary tools to handle diverse data types, ensure data consistency, and maintain a high level of security while enabling powerful analytics capabilities.

Cohesity Gaia's architecture consists of a control plane (Gaia-CP) and a data plane (Gaia-DP) that work together to manage and process enterprise data. The control plane is responsible for orchestrating various workflows, managing data models, and providing APIs for user interactions. The data plane is responsible for accessing data stored in the Cohesity cluster. Cohesity Gaia vectorizes the data for which dataset creation is requested, which creates embeddings in a Cohesity-managed container service.

High Level Application Flow

1. User interacts with the Cohesity Gaia application, providing a query or a request.
2. The Cohesity Gaia Embeddings Service, together with the Cohesity Gaia data service, retrieves relevant data by matching embeddings and documents based on the user's query.
3. The user's query and context is forwarded to the LLM.
4. The LLM generates an answer or response based on the user's query and context and provides it to the user through the Cohesity Gaia application.

Secure Data Management

Inspired by web-scale principles, the security-first architecture at Cohesity, combined with secure software development and release practices, ensures enterprise-class security. Here are the built-in security mechanisms of the Cohesity platform, securing your data stored on Cohesity.

Encryption and Key Management

Cohesity Gaia employs state-of-the-art encryption methods, using AES-256 encryption to secure all data, both in-transit and at-rest. The encryption keys are managed by a robust key management system (KMS), which provides secure storage, management, and distribution of cryptographic keys. The KMS is designed to handle key lifecycle events, such as key rotation and key revocation, ensuring that data remains protected even as encryption technologies evolve.

Secure communication

Cohesity Gaia prioritizes data security during transit by utilizing modern encryption methods, such as mutual Transport Layer Security (mTLS) and HTTPS. These secure communication channels ensure that data remains confidential and protected while being transmitted between components and services within the Cohesity Gaia system. Additionally, Cohesity Gaia's communication infrastructure is designed to support regular security updates and patches, maintaining a high level of protection against potential vulnerabilities.

Fine-grained RBAC Policies

Cohesity Gaia incorporates advanced, fine-grained RBAC policies that precisely govern access to the Gaia APIs. These specialized policies ensure that only authorized users can access and manage the stored data, effectively mitigating the risk of data exposure or unauthorized access. The RBAC system is designed to accommodate various levels of access and privileges, offering granular control over user permissions and actions within the Cohesity Gaia environment. Only Authenticated and Authorized users who has access to a particular dataset, will be able to interact with a given dataset.

Identity and access management (IAM)

Cohesity Gaia implements a sophisticated IAM framework to manage user access, authentication, and authorization. This comprehensive system includes support for RBAC, single sign-on (SSO), and multifactor authentication (MFA) mechanisms. By leveraging these advanced IAM tools, Cohesity Gaia ensures secure access to stored data while offering seamless integration with enterprise identity management solutions.

Policy-Driven Data Scoping

Gaia Admins can include/exclude files, folders, or data types to ensure compliance and data integrity is met.

Multi-Tenancy for Tenant Isolation

The Cohesity-managed Data Service is a highly scalable multi-tenant service wherein each tenant (Customer Helios Account) is logically isolated from other tenants, via the implementation of Cohesity Organization in Data Cloud Data Service hosted on Cohesity-managed cloud accounts. Cohesity organizations are logically segregated via an Organization ID that uniquely identifies all the Tenant's resources. Resources, such as cloud vaults, data, datasets, policies, users, etc. are restricted to the Organization to which they belong.

VectorDB Storage and access

A vector database is used by Cohesity Gaia to store generated text embeddings for a dataset. It resides on a Cohesity-managed container service. Access to the vector database is controlled and monitored, ensuring data confidentiality and integrity.

Immutable Backups

- Cohesity backup snapshots are immutable and at no point are they exposed to any external clients. Only the backup service running on Cohesity can write to the file system by means of authenticated APIs.
- All read/write operations to internal Views are sandboxed. For restore operations, the internal View is cloned and presented as a drive (IVM) or share (SMB, NFS, etc.) to the source.
- Backup and restore communications are secure.
- Cohesity Gaia retrieves various data sources and formats securely.

Secure API Access

Cohesity Gaia ensures secure API access by implementing robust authentication and authorization protocols, data encryption, and validating inputs to keep the communication secure. Users can interact with Cohesity Gaia APIs through SSO using OpenID Connect. This involves obtaining an access token from the identity provider and including it in the authorization header of API requests.

Cohesity allows you to interact via Cohesity Gaia APIs, making it Simple, Scalable, Flexible, and Secure. The Cohesity Gaia APIs allow you to seamlessly integrate with your applications.

Security Management

Cohesity implements an Information Security Management System (ISMS) that establishes policies and controls designed to meet the security objectives of our organization. Our ISMS aligns with ISO 27001 and the NIST CyberSecurity Framework to protect the organization, its personnel, and information assets.

- Policies are reviewed at least on an annual basis by the Information Security Committee and updated as appropriate.
- Annual information security training is required for all employees.

Background checks are performed on new Cohesity employees who are also required to review and acknowledge their receipt of relevant policies.

Compliance and Certifications

Cohesity is committed to following industry standards and best practices for data security, including relevant regulations and certifications. By aligning with these standards, Cohesity Gaia is designed to provide a secure and reliable data management solution for enterprises, allowing them to confidently store and process sensitive information while maintaining regulatory compliance. Furthermore, Cohesity as a company regularly undergoes regular audits and assessments to validate its security posture, demonstrating an ongoing commitment to maintaining the highest levels of data protection.

Cohesity recognizes the criticality of complying with standards and protecting the confidentiality, integrity, and availability of information assets. Cohesity maintains the following third-party assessments and assurances to validate the security posture of our products and services against industry standards.

- ISO 27001:2022.
- SOC 2 Type II.
- Cohesity holds a FIPS 140-2 Level 1 validation (AES 256-bit encryption).
- Cohesity performs regular penetration tests by qualified third-party assessors.

Secure Software Development Life Cycle

Cohesity embeds security into every phase of the software development life cycle. The secure development lifecycle at Cohesity delivers secure products to customers and eliminates any security vulnerabilities throughout the product life cycle. To deliver on this goal, Cohesity practices:

- Security Training
- Security in Design
- Threat Model in Architecture
- Vulnerability Management
- Vulnerability Management Policy
- Penetration Testing
- Static Code and Binary Analysis
- Dynamic Scanning
- Third-party Component Security
- Support for Product Infrastructure and Tools
- Secure Product Release
- Product Incident Response

Securing Your Data

Cohesity takes the security of our customers' data very seriously. Cohesity has designed, developed, and operated all the product offerings with security as a core tenet guiding our approach. What's more, the architecture is modular, enabling a fast, scalable solution while remaining secure, available, and flexible. Cohesity implements the security controls with a defense-in-depth approach across each module, while the communication between modules is secured across the services.

Cohesity Gaia tackles security challenges by incorporating multiple security measures alongside a secure data management system. Built on RAG AI, Gaia provides reliable and precise data insights using its indexed data.

Cohesity Gaia prioritizes enterprise data protection, security, and user privacy through a comprehensive suite of measures. It does not utilize any customer data for model training or learning, ensuring confidentiality and compliance with data protection regulations. The data is indexed only at the time of dataset creation, and the users can choose to disable chat history.
To enhance safety, Gaia automatically blocks profanity and inappropriate content, fostering a respectful environment.

In this section of Securing Your Data, we will discuss the various security measures that exist to secure your data through Identity and Access Management with SSO Support, Integration of SSO, Workflow of SSO Authentication, Managing Users, and the Implementation of fine-grained, Specialized RBAC policies, filtering of files/folders, Secure API keys and Implementing MFA. These security mechanisms restrict access to Cohesity Gaia APIs, ensuring that only authorized users can access specific data sets and also help balance data accessibility for Cohesity Gaia with the need to protect sensitive information.

Identity and Access Management (IAM)

Cohesity Gaia streamlines operational workflows by implementing a sophisticated IAM framework that manages user access, authentication, and authorization, while efficiently handling complex scenarios through its advanced architecture. This comprehensive system includes support for RBAC, API Keys, Single Sign-On (SSO), and Multifactor Authentication (MFA) mechanisms. By leveraging these advanced IAM tools, Cohesity Gaia ensures secure access to stored data while offering seamless integration with enterprise identity management solutions.

Now let's understand the various security mechanisms built-in Cohesity Gaia.

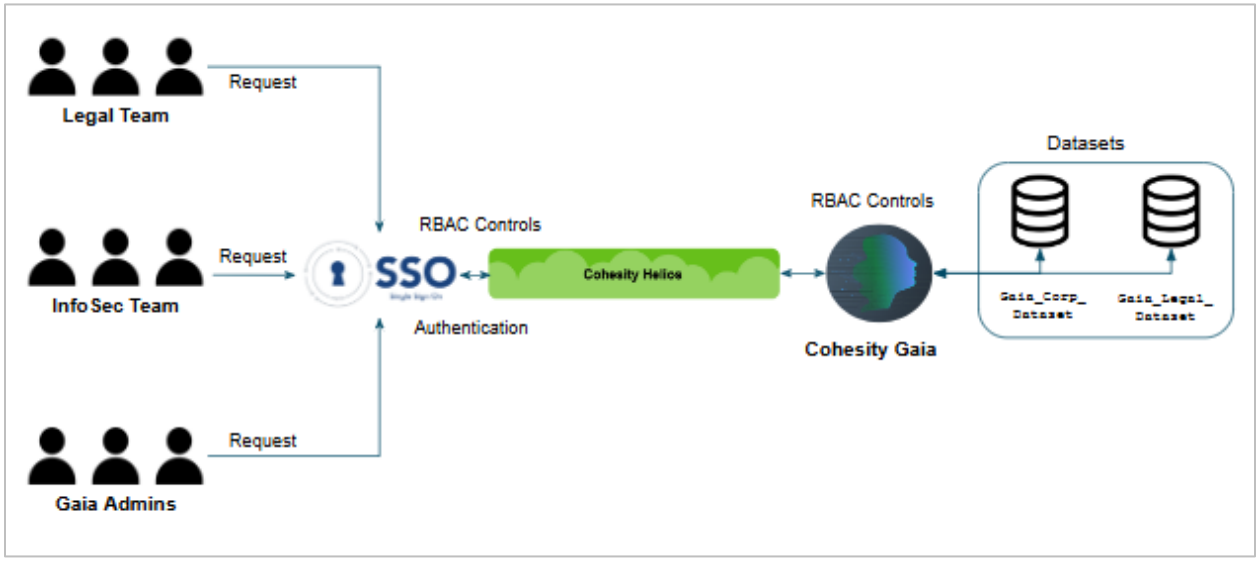
Cohesity Offers Seamless Single Sign-On Support

SSO simplifies access by allowing users to log in once and gain access to multiple applications without needing to remember separate passwords for each one. This not only improves user convenience but also enhances security by reducing password fatigue and minimizing the risk of weak or reused passwords. For organizations, SSO streamlines user management, strengthens security, and helps ensure compliance by centralizing authentication and access control.

SSO Authentication Workflow for Accessing Cohesity Gaia

Below is the workflow diagram of SSO Authentication to access Cohesity Gaia. This is an illustration of SSO authentication configuration for various teams using Cohesity Gaia, to secure your data with SSO.

Figure 3: SSO Authentication to access Cohesity Gaia



Step	User Management and Security Action	Objective
1. User Management in IdP	Users from the Legal, InfoSec, and Admins teams are added to respective groups in the Identity Provider (IdP) Application.	The IdP handles identity verification and user grouping.
2. Register IdP as SSO Provider in Cohesity Gaia	The IdP application is registered as the Single Sign-On (SSO) provider within Cohesity Gaia.	Enable secure authentication for all users accessing Cohesity Gaia through the IdP.
3. Add Users/Groups to Access Management in Cohesity Gaia	Users and groups created in the IdP are added to the Access Management system in Cohesity Gaia.	Define who has access to the system.
4. Assign RBAC Roles	Role-Based Access Control (RBAC) roles are assigned to the respective groups: • Legal Team: Granted query permissions.	Ensure each team has the appropriate level of access. **NOTE**: The minimum required role to access Helios is the Viewer Role. And to Converse with the

Step	User Management and Security Action	Objective
	• InfoSec Team: Ensures security policies are followed. Gaia Admins Team: Assists with Dataset creation/deletion/refresh for the Legal team.	Gaia - AI Assistant, we need the Gaia Viewer Role assigned as well.
5. Authorization Based on Assigned Roles	Upon authentication, the assigned roles dictate what level of access each group has within Cohesity Gaia.	Ensure that access is granted only according to roles and responsibilities.
6. Security Oversight by InfoSec Team	Continuous monitoring and ensuring the security of data access within Cohesity Gaia by the InfoSec team.	Ensure secure data access and compliance with internal policies.
7. Periodic Reviews & Audits	The admin team periodically reviews access rights, and the InfoSec team conducts security audits.	Ensure ongoing compliance and security.

Cohesity integrates with all major SSO services that support SAML & OpenID Connect protocol standards. This enables each Organization to apply its specific controls for password policy, multifactor authentication, and other controls through the upstream Identity Provider. We will understand how Cohesity offers seamless SSO Integration in the next section.

Supported Identity Providers for SSO Integration with Cohesity

Here are the qualified Identity Providers for SSO Integration with Cohesity. We adhere to industry-standard protocols for Single Sign-On (SSO) integration. If a particular SSO solution is not listed, but its Identity Provider (IdP) complies with established industry standards, it should be compatible with our system.

You can configure Cohesity Helios to use an Identity Provider (IdP) to enable SSO access to your Cohesity Helios instance.

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

- **IdP-initiated login**: Sign in to Cohesity Helios using the IdP sign-in page
- **SP-initiated login**: Sign in with the SSO link on the Cohesity Helios login page.

Integrating with SSO Identity Providers

To integrate with an IdP, users must configure details on both the IdP and the SP, Cohesity. SSO support is delivered through the Cohesity REST API, providing extensibility and reliability.

Cohesity currently supports two SSO protocols

1. SAML 2.0 server-based single sign-on (SSO) authentication.
2. OpenID Connect authentication (OpenID Connect is an open authentication protocol that uses the OAuth2.0 framework).

The IdP/SSO providers support MFA for users. This feature allows you to implement MFA with external MFA systems.

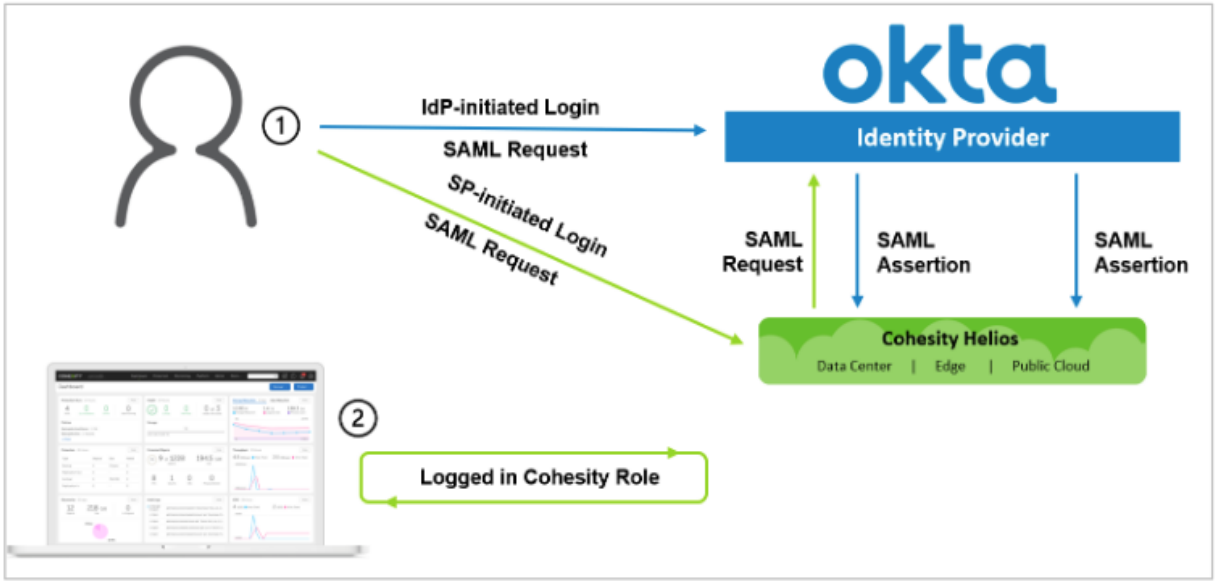
SAML 2.0 SSO allows users to log in to Helios via a browser, while OpenID Connect SSO allows applications to log in to Helios on behalf of the user.

Authentication workflow for SAML 2.0

The authentication workflow for SAML 2.0 SSO starts with the IdP or the SP:

1. The user logs in:
   a. **Via IdP**: The IdP identifies and authenticates the user and sends a SAML 2.0 assertion to the SP, Cohesity Helios.
   b. **Via SP**: A user requests to log in to the SP, Cohesity Helios, via SSO. The SAML 2.0 request is redirected to the IdP. The IdP identifies and authenticates the user, and then sends a SAML 2.0 assertion to Cohesity Helios.
2. Cohesity Helios authorizes this user with the SAML 2.0 assertion and maps the user to the appropriate role.

Figure 4: IdP Authenticates Cohesity User and Assigns Appropriate Cohesity Role



Authentication workflow for OpenID Connect (OIDC)

The authentication workflow for OpenID Connect SSO starts with the Client:

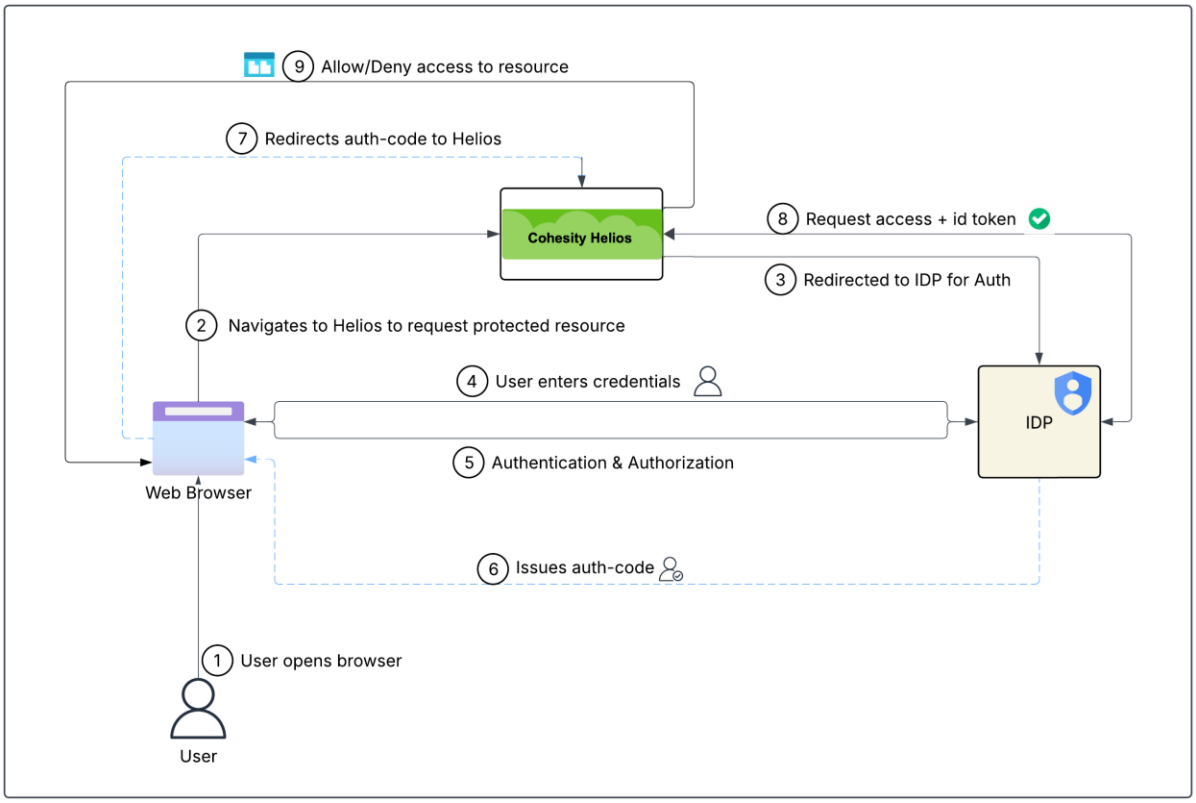
The user logs in:

a. Via IdP: The IdP identifies and authenticates the user, sends the ID Token (JWT), and redirects the user to Cohesity Helios.

b. Via SP: A user requests to log in to the SP, Cohesity Helios, via SSO

   1. Cohesity Helios redirects the user to the Authorization Server (IdP)
   2. The IdP authenticates the user and issues an ID Token (JWT)
   3. Cohesity Helios receives the ID token, verifies it, and maps the user to the appropriate role.

Figure 5: Authentication workflow for OpenID Connect (OIDC)



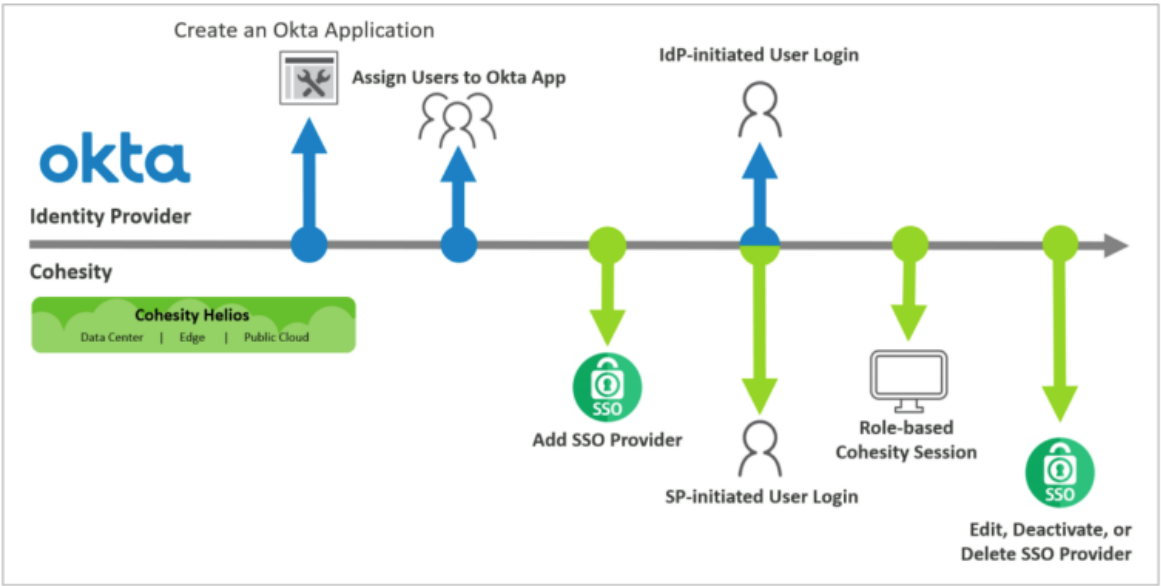
Configure Access Management with SSO Identity Providers on Cohesity

To configure and use SSO Provider on Cohesity Helios:

1. **Create your SSO Application:** This will be used for Cohesity Helios.
2. **Assign users to your SSO Application:** Assign users to the SSO application.
3. **Add your SSO Provider:** Use the credentials to configure access management in Cohesity Helios

4. **Role-based Cohesity Session:** Users log in to Cohesity Helios via SSO Application (IdP-initiated) or Cohesity Helios SSO login (SP-initiated)
5. **Manage SSOs:** Edit, deactivate, or delete your SSO Provider.

Figure 6: Access Management with IdP SSO Lifecycle



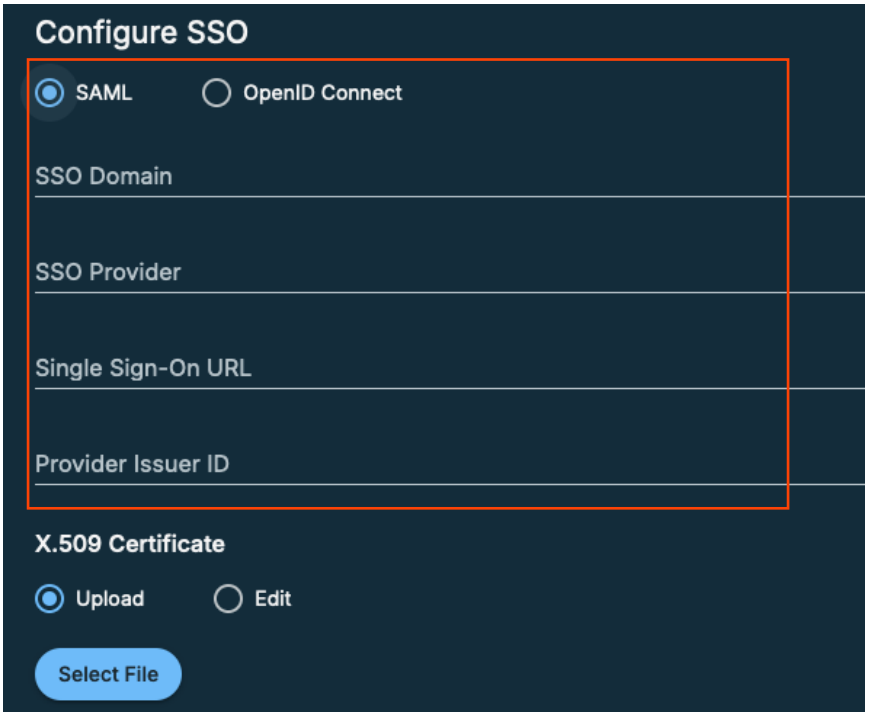
Prepare Required Information for SSO Integration

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

To create the SSO Application for SAML 2.0, which will integrate with Cohesity Helios, you will need:

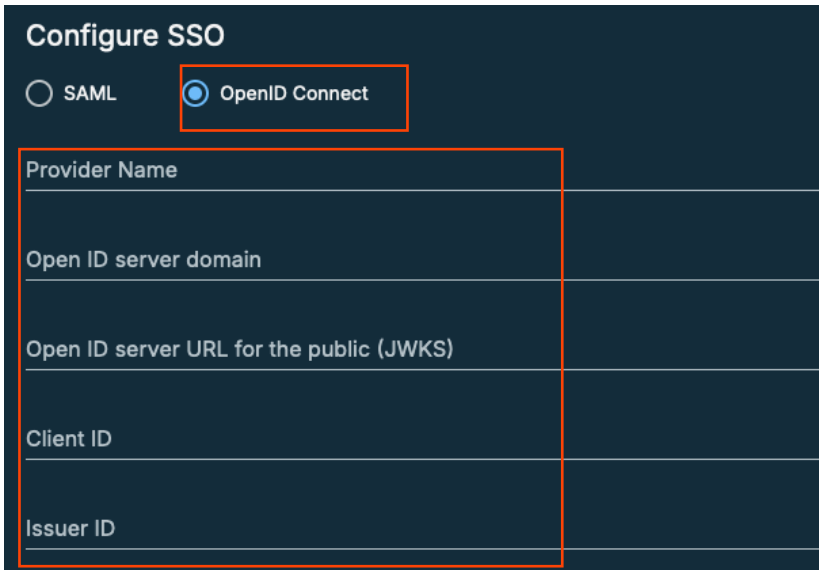
- **SSO Domain:** Unique domain name that will differentiate this IdP from others. As Cohesity supports multiple IdPs, this must be a unique string (usually a company domain). For a user to be redirected to this IdP, the user will need to log in via SSO using username@SSO_DOMAIN.

  When a user logs in to Cohesity Helios using SSO and enters the email address foo@bar.com, Cohesity Helios looks for the IdP with the SSO Domain configured as bar.com and redirects this user foo to the matching IdP. This is how Cohesity Helios determines which IdP the user needs to be forwarded to.
- **SSO Provider:** From the drop-down, select the SSO provider's name of your choice. Select the "I have read the SSO documentation provided by <SSO provider name>" check box. Cohesity recommends reading the SSO documentation before proceeding to the next step.
- **Single Sign-On URL:** Paste the URL that is copied from your IdP
- **Provider Issuer ID:** Paste the issuer ID copied from your IdP
- **X.509 Certificate:** Click Select File and browse to the location to select the file you downloaded and renamed previously.



To create the SSO Application for OpenID Connect (OIDC), which will integrate with Cohesity Helios, you will need:

- OpenID Server Domain: Enter a unique domain name.
- OpenID Server URL for the public (JWKS): Enter the JSON Web Key Set (JWKS) URL. You can get this URL from your identity provider.
- Client ID: Enter the ID of the application created in the identity provider.
- Issuer ID: Enter the Issuer ID URL. You can get the URL from your identity provider.

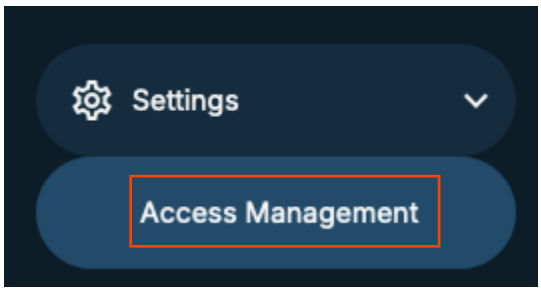


Please refer to the Configure SSO documentation for more information.

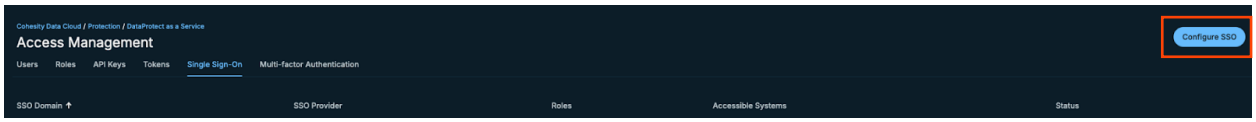
Add SSO Provider on Cohesity

Now that you have created the SSO application on your Identity Provider, and fetched all the required information, we will proceed to Configure SSO on Cohesity Helios.

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



3. Navigate to Single Sign-On tab in **Access Management.**
4. Click **Configure SSO** to perform the SSO Configuration on Cohesity Helios.



5. In the Configure SSO form, use the information that was captured earlier to complete the following fields for **SAML**:
   a. SSO Domain
   b. SSO Provider
   c. Single Sign-On URL
   d. Provider Issuer ID
   e. X.509 Certificate
   f. Default Role for all SSO Users
   g. Access Scope

   (OR)

   In the Configure SSO form, use the information which was captured earlier to complete the following fields for **OpenID Connect (OIDC)**:

   a. Provider Name
   b. OpenID server domain
   c. OpenID server URL for the public (JWKS)
   d. Client ID
   e. Issuer ID
   f. Public Key Expiration (Seconds)
   g. Public Key Refresh Interval (Seconds)

h. Token Validity (Seconds)

i. Default Role for all SSO Users

j. Access Scope

Cohesity Helios validates the connection to the SSO Provider. If the connection succeeds, the SSO Provider is added to the SSO provider list in Cohesity Helios. Users can start accessing Cohesity Helios via their SSO Provider 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 roles to them individually.
- Add an SSO group and assign the group the desired role.

Add SSO Users and Groups and provide the desired roles to ensure data accessibility and data security to the authorized users.

The users can be added directly to Cohesity Helios, or users can be added to a group in the Identity Provider (IdP) application and that group can be added to Cohesity Helios, to provide access to Cohesity Gaia.

Create a group in your IdP (For ex: legal_team) and assign it to IdP app (For ex: Cohesity Gaia). And add users to the group:

1. user1@SSO_domain.com
2. user2@SSO_domain.com

Now that we have SSO Integration ready to be configured, we will take a look at the RBAC policies being offered.

Fine-grained RBAC policies

Cohesity Gaia incorporates advanced, fine-grained RBAC policies that precisely govern access to the Gaia APIs. These specialized policies ensure that only authorized users can access and manage the stored data, effectively mitigating the risk of data exposure or unauthorized access. The RBAC system is designed to accommodate various levels of access and privileges, offering granular control over user permissions and actions within the Cohesity Gaia environment.

Granular Role-based Access Control enables an organization to grant the least privileges to a user required to do their job, minimizing risk, and keeping areas outside their domain out of reach.

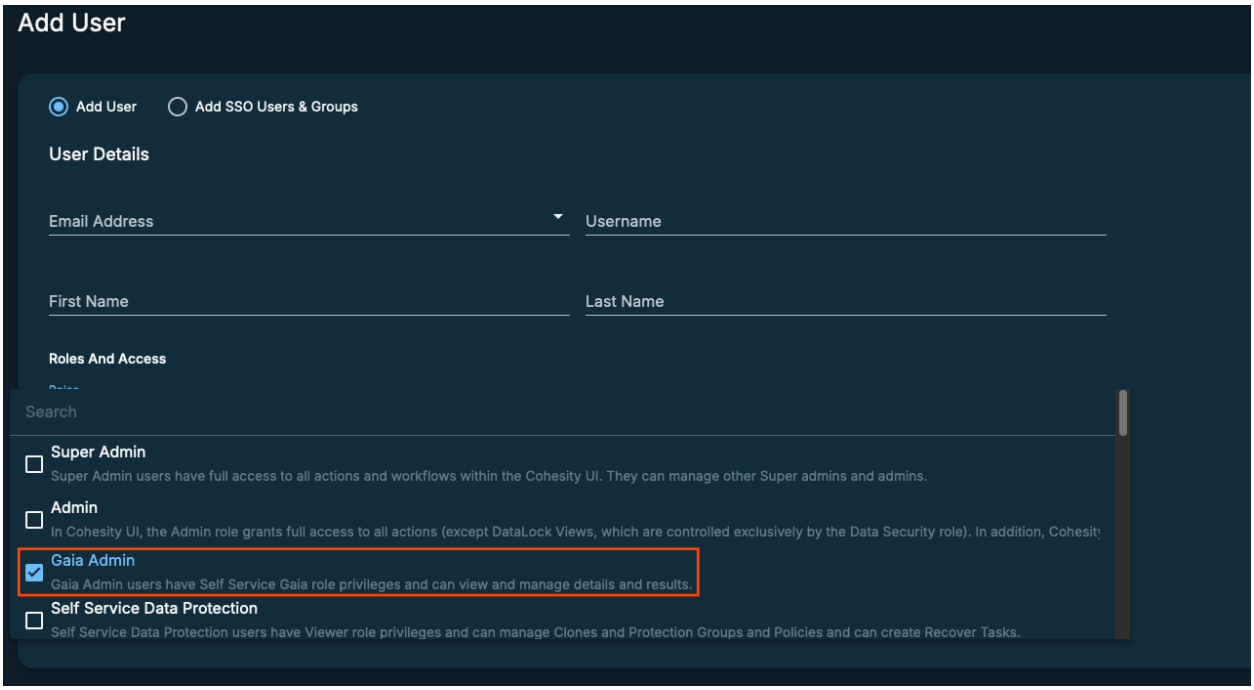
Granular RBAC for Cohesity Gaia consists of:

- **User roles – Standard and Custom**. Cohesity has two types of user roles that you can assign to specific users to control user access to the Cohesity cluster:
  - **Standard Roles**. Cohesity has several default system roles that act as templates based on different user privileges: Super Admin, Gaia Admin, Gaia Viewer and Viewer roles.

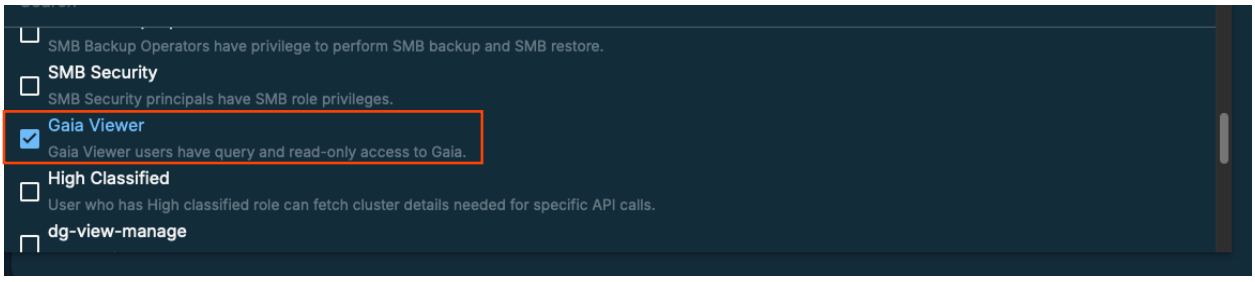
- **Custom Roles**. Cohesity administrators can create custom roles by picking up individual privileges. Users who are assigned these roles will have only those privileges.

- **Ability to restrict user role to granular functionality**. You can restrict Cohesity user roles to specific workflows, thereby limiting what a user with a certain role can do on the cluster. For example, you can restrict specific users to perform activities such as creating, editing, or deleting datasets.
- **Restrict user access to a specific object**. You can restrict users or groups to have access only to specific datasets. No other dataset will be visible to the user other than the datasets that are assigned to it.

Gaia Admin: Gaia Admin users have Self Service Gaia role privileges and can view and manage datasets and results. The Gaia Admin user has privileges listed here.



Gaia Viewer: Gaia Viewer users have read-only access to Gaia and can converse with the Gaia - AI Assistant. This role has the privileges listed here.

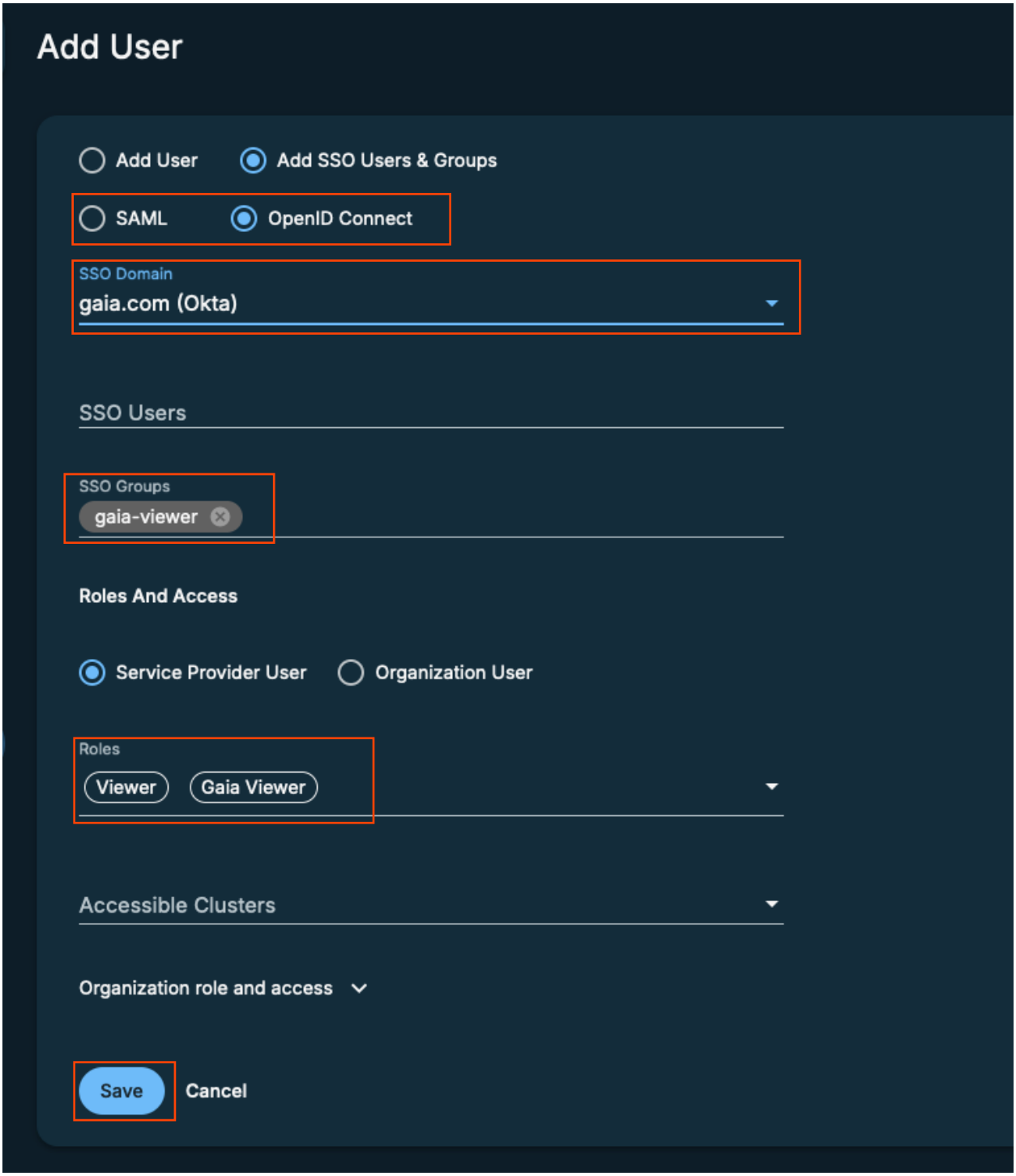


You can also create a custom role and Assign privileges as required:

To manage user access to the Cohesity Helios we recommend that you add users and groups. Once you create them, the users can start using Cohesity with their logins.

Add Users or Group in Cohesity Helios, by going to Settings > Access Management > Add SSO Users & Groups

The SSO Groups can be added as shown below, in both SAML or OIDC.

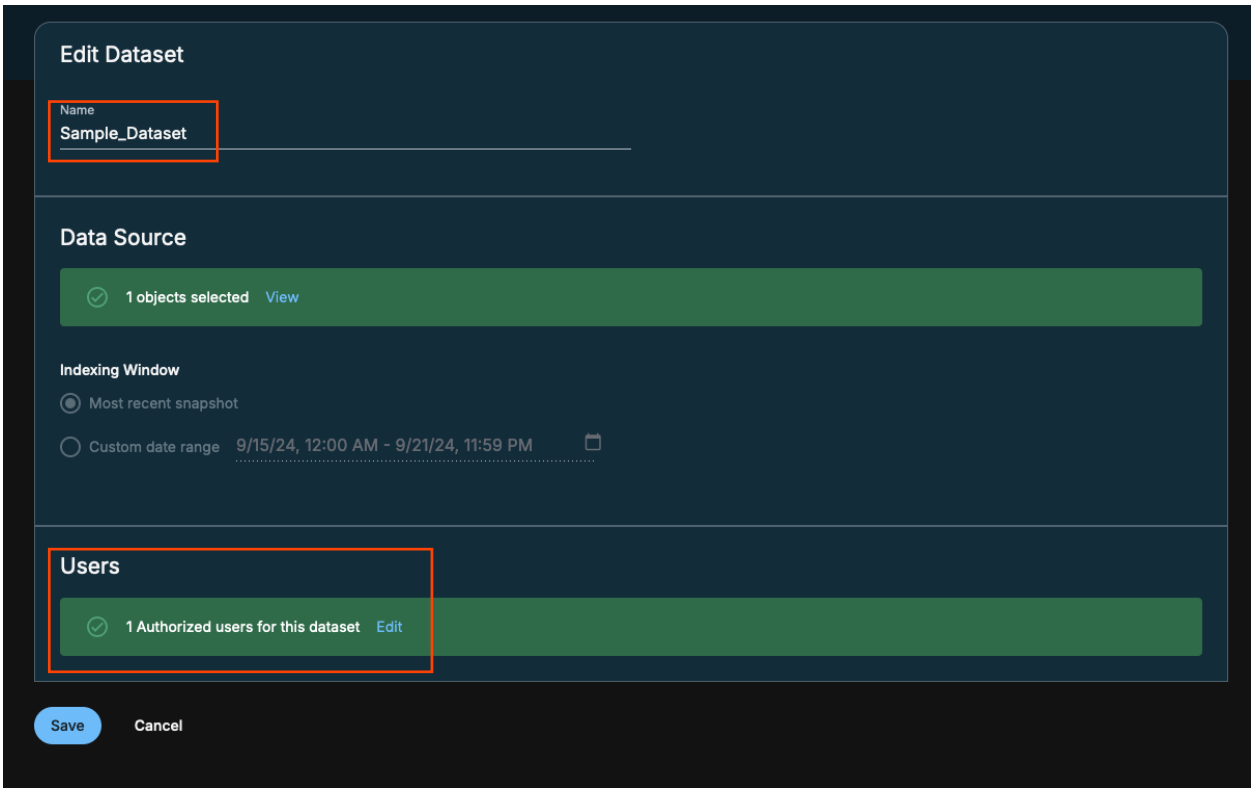


NOTE: Cohesity recommends enforcing Multifactor Authentication (MFA) for all local users.

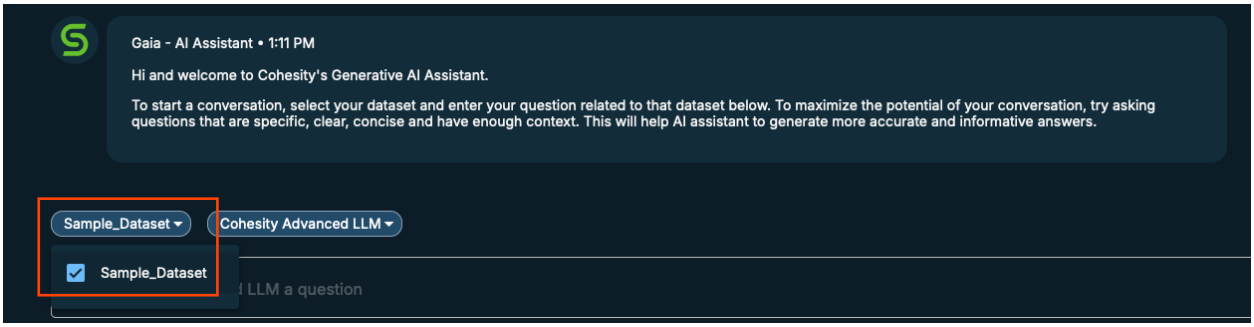
Restricting User or Group Access to a Dataset

After adding the users or groups in Cohesity Helios, you can restrict users or groups to have access only to specific datasets. To perform this, when creating a dataset, add Users or Groups in the Authorized Users who will have access to that particular dataset.

For example: Below we have a Gaia-viewer group, which has Gaia Viewer, and Viewer Role assigned to Sample_Dataset.



Once the user logs in, they will only have access and visibility to the dataset for which they have been given authorization.

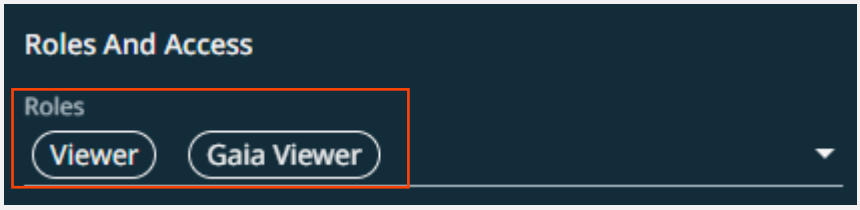


Assign one of the following built-in roles to users or groups who will be using Cohesity Gaia:

NOTE: The minimum required role to access Helios is the Viewer Role.

And to Converse with the Gaia - AI Assistant, we need Gaia Viewer Role assigned as well.

Ensure you assign both the **Viewer** and **Gaia Viewer** roles to grant users read-only access to all workflows.



Inclusion and Exclusions

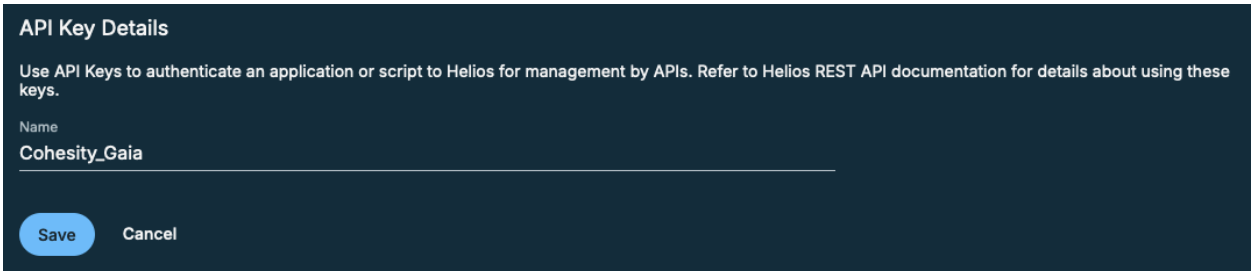
Cohesity Gaia allows you to create a dataset by incorporating files or folders filtering, which enables the assignment of these datasets to authorized users with RBAC. This provides several benefits, such as:

1. **Efficient Dataset Creation**: Filtering of files/folders helps in selecting only relevant data, avoiding the inclusion of unnecessary or irrelevant files/folders
2. **Enhanced Security through RBAC**
   a. **Controlled Access**: With RBAC, you can assign datasets to authorized users based on their roles, ensuring that only authorized users can access the dataset.
   b. **Custom Access Levels**: Granular control over who can view datasets and query, to align with organizational data protection policies.
3. **Compliance and Data Integrity**: RBAC ensures that access to sensitive data is limited to authorized users, helping organizations comply with legal and regulatory requirements.

You can Include and Exclude files or folders for Indexing with specific file types, and it supports Directory Regex Path for both Inclusion and Exclusion.

API Keys

You can Create API keys and use these API Keys to authenticate an application or a script, which gives you the capability to expand the use cases of Cohesity Gaia by using the built-in APIs.



Multifactor Authentication (MFA)

Multifactor Authentication (MFA) provides a two-step verification method to authenticate and access Cohesity Helios GUI. Multifactor authentication is an additional layer of security used to verify the identity of a user. With Cohesity, you can use native MFA or configure MFA with external MFA providers such as Ping, Duo, Okta, and more.

Native Multifactor Authentication

Cohesity Helios GUI supports Multifactor authentication for local users. Cohesity recommends that the Administrators enable MFA for all or specific local users.

Administrators can select one or both of the following authentication methods:

- **Authenticator App**: Cohesity recommends you install a Time-based One-Time Password (TOTP) authenticator app such as Okta Verify, Google Authenticator, Microsoft Authenticator, Duo Mobile, etc., on your device and enter the verification code generated by the app.
- **Email**: Users must enter the verification code sent to their email address.

After MFA is enabled, users can access the Cohesity Helios GUI by providing their local user password and the verification code generated by the authenticator app or received in their email.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Jedidiah Sonavane is a Solutions Architect, part of AI Team here at Cohesity. He focuses on Cohesity Service Provider/Organization, Cloud Archive On-Prem and Cohesity Gaia. His work includes proofs of concepts, enterprise data protection, solution design, validation, testing, qualification, and ensuring software usability. He collaborates closely with teams to tailor solutions that meet customer needs while adhering to industry standards and best practices.

Other essential contributors included:

- Akshay Kumar, Sr Manager, Product Solutions
- Bharath Nagaraj, Sr Principal Field Technical Director
- Sai Kiran Polavarapu, Staff 2 Engineer
- Karthick Radhakrishnan, Director, Security COE

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.2	Nov 2025	Content Updates
1.1	Nov 2024	Content Update
1.0	Nov 2024	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 44 of the Fortune 100.

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