COHESITY

Integrate Dasera DSPM with Cohesity Data Cloud

Enhance security visibility, investigation, and rapid response to Cohesity incidents

Version 1.1

August 2025

ABSTRACT

The Cohesity Data Cloud provides cyber resilience with modern data management and protection capabilities. Integrating it with DSPM vendor solutions further enhances an organization's security operations by providing comprehensive visibility into sensitive data.

This guide explains how you can integrate the Dasera DSPM platform with Cohesity Data Cloud to enhance the security, visibility, investigation, and rapid response of Cohesity incidents to protect customer-critical data.

Table of Contents

Figures

Tables

Introduction

Data Security Posture Management (DSPM) is essential in today's data security landscape because it helps organizations protect their data and maintain compliance. DSPM can help organizations proactively identify and address security risks, which can help mitigate potential breaches and data leaks. Organizations today face a significant challenge regarding critical data visibility across many repositories. Accelerating cloud adoption, rapidly expanding and dispersing data across multiple systems, locations, and storage solutions compounded by an explosion of microservices, puts customers at risk of significant data sprawl. Due to these visibility gaps, critical and sensitive data becomes hidden from IT teams and often goes unprotected. The need for DSPM capabilities and modern data security and management services has never been greater. DSPM gives customers a deep understanding of their sensitive data, who has access to it, how it is used, and where it is stored.

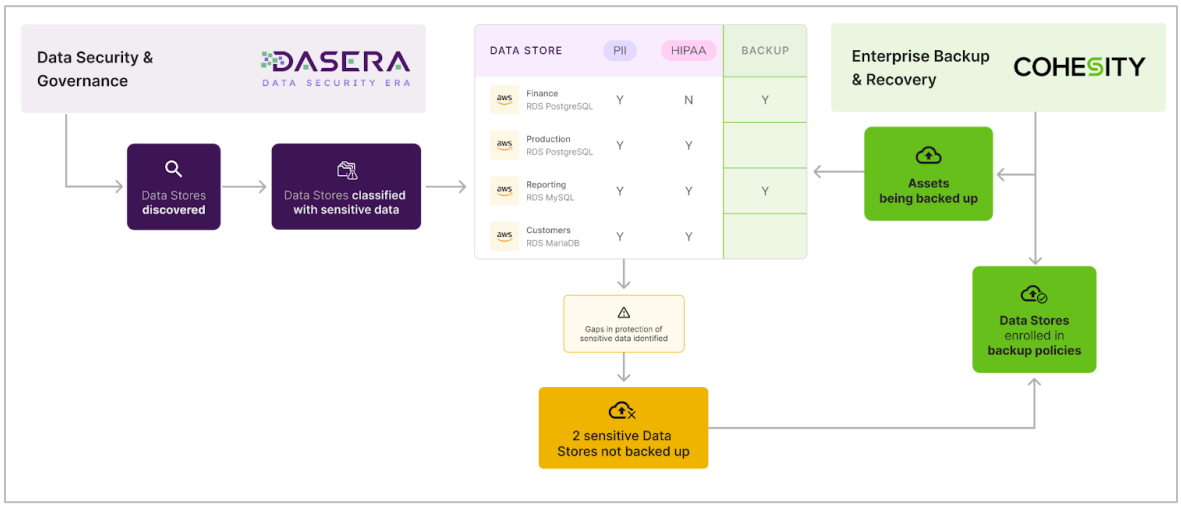
Cohesity & Dasera is the first integration, developed by DSPM vendors using Cohesity's Open APIs, that enables automated and continuous data classification and risk assessment across cloud data stores. This integration optimizes protection strategies and data retention based on the criticality of data in Cohesity-backed environments. It also allows for prioritizing data restoration according to business importance and enhances the incident response process through real-time analysis of incident evidence. With Cohesity's modern data security and management technology, customers have a robust cyber resilience posture. Refer to Dasera DSPM Overview and Cohesity Data Cloud Overview for more information on the two platforms.

This guide explains how to integrate the Dasera DSPM, a leading DSPM platform, with Cohesity Data Cloud to accelerate the protection of sensitive and vulnerable data assets. It also allows customers to prioritize protecting cloud workloads with critical risks, increasing their resilience in the face of potential attacks.

Cohesity Data Cloud and Dasera DSPM Integration

Managing and securing data across hybrid environments is a significant challenge in today's complex data landscape. Dasera, joining Cohesity's Data Security Alliance, provides a unified solution that revolutionizes Data Security Posture Management (DSPM) and data protection across multi-cloud environments. This collaboration integrates Dasera's robust DSPM capabilities with Cohesity's AI-powered data security and management platform. This synergy offers a consolidated view of your data estate, enhancing compliance and mitigating risks.

For example, this integration can reveal previously uncovered data assets with Personally Identifiable Information (PII) that were not backed up. This information enables IT backup administrators to adjust protection priorities and provides security teams with the data to fulfill their protection mandates effectively.



Integration Benefits

- **Enhanced Data Discovery**: Automate sensitive and critical data detection across multi-cloud environments, improving oversight and control of your data landscape.
- **Resilient Data Security Posture**: Proactively identify and rectify vulnerabilities within cloud workloads, ensuring comprehensive data protection and swift incident recovery.
- **Advanced Risk and Compliance Reporting**: Strengthen your cybersecurity frameworks with enhanced risk assessments and compliance reporting, building a more resilient and secure data infrastructure.
- **Unified Data Visibility and Control**: Comprehensive monitoring of all data assets, enhancing governance and risk management.
- **Enhanced Data Security and Compliance**: Improved defense against cyber threats and simplified compliance with regulatory standards such as GDPR and CCPA.
- **Optimized Data Protection Strategies**: Cohesity's scalable backup and disaster recovery solutions complement Dasera's classification and protection of overlooked data assets.

- **Proactive Risk and Configuration Analysis**: Identification of misconfigurations and security gaps with immediate remediation capabilities, ensuring data integrity and security.
- **Streamlined Operational Efficiency**: Reduction in manual efforts and minimized risks, accelerating the time-to-value for data management initiatives.

Prerequisites

Dasera Access

1. Access to a Dasera-hosted application.
2. Dasera administrator user.
3. Connectivity to cloud source

Cohesity

1. Access to Cohesity Helios.
2. API key to connect Dasera to Cohesity for integration.
3. Connectivity to cloud source.

NOTE: Refer to How to fetch API Keys from Cohesity Data Cloud to generate API keys.

Workflow

The Cohesity Data Cloud and Dasera Integration is initiated from the Dasera application. Dasera uses Cohesity Open APIs to integrate with Cohesity, allowing Dasera to send data to Cohesity periodically.

The cloud source scanned for sensitive information must be registered at Cohesity and Dasera. Once the cloud data source is registered and the required data sources are connected, Dasera initiates a scan. The user can configure the scan frequency, schedule, and sampling rate from Dasera.

Dasera scans data stores to discover and classify sensitive data. Classification is performed via machine learning with a combination of heuristic signals. Scanned data is matched against relevant heuristic signals to determine if the data store contains sensitive data, its type and sensitivity level, and the resulting confidence score.

Dasera continuously classifies sensitive data, then programmatically assigns sensitivity levels and business purpose tags and maps them to known regulations. This approach involves classifying data based on its sensitivity and applying appropriate security controls based on that classification. The platform provides 50 out-of-the-box, built-in Custom Sensitive Data Types.

Dasera samples data from scanned data stores to identify and classify sensitive data. Across data types, classification is based on a combination of heuristic signals, including but not limited to:

1. Keywords
2. Field or file names
3. Field or file content
4. Dictionaries
5. Proximity
6. Query logs
7. Regex
8. Checksums

Built-in Tags

The following Data Tags & Tag Categories are built into Dasera and can be used immediately.

Table 1: Data Tags & Tag Categories

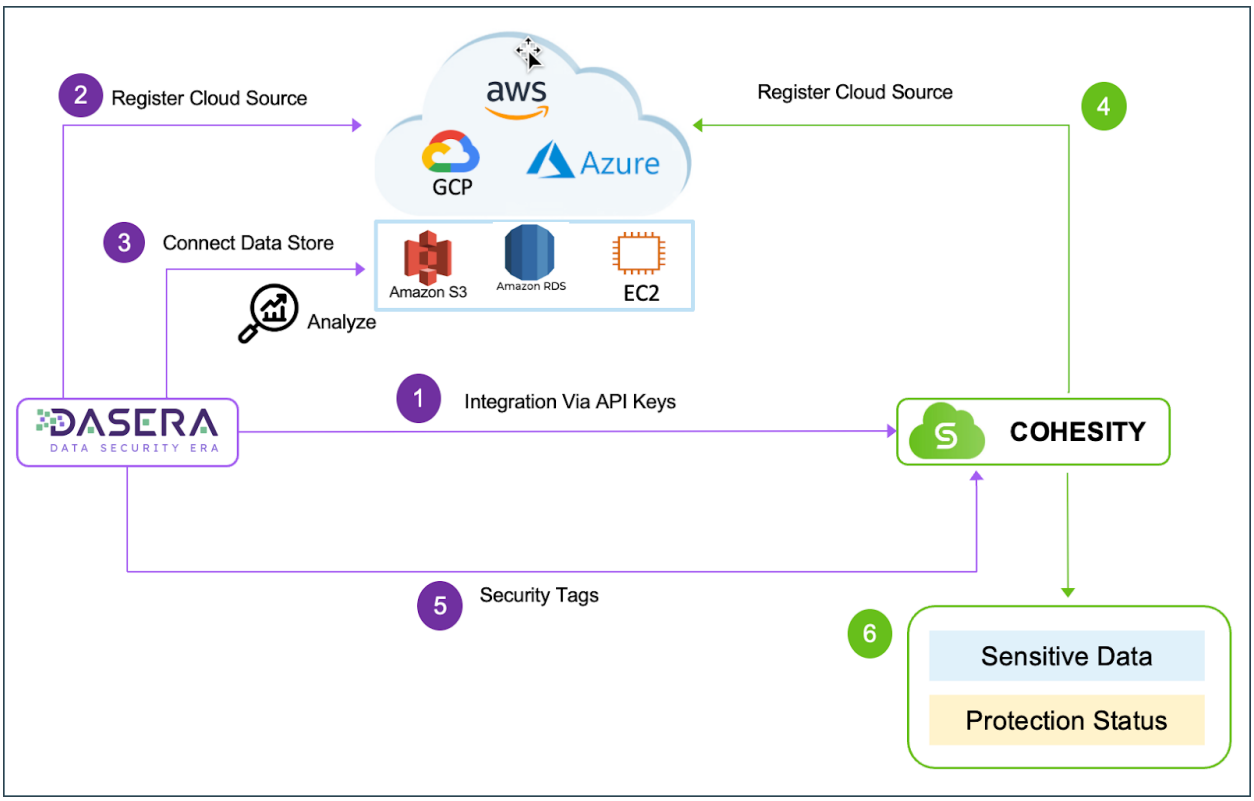
Tag Category	Tag Name
Compliance	• GDPR • CCPA • DPDP • PCI • SOX

Tag Category	Tag Name
Healthcare	• HIPAA-HI • HIPAA-PI
Other	• PII

Once the sensitive data has been identified, tagged, and mapped to the known regulation, organizations can remain compliant with industry regulations such as GDPR, CCPA, and HIPAA.

These tags are propagated to the Cohesity Security Center, where IT backup administrators can take corrective action to prioritize the backup and recovery of sensitive data assets.

Figure 1: Integration Workflow

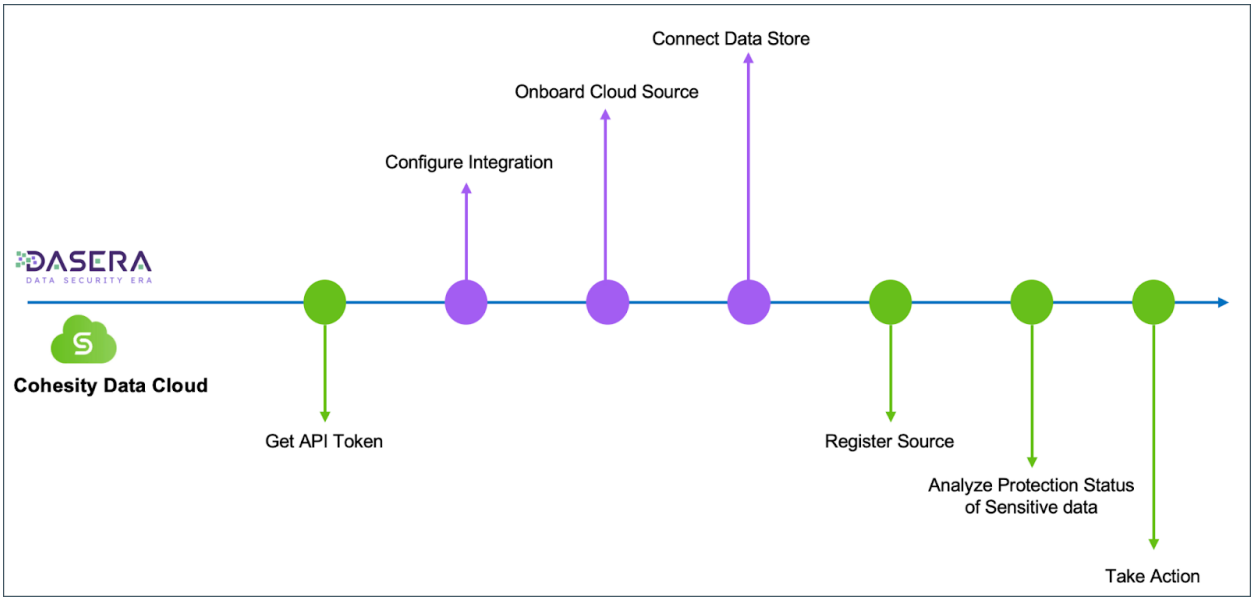


Configure Dasera DSPM Integration

The Cohesity Data Cloud integration with Dasera enables you to identify gaps in the protection of sensitive data within cloud accounts that Cohesity can see, assets at risk based on sensitive data classification, and exposure to potential attacks. It helps to prioritize data protection and enables quick action to recover critical workloads as needed.

To integrate Cohesity Data Cloud with Dasera DSPM, perform the following steps:

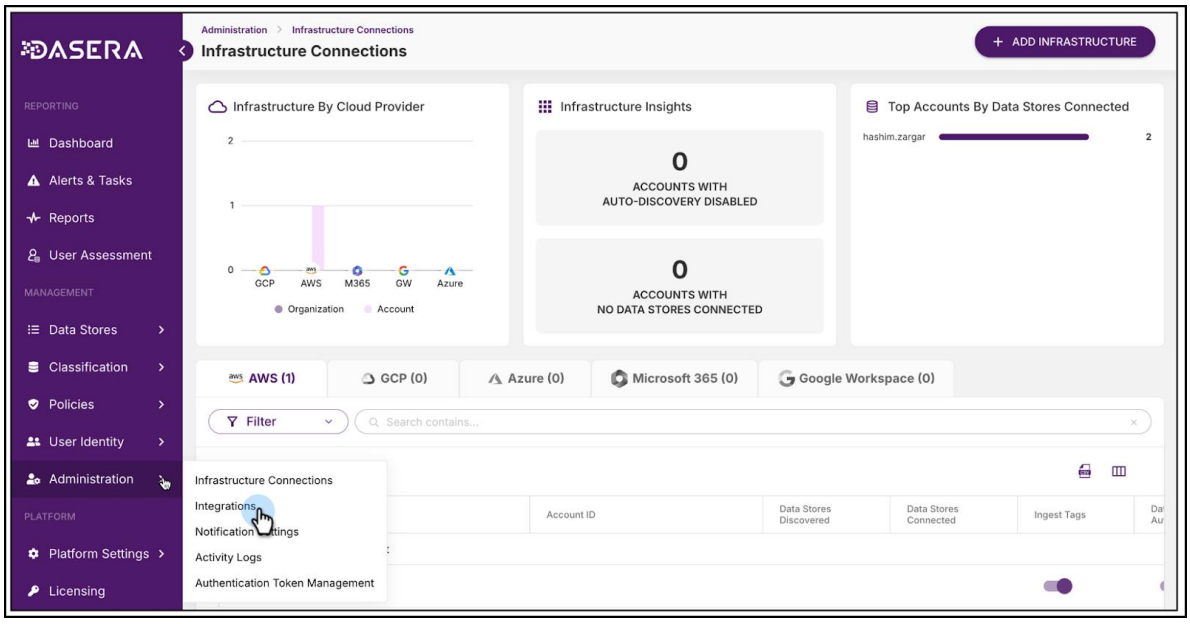
Figure 2: Steps - Configure Dasera DSPM Integration



Setting up Cohesity Integration on Dasera

1. Log in to the Dasera Application to set up the Cohesity Integration.

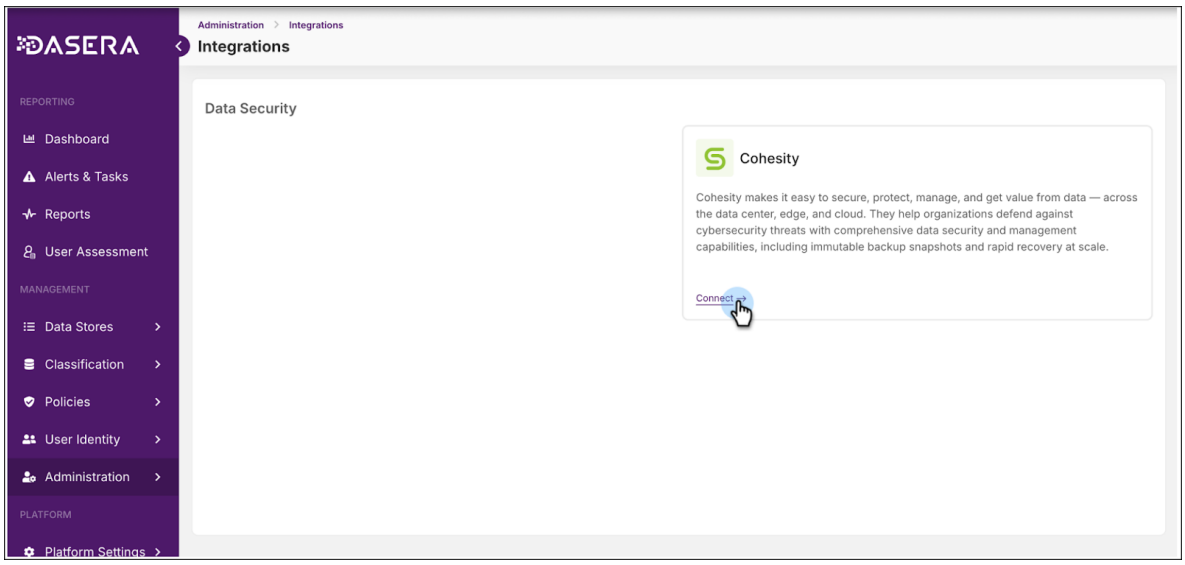
   In the Dasera UI, under **Management,** hover over **Administration** and click **Integrations**.



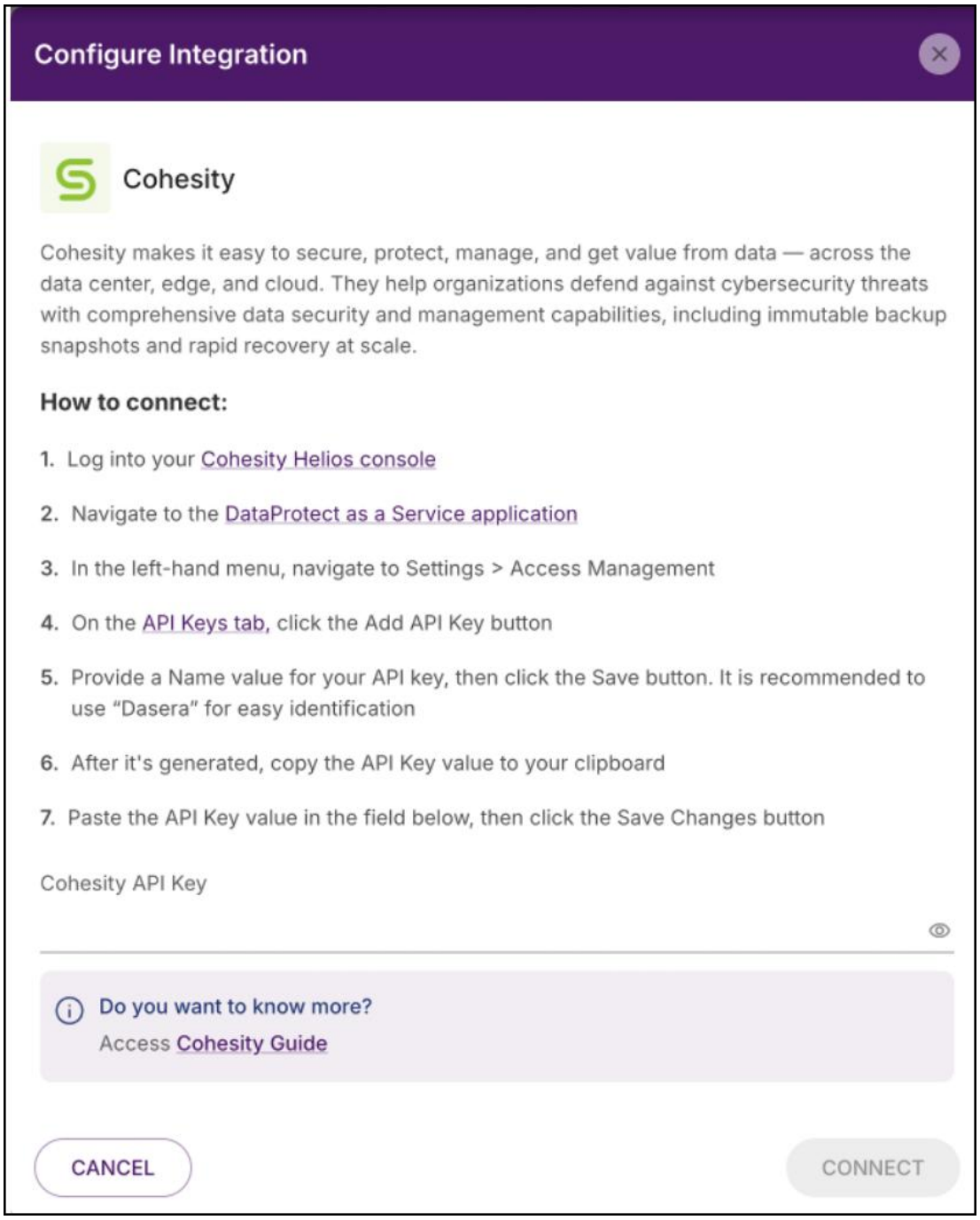
   To set up integration, the user can have the following Platform roles.

   - Super_Admin
   - Data_Set_Admin
   - Data_Team_Member

2. In the **Integrations** dashboard, hover over **Cohesity** and click **Connect**.

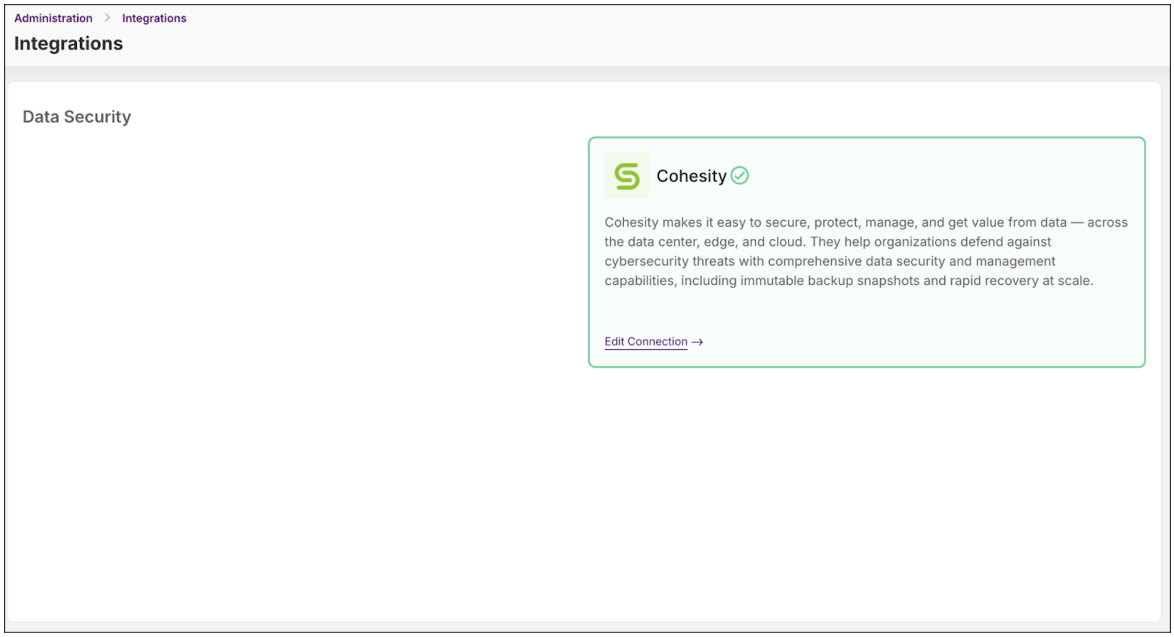


3. To generate the API keys from Cohesity Helios, follow the steps in the *How to Connect* section. Then, enter the Cohesity API Key in the **Configure Integration** menu.



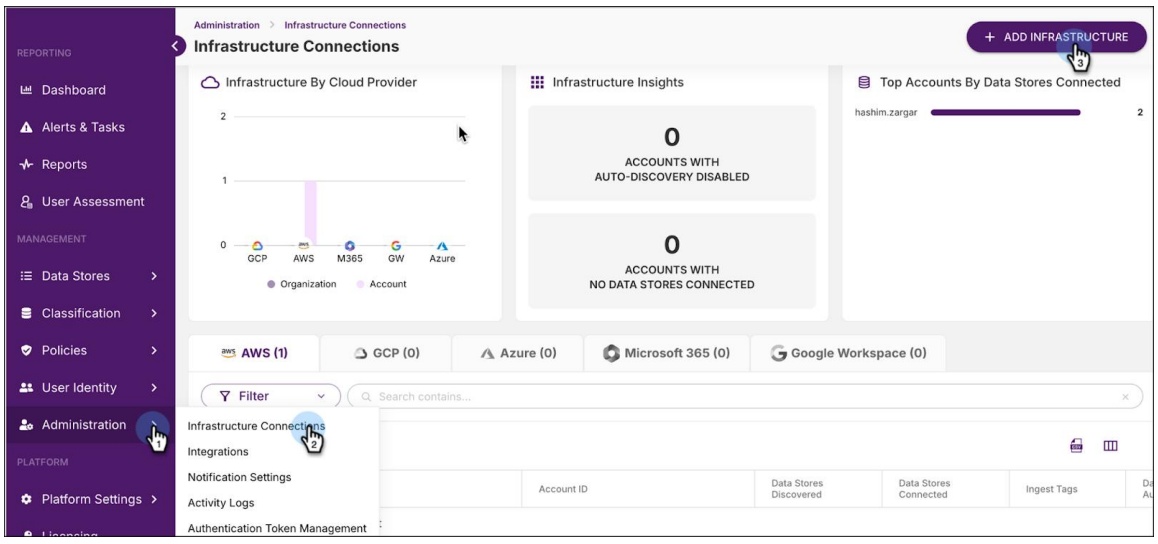
Refer to the How to fetch API Keys from Cohesity Data Cloud to generate the API key. Copy the key, paste it under the **Cohesity API Key** in Dasera UI, and click **Connect**.

4. The Cohesity integration will be connected under Integrations, signified by a green check mark.

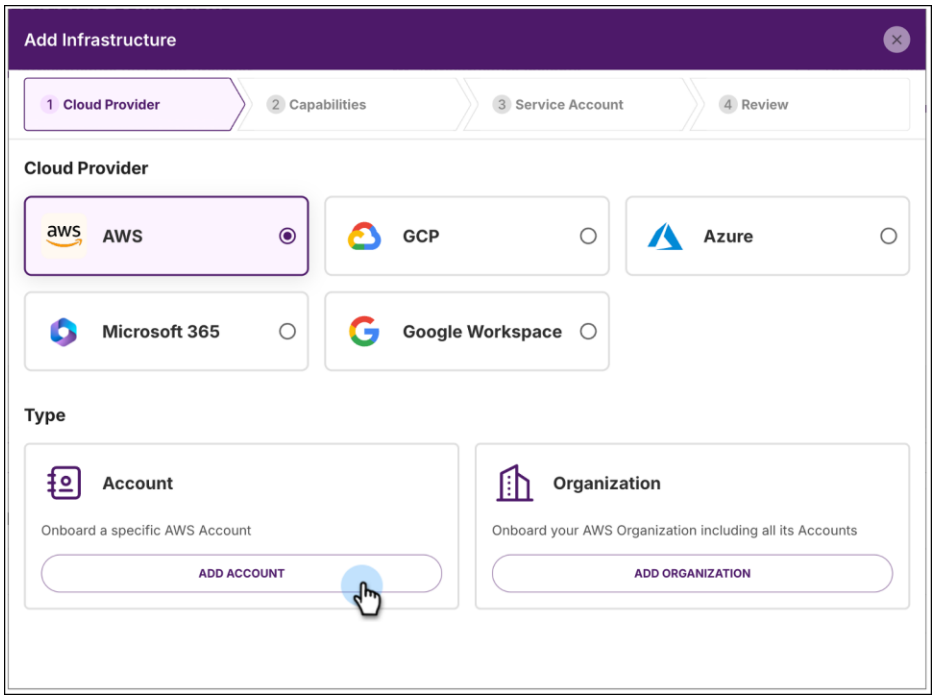


Onboard AWS Infrastructure on Dasera

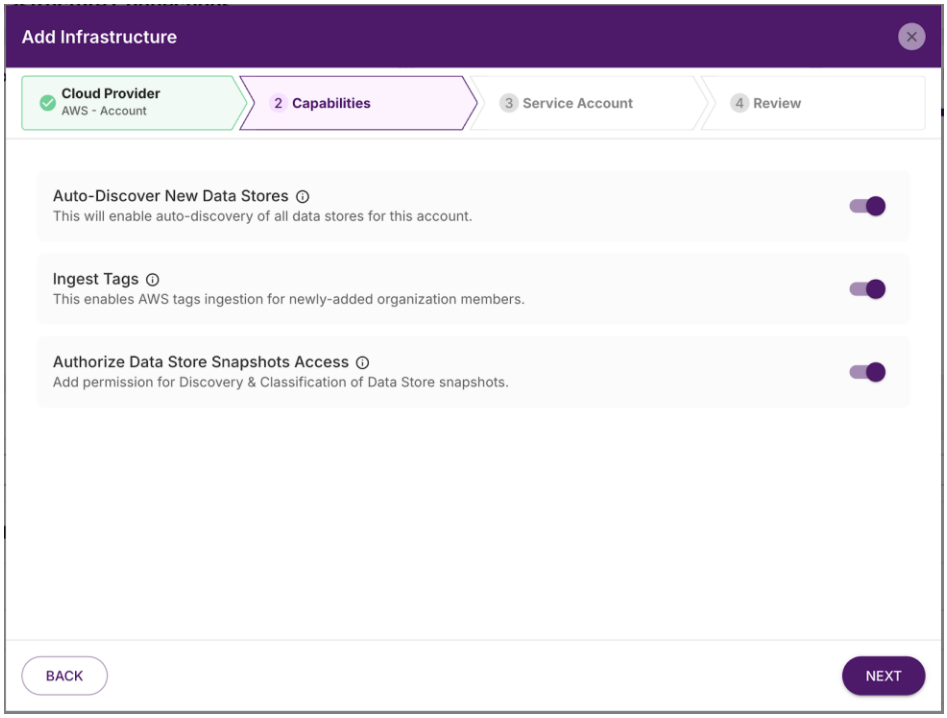
1. Log in to **Dasera**.
2. Navigate to **Administration** > **Infrastructure Connections** and click **Add Infrastructure**.



3. Select the cloud provider you want to analyze for sensitive information in the **Add Infrastructure** menu. The same account should be registered as a source on Cohesity (Refer to the Register the Source section for registering a source on Cohesity).
4. Ensure the cloud provider (here AWS) is selected and click **Add Account**.



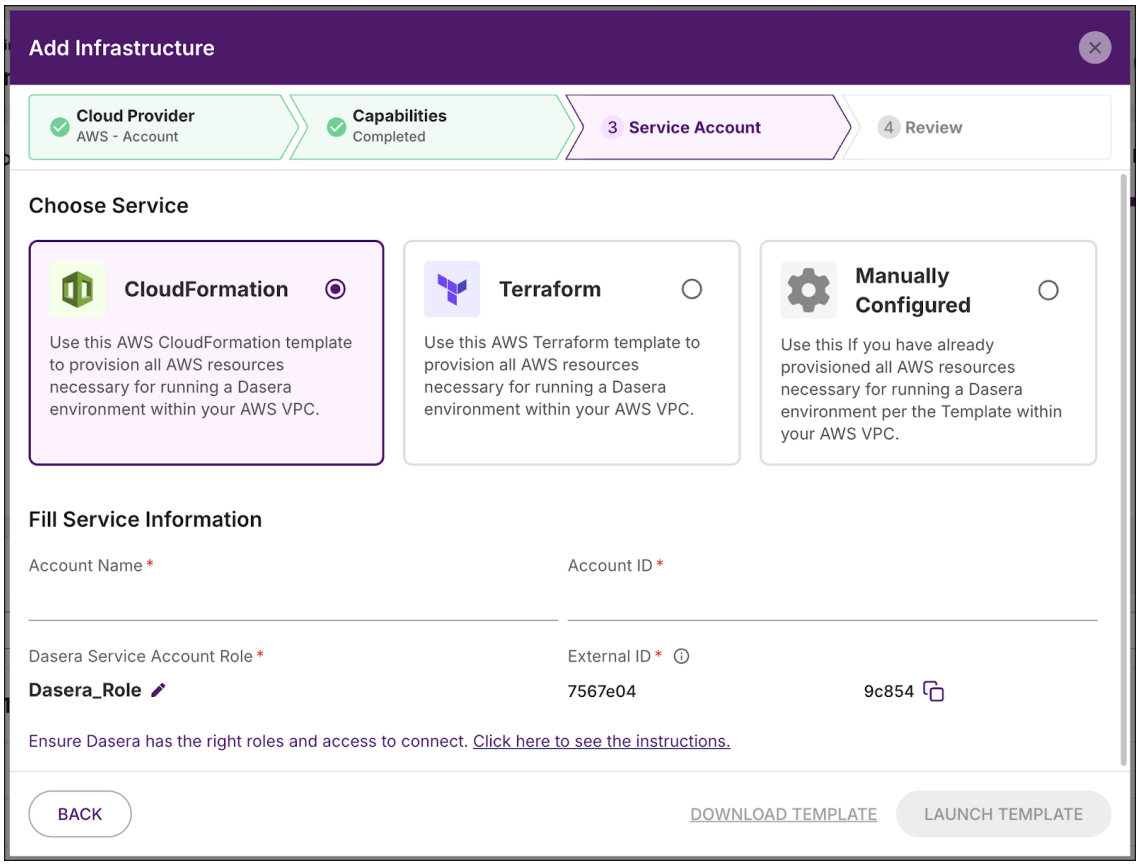
5. Depending on your preference, you can leave **Auto-Discover New Data Stores**, **Ingest Tags**, and **Authorise Datastore Snapshots Access** on or toggle it off in the **Capabilities** menu. Click **Next**.



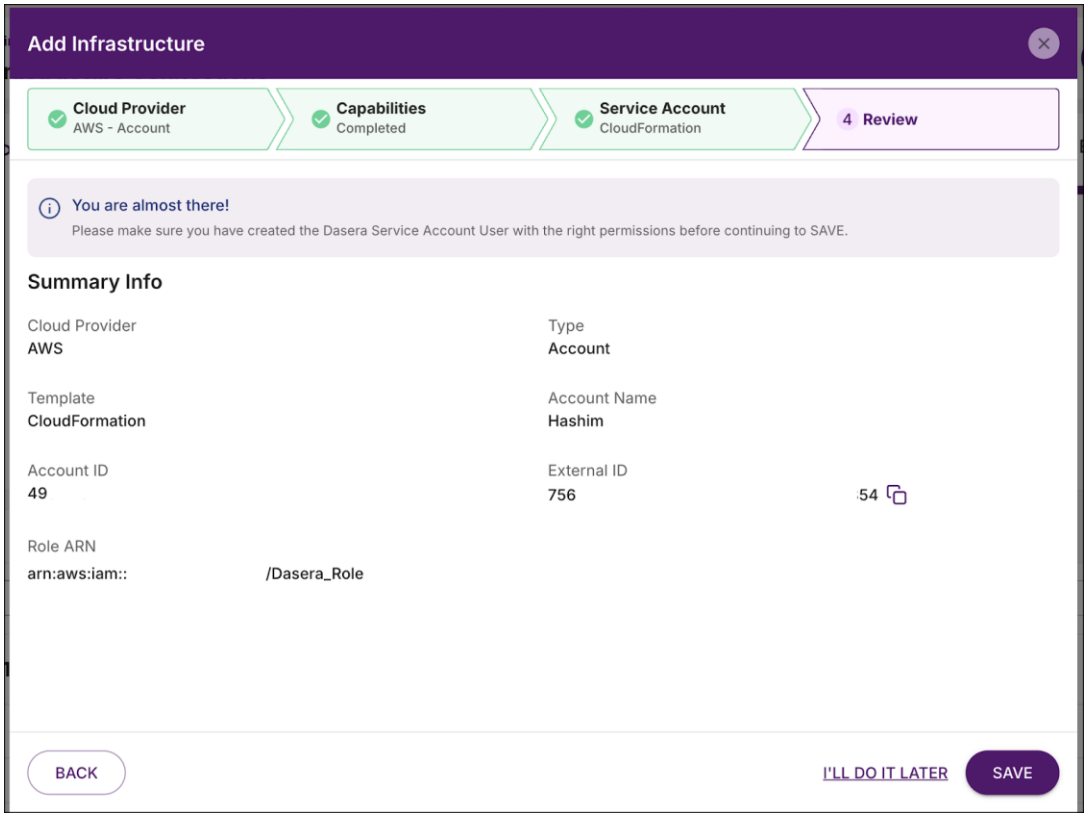
6. In the **Service Account** menu, select the Service to create the role on the AWS account. You can use CloudFormation or Terraform or manually configure the role on AWS. Here, we will use CloudFormation to set up the service account.

   Fill in the details below in the service information.

Field	Value
Account Name	Any value (this is used to identify your infrastructure connection within Dasera).
Account ID	Obtain from your AWS console.
Dassera Service Account Role	Will default to **Dasera_Role**. Note that this value needs to be unique to each onboarded account.
External ID	A unique identifier that third parties like Dasera use to assume a role in AWS account.



7. Click **Launch Template**.
8. The Launch Template will launch a CloudFormation Stack creation template to create the Dasera role with the required policies in your AWS account. Click Create Stack and wait for the Stack creation to complete.
9. On the Dasera UI, validate the summary details and click **Save**.



NOTE: Once the cloud infrastructure has been added, it cannot be removed or disconnected.

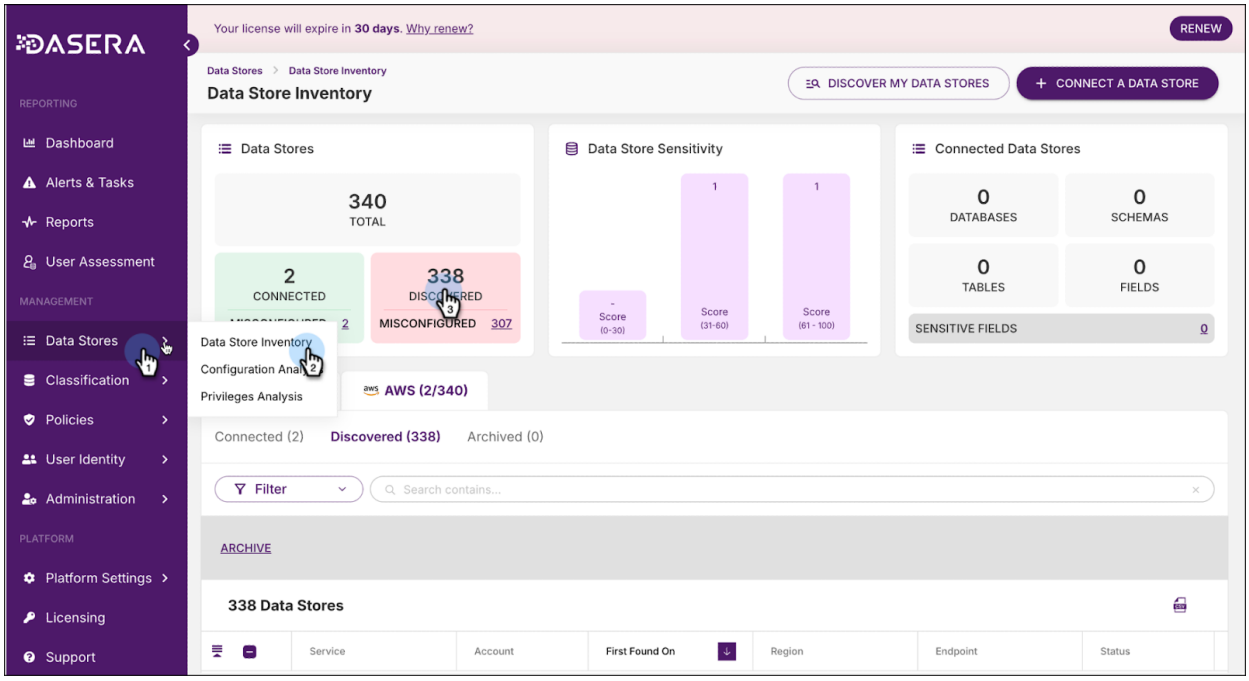
To validate whether the infrastructure has been added, navigate to Administration in the Dasera UI. Under **Administration**, click **Infrastructure Connection**. The Infrastructure Connections dashboard has all the information about the connected cloud providers and their associated accounts.

Datastore Discovery

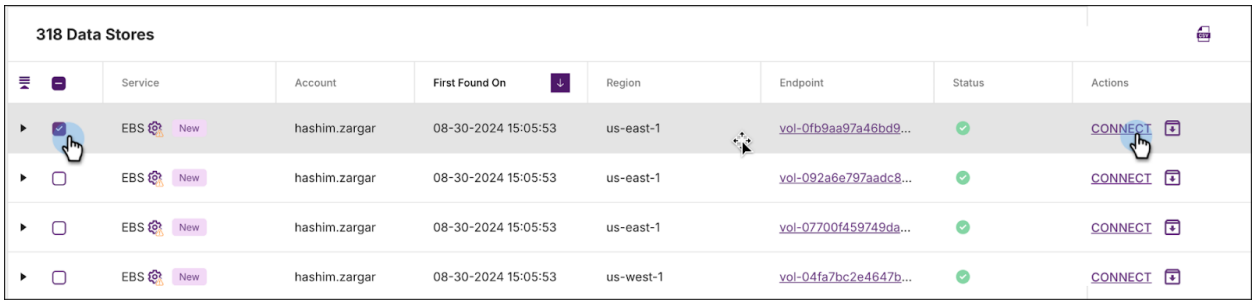
Once the cloud infrastructure has been configured, all the available data stores are discovered automatically. The data stores should be connected manually to scan for sensitive information. Once connected, Dasera will periodically trigger a scan for sensitive information and tag it according to its type. Dasera will monitor for compliance and PIIs and tag the data stores, allowing the users to understand the visibility of various data types, be it phone numbers, social security numbers, or any form of PII, and take appropriate actions.

Follow the below steps to connect to a datastore:

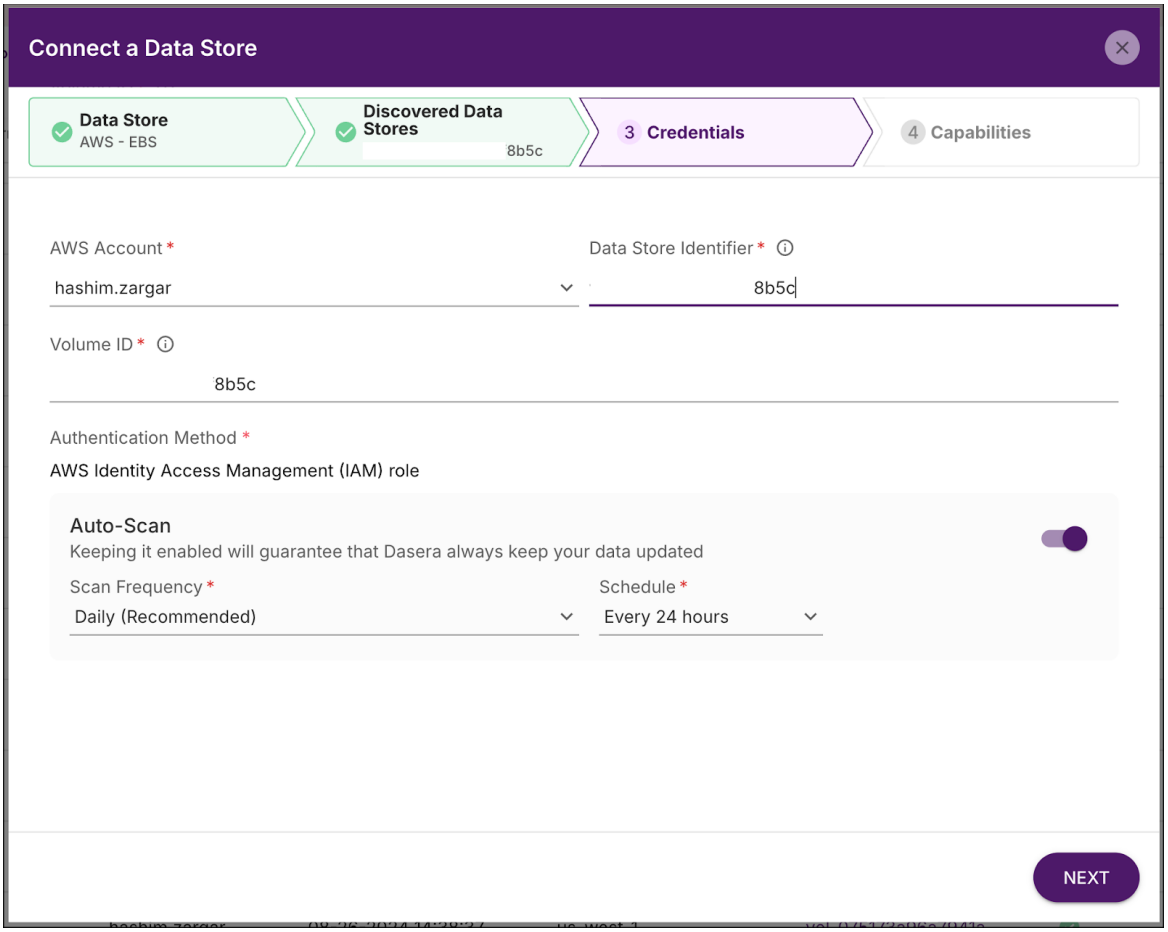
1. In the Dasera UI, under Data Stores, select **Data Store Inventory**. The data store inventory lists all the discovered data stores. Click Total or Discovered to list all the discovered data stores.



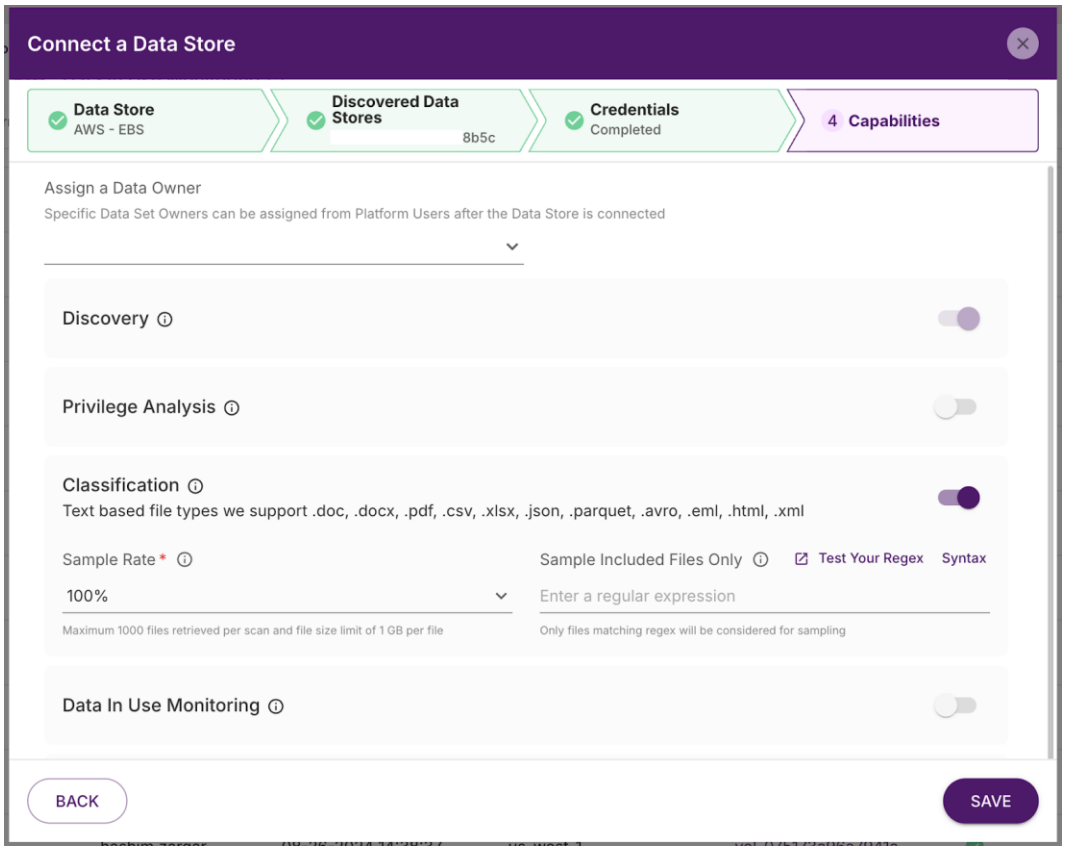
2. Scroll down to see all the listed data stores.
3. Select the data stores you want to scan and click **Connect**.



4. In the **Credentials** menu, enter valid credentials for the type of service. Below is an example of an EBS datastore credential menu. Click **Next**.



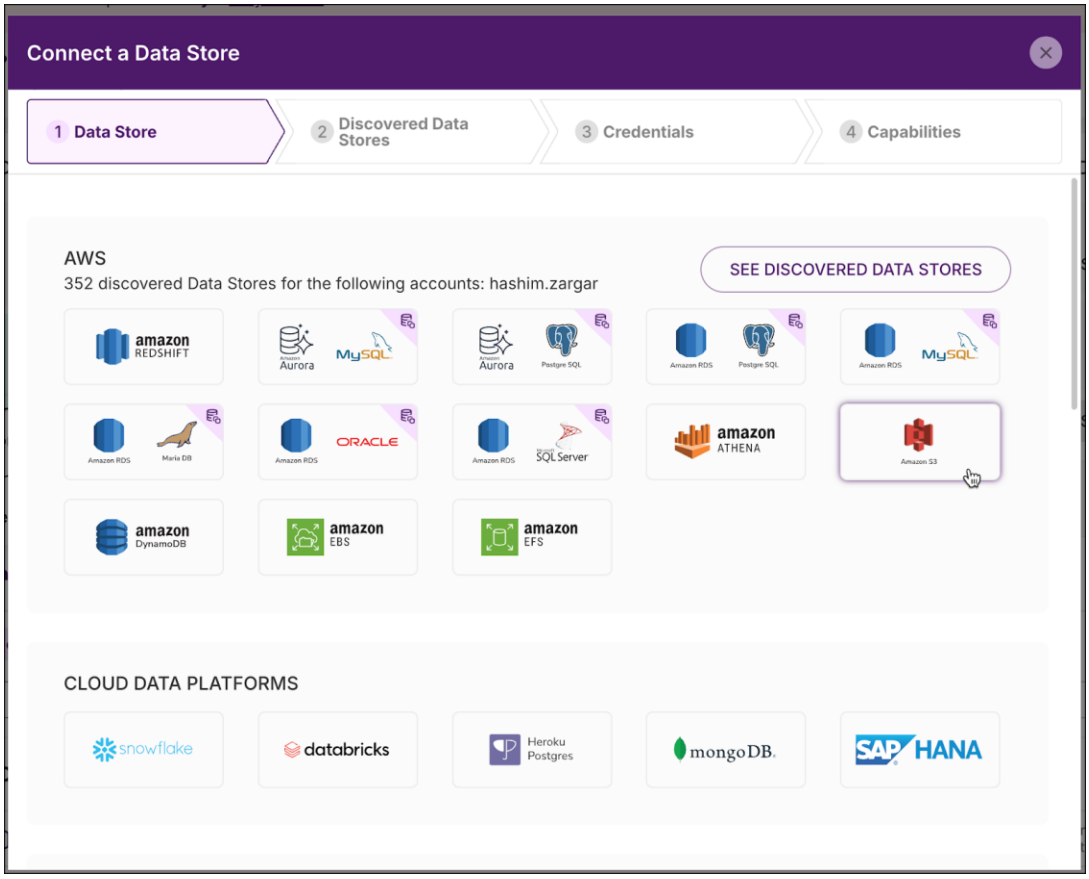
5. In the **Capabilities** menu, assign the data owner from the drop-down menu. Select the other options as per requirement and click **Save**.



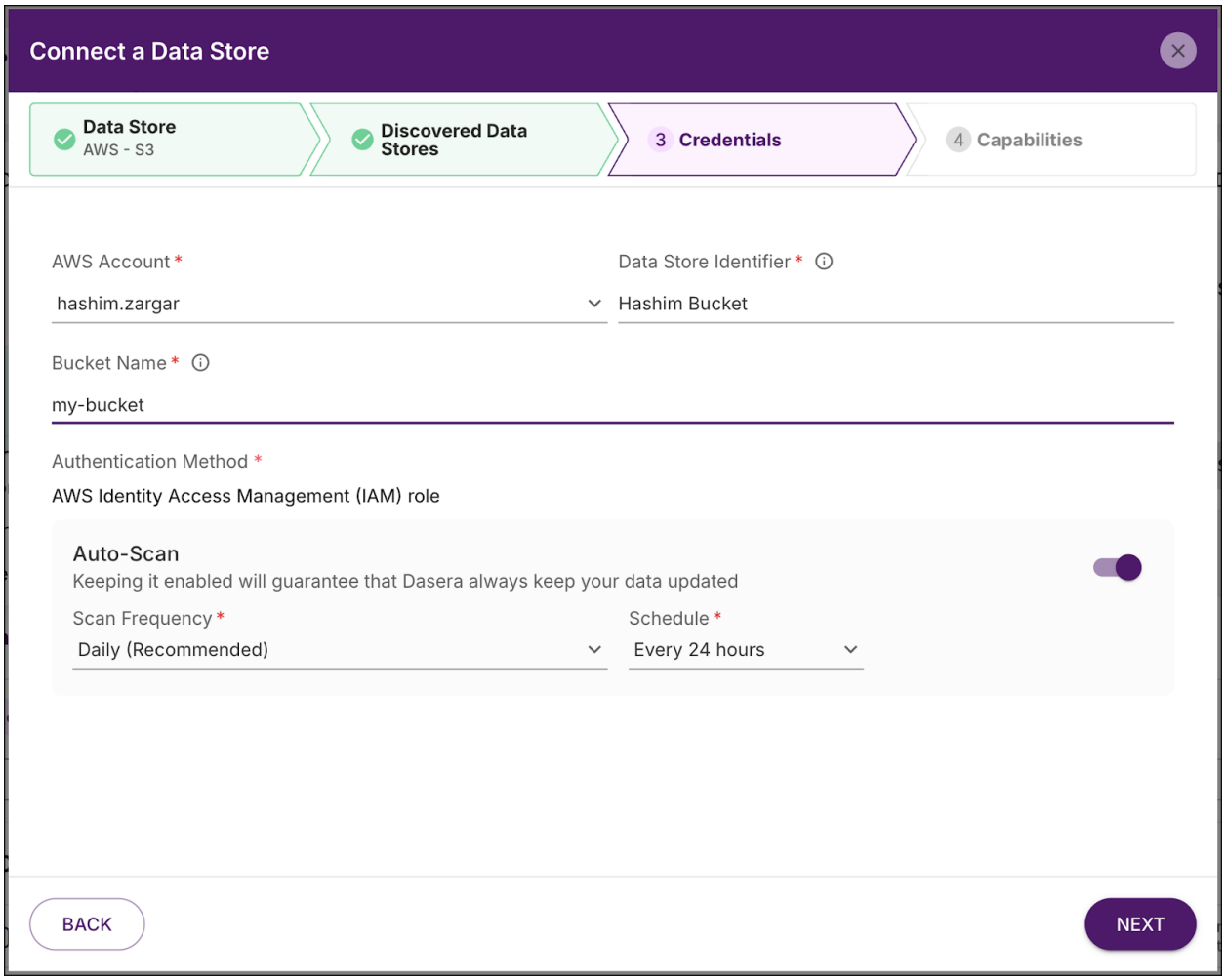
Connect a Data Store

Alternatively, you can connect to a data store and scan for vulnerabilities.

1. Under **Data Stores** > **Data Store Inventory**, click **Connect a Data Store**. Select the data store you want to connect to. The UI provides multiple data store options depending on the cloud service provider. Below is an example of AWS data stores, wherein we will connect to Amazon S3.

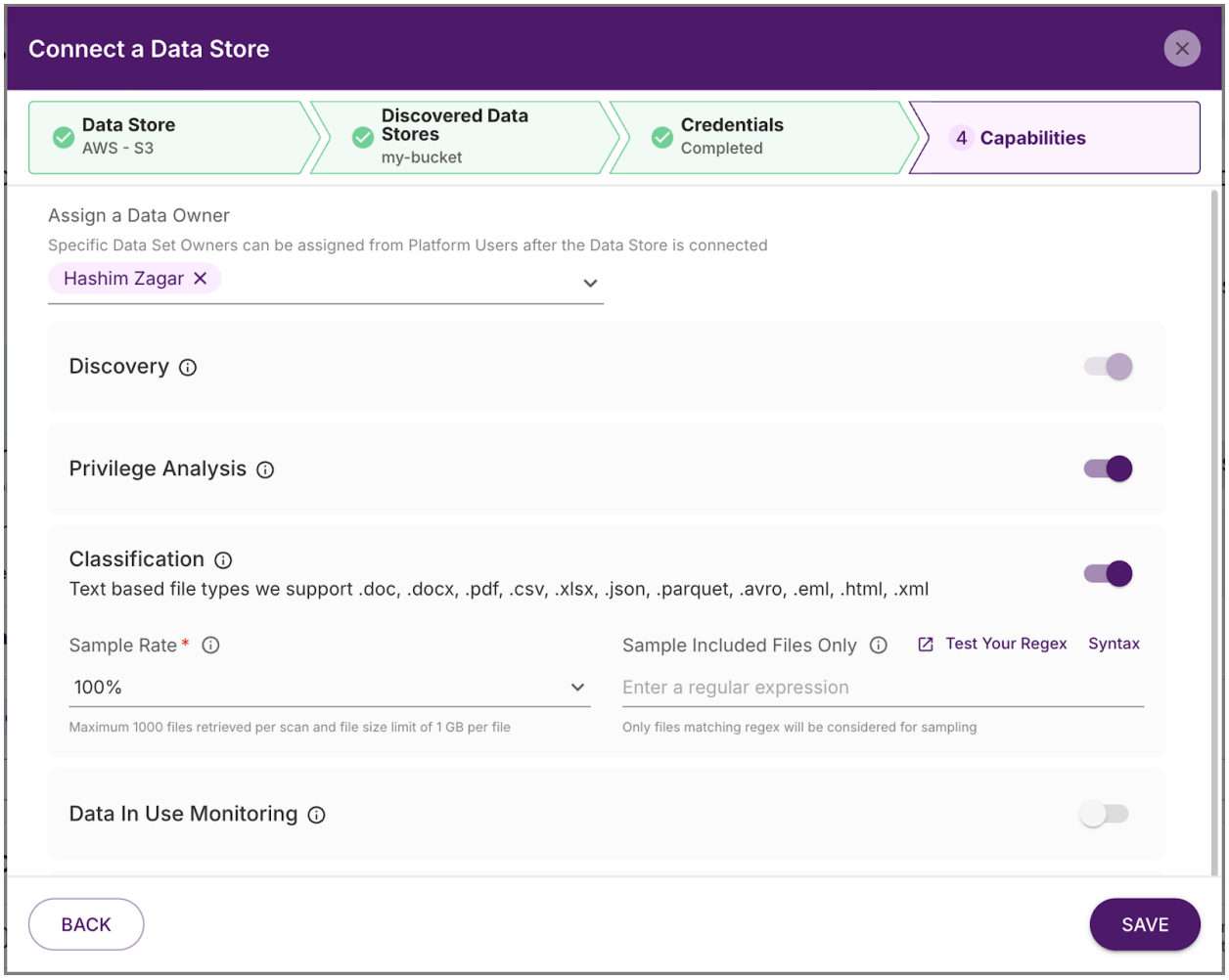


2. In the **Credentials** section, enter the data store identifier and the bucket name. You can also set the scan frequency and schedule. Click **Next.**



Field	Description
Data Store Identifier	Enter a human-readable name of the data store. The name can be any string that is used to identify the data store in the Dasera UI and in notifications.
Bucket Name	The S3 Storage bucket name that you wish to connect.

3. Assign the Data Owner and set the other components as required.

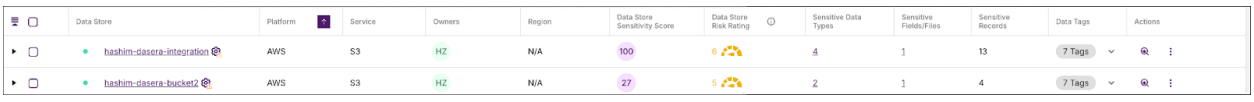


Connected Data Stores

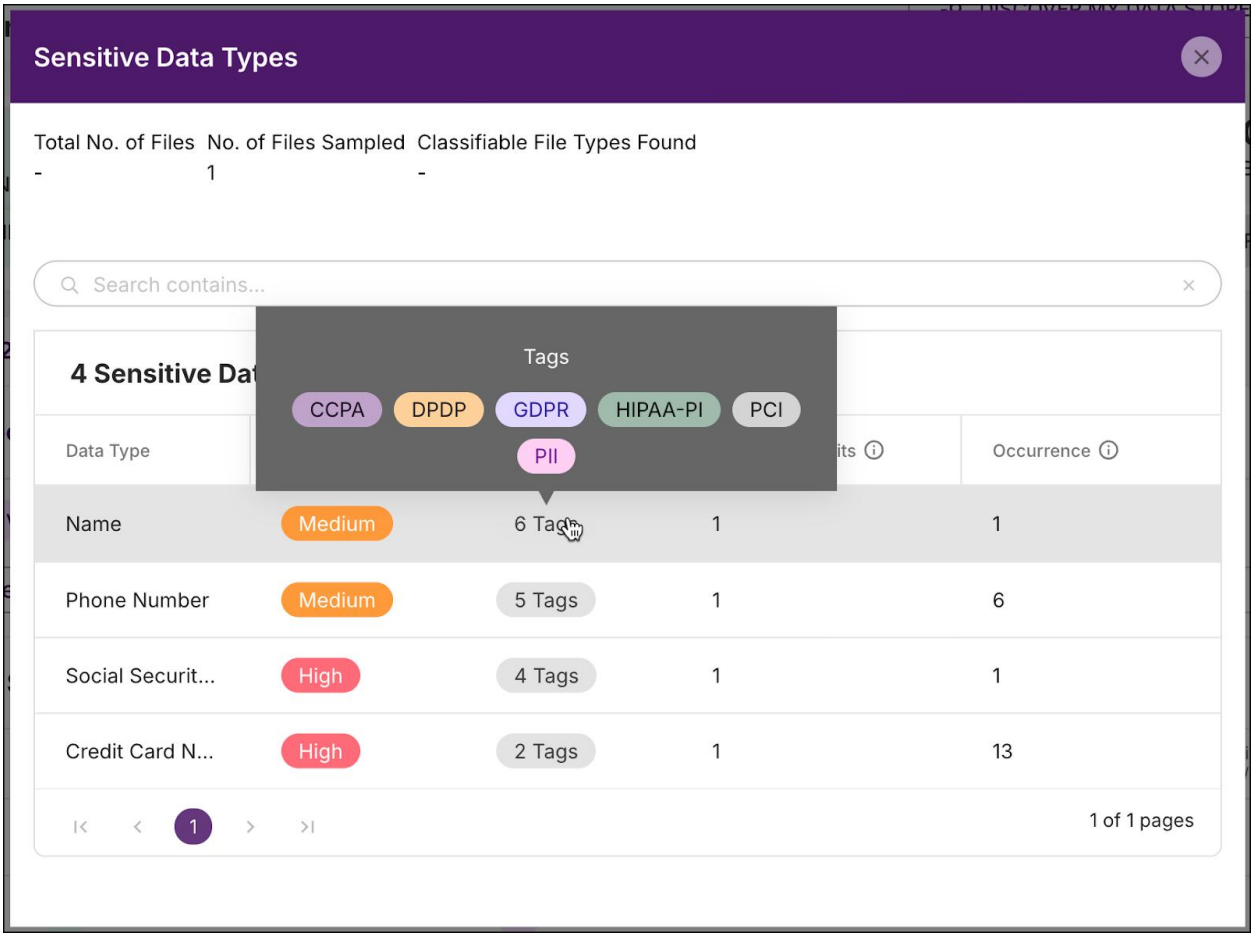
Once the data stores are connected, Dasera initiates a scan immediately. Depending on the frequency, the data stores are periodically scanned.

Under **Connected Data Stores**, you can check the scan status and other helpful information, such as **Sensitive Data Types** and **Data Tags**.

The below image is an example of the scanned data stores.



Clicking on the Sensitive Data Types value displays sensitive information about the data store. This information could include names, phone numbers, credit card details, etc. Hovering over the Data Tags displays the tags associated with the data type. These tags include HIPPA, PII, PCI, etc., indicating the regulatory compliance the datastore and its stored information should follow.



Cohesity Data Cloud

Register the Source

The source registered at Dasera, where the data stores are scanned for sensitive information, must also be registered at Cohesity.

Follow the steps in Register a Source to register the source at Cohesity.

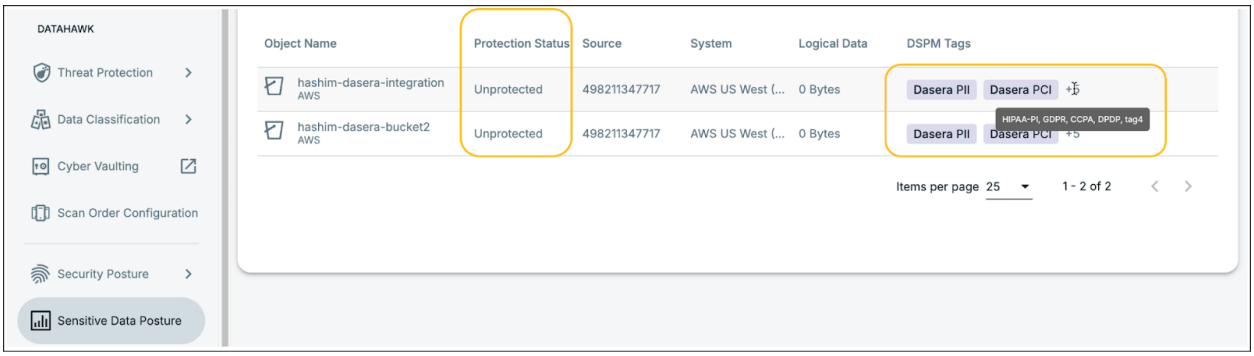
Analyze Sensitive Data

The Dasera DSPM tags applied to the data stores will be reflected in the Cohesity Data Cloud's Security Center. No further configuration is required at Cohesity Data Cloud. After scanning the data stores and applying appropriate tags at Dasera, Dasera tags will sync with Cohesity to accurately reflect the scan findings as DSPM tags in the Cohesity console.

Log in to the Cohesity Data Cloud and click **Security Center** under **Security**. In the Security Center, click **Sensitive Data Posture**.

In the Sensitive Data Posture, search for the data stores scanned at Dasera. These data stores will be reflected in the Sensitive Data Posture UI with their Protection Status and all the relevant tags pushed by Dasera DSPM.

In the example below, the two data stores with sensitive information are **Unprotected**. The IT backup administrators can prioritize protecting these data stores to adhere to regulations and compliance requirements and ensure they are backed up.



Take Corrective Action

Once the workloads containing sensitive data have been identified as Unprotected, the IT backup administrators should prioritize protecting these critical workloads. Add a workload to the Protection Group and select the appropriate protection policy to protect and back up the sensitive workload.

To protect Amazon S3 workloads, refer to Protect Your Amazon S3 Buckets.

Appendix

Dasera DSPM Overview

Dasera is a Data Security Posture Management (DSPM) platform that automates data security and governance controls, on-prem and in the cloud, to protect data throughout its journey. It provides visibility, control, and remediation for structured, semi-structured, and unstructured data across cloud and on-prem databases, data lakes, and data warehouses. With Dasera, you get robust Data Security Posture Management (DSPM), Data Access Governance (DAG), and Data Detection and Response (DDR), enhancing compliance and audit readiness.

Cohesity Data Cloud Overview

Cohesity Data Cloud is a unified platform for securing, managing, and extracting value from your data that reduces your attack surface, lowers costs, and minimizes risk. Cohesity Data Cloud is available as self-managed software and SaaS with rich features.

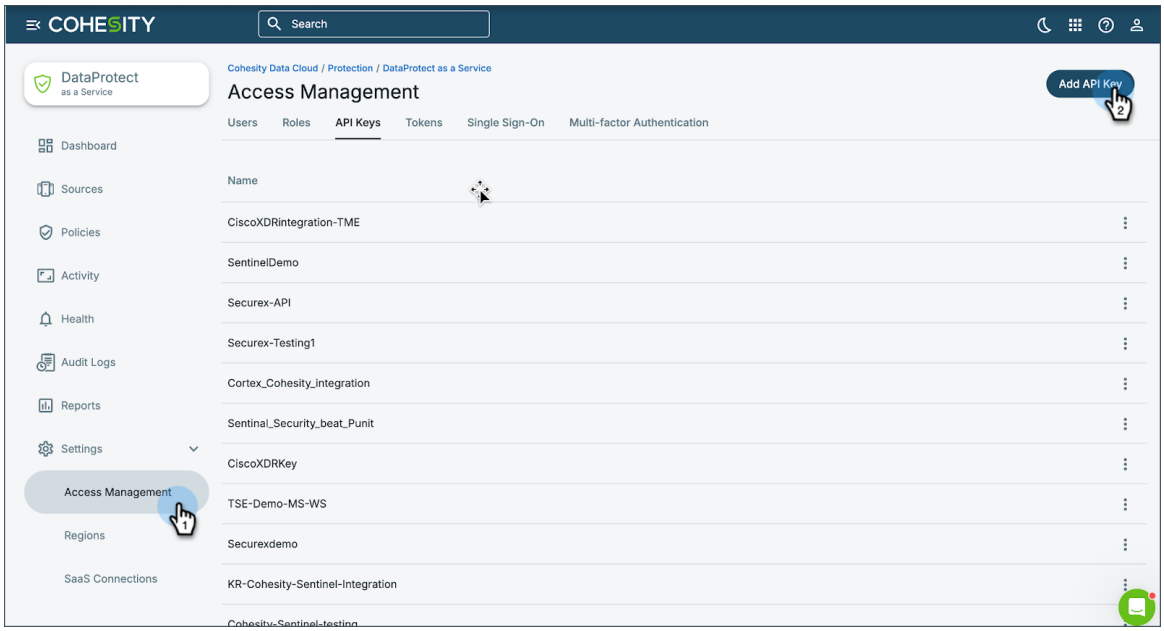
- **Modern Backup and Recovery**—The most comprehensive, modern, web-scale data management and backup and recovery solution to protect cloud-native, SaaS, and on-prem data at scale. You get instant recovery at scale and with direct metadata snapshots (so that each backup performs like a synthetic full), the ability to instantly put backed-up file shares online, and continuous data protection (CDP).
- **Traditional and Modern Workloads**—Support for VMs, databases, files, containers, cloud-native, SaaS, Storage, and traditional workloads.
- **Defend Against Ransomware Attacks**—Multilayered security architecture with Zero Trust Security, including granular RBAC, MFA, SSO, immutable snapshots, and ML-based ransomware attack detection. Protect and recover against ransomware with threat protection, cyber vaulting, and ML-powered data classification.
- **Threat Protection and Data Classification**—Highly curated and managed threat feeds, trained with ML, threat detection and response to your specific needs by augmenting the extensive library of over 117,000 behavioral patterns, create multiple YARA rules defining Indicators of Compromise (IOC), or import custom rules. Highly accurate NLP and ML-based engines classify sensitive data, automatically or on-demand, including personally identifiable information (PII), PCI, and HIPAA.
- **Global Search and Unified Management**—Reduce recovery point objectives to minutes by eliminating slow-to-access, chain-based backups. A single management platform offering multilayered security architecture, unifying operations with integrated solutions for backup, CDP, DR, search, ransomware attack detection, and vulnerability scanning into a single scalable environment.
- **Cloud Vault**—Cohesity FortKnox is a SaaS cyber vaulting and recovery solution that provides your data with additional layers of managed security and protection against cybersecurity threats. To learn more, refer to Cohesity product documentation.

- **Cloud Archive**—Policy-based data archival to meet long-term data retention, compliance, and regulatory requirements.
- **Cohesity Cloud Services**—Cohesity-managed data security and management with SaaS that runs multiple cloud data services, including backup, cyber vaulting, threat defense, data classification, DR, and more on a single multi-cloud platform.
- **Cohesity Gaia**—combines generative AI with your enterprise data. Unlock data insights by bringing retrieval augmented generation (RAG) AI and large language models (LLMs) to enterprise data within Cohesity. Ask natural language questions and get context-rich answers.
- **Business Continuity**—Simplify business continuity and disaster recovery with automated failover and failback orchestration for your mission-critical workloads. Get your critical applications online after a breach or outage through automated orchestration.
- **Security Integrations**—Cohesity integrates with leading perimeter and end-point security vendors, giving you greater visibility and actionable alerts in your Security Operations Center (SOC).
- **Deployment**—Software-defined solution for on-premises, public cloud, backup as a service, and edge sites.
- **API-first Extensibility**—Derive business insights with the Cohesity Marketplace partner ecosystem. Streamline operations and easily integrate on-prem and cloud environments with pre-built automated workflows and API integrations.

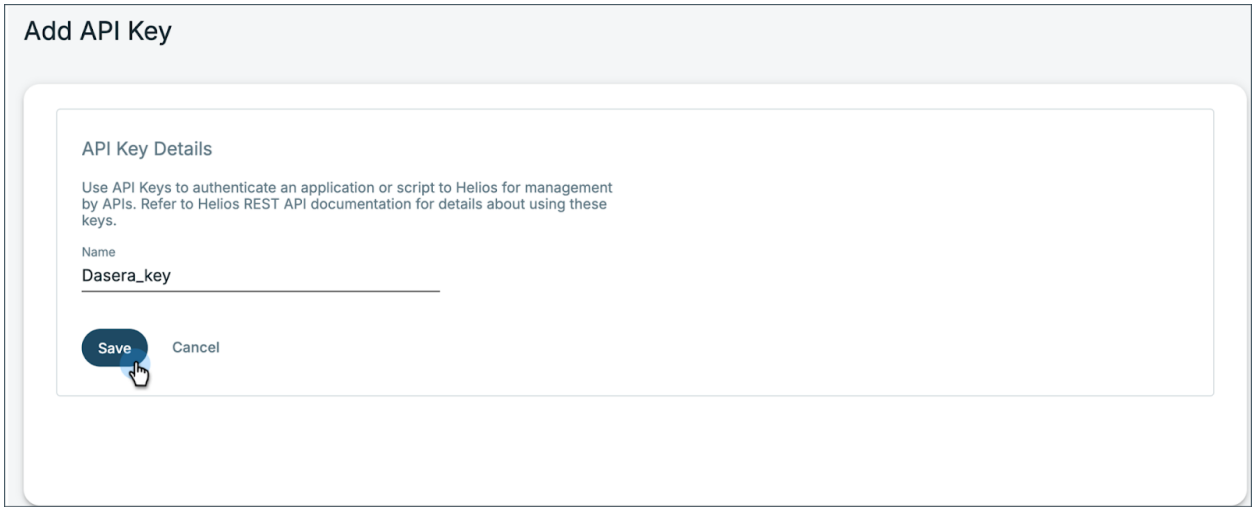
To learn more about how Cohesity provides **AI-powered data security and management**, refer to Cohesity.com.

How to Fetch API Keys from Cohesity Data Cloud

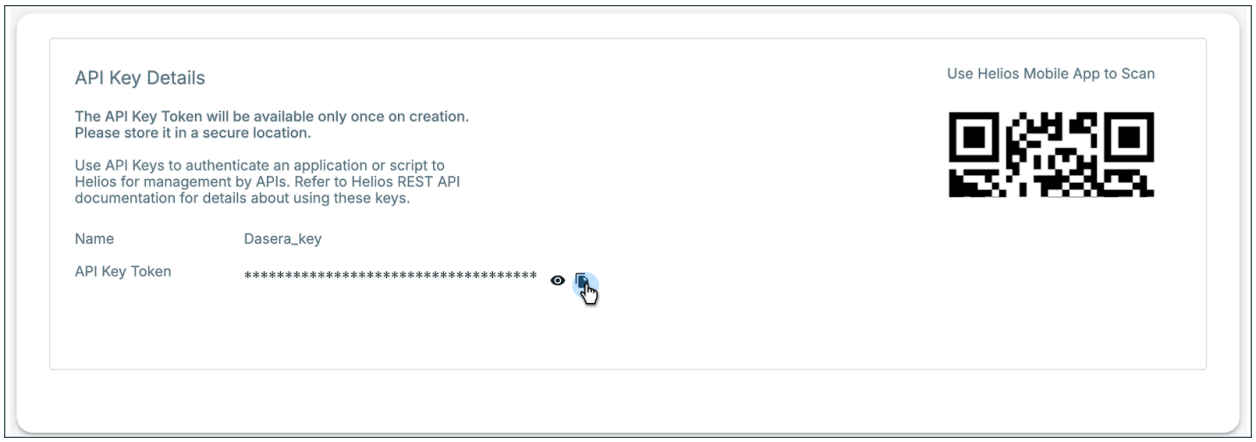
1. In Cohesity DataProtect as a Service, go to **Settings** > **Access Management** > **Add API Key** to generate API Keys.



2. Name the API key for identification in the **Add API Key** menu and click **Save**.



3. Copy the API Key and keep it safe for future use.



Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Security Center of Excellence Team – Focuses on Cohesity Security solutions and integrations.

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.1	Aug 2025	Republished with latest template
1.0	Oct 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.