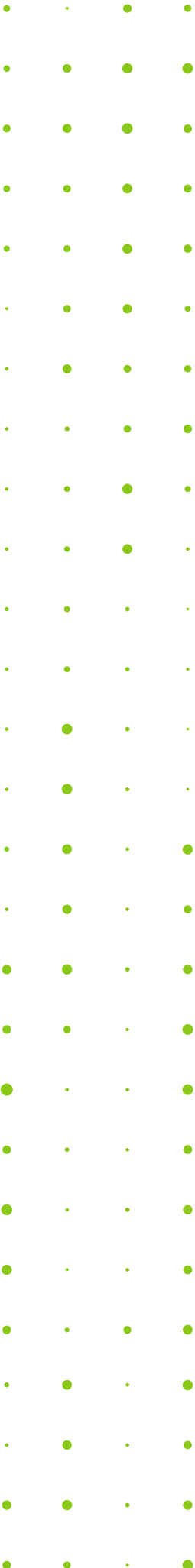


# COHESITY

## DataProtect as a Service for Government (FedRAMP) User Guide

September 19, 2024



© 2024 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, DataHawk, 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.

No part of this documentation or any related software may be reproduced, stored, transmitted, or otherwise distributed in any form or by any means (electronic or otherwise) for any purpose other than the purchaser's personal use without the prior written consent of Cohesity, Inc. You may not use, modify, perform or display this documentation or any related software for any purpose except as expressly set forth in a separate written agreement executed by Cohesity, Inc., and any other use (including without limitation for the reverse engineering of such software or creating compatible software or derivative works) is prohibited, except to the extent such restrictions are prohibited by applicable law.

**Published on September 19, 2024**

# Contents

Cohesity DataProtect as a Service for Government (FedRAMP) .....	5
Supported Software for DataProtect as a Service for Government (FedRAMP) .....	6
Microsoft 365 Editions .....	6
Supported Workloads and GovCloud Regions .....	8
Supported Workloads and Cloud Providers .....	8
Get Started .....	9
Sign in to Cohesity DataProtect Delivered-as-a-Service for Government (FedRAMP) .....	9
Select Regions and Encryption Key Management System .....	10
Add Users .....	12
Register a Source .....	14
Protect a Source .....	14
Recovery Options .....	14
Access Management .....	16
Manage Users & Groups .....	16
Add a Single Sign-on Provider .....	18
Add API Keys .....	48
Policies .....	50
Create a Policy .....	50
Microsoft 365 .....	52
Microsoft 365 Requirements .....	52
Register Microsoft 365 Sources .....	71
Explore Microsoft 365 Sources .....	79
Exchange Online Mailboxes .....	81
OneDrive for Business .....	101
SharePoint Online .....	111
Microsoft Teams .....	121
Microsoft Groups .....	133
Monitoring .....	140
Reports .....	140
Detect Ransomware Attacks .....	158
Alerts .....	159
Audit Logs .....	179

How-To Videos .....	185
Cohesity Support .....	186
Reach Cohesity Support .....	186
Support/Service Assistance .....	186
Cohesity Software Running on Partner Hardware .....	187

# Cohesity DataProtect as a Service for Government (FedRAMP)

Today's companies and organizations are overwhelmed with the exponential growth in the amount of data they collect, manage, and store. You need to be able to focus on managing your data without worrying about additional hardware in your data center.

We designed Cohesity Helios for Government (FedRAMP) as a platform to provide enterprise-ready Data Management-as-a-Service (DMaaS) by hosting a series of Software-as-a-Service (SaaS) applications for data management. The first in the series is Cohesity DataProtect as a Service for Government (FedRAMP), Cohesity's SaaS offering that provides protection for your virtual and physical workloads, databases, and applications. You can sign up and start backing up your data today.

Log in to Cohesity DataProtect as a Service for Government (FedRAMP) to protect data from your data center and SaaS applications in just a few steps:

1. Select a GovCloud region for your backups.
2. Register a source.
3. Select the objects on that source to protect.
4. Protect those objects.

# Supported Software for DataProtect as a Service for Government (FedRAMP)

DataProtect as a Service for Government (FedRAMP) supports the protection of Microsoft 365.

## Microsoft 365 Editions

The following table lists the Microsoft 365 editions DataProtect as a Service for Government (FedRAMP) supports:

**Note:** DataProtect as a Service for Government (FedRAMP) does not support GCC High.

Microsoft Plans	Editions
Microsoft 365 For Business	<ul style="list-style-type: none"> <li>• Microsoft 365 Business Basic</li> <li>• Microsoft 365 Business Standard</li> <li>• Microsoft 365 Business Premium</li> </ul>
Microsoft 365 For Enterprise	<ul style="list-style-type: none"> <li>• Microsoft 365 E3</li> <li>• Microsoft 365 E5</li> <li>• Microsoft 365 F3</li> </ul>
Office 365 For Enterprise	<ul style="list-style-type: none"> <li>• Office 365 E1</li> <li>• Office 365 E3</li> <li>• Office 365 E5</li> </ul>

Microsoft Plans	Editions
Microsoft 365 GCC (Government Community Cloud)	<ul style="list-style-type: none"><li data-bbox="813 289 1071 352">• Office 365 Government G1</li><li data-bbox="813 380 1071 443">• Office 365 Government G3</li><li data-bbox="813 470 1071 533">• Office 365 Government G5</li><li data-bbox="813 560 1000 623">• Microsoft 365 Government G3</li><li data-bbox="813 651 1000 714">• Microsoft 365 Government G5</li><li data-bbox="813 741 976 762">• Office 365 F3</li></ul>

# Supported Workloads and GovCloud Regions

You can use Cohesity DataProtect as a Service for Government (FedRAMP) to store your backups on the Cohesity-managed SaaS platform in the AWS GovCloud (US-East) region.

## Supported Workloads and Cloud Providers

The following table lists the supported workloads on AWS GovCloud (US-East) region:

Cloud Provider	Supported Workloads
AWS GovCloud	Microsoft 365 (Exchange, OneDrive, SharePoint, Groups, and Teams)



# Get Started

To get started:

1. [Sign in to Cohesity Helios for Government \(FedRAMP\)](#) that has Cohesity DataProtect as a Service for Government (FedRAMP) enabled.
2. [Select a cloud region for your backups and choose a Key Management System](#) for your data encryption.
3. [Register](#) your source.
4. Select the objects on that source to protect.
5. [Protect](#) those objects.

## Sign in to Cohesity DataProtect Delivered-as-a-Service for Government (FedRAMP)

To sign in to Cohesity DataProtect Delivered-as-a-Service for Government (FedRAMP), perform the following steps:

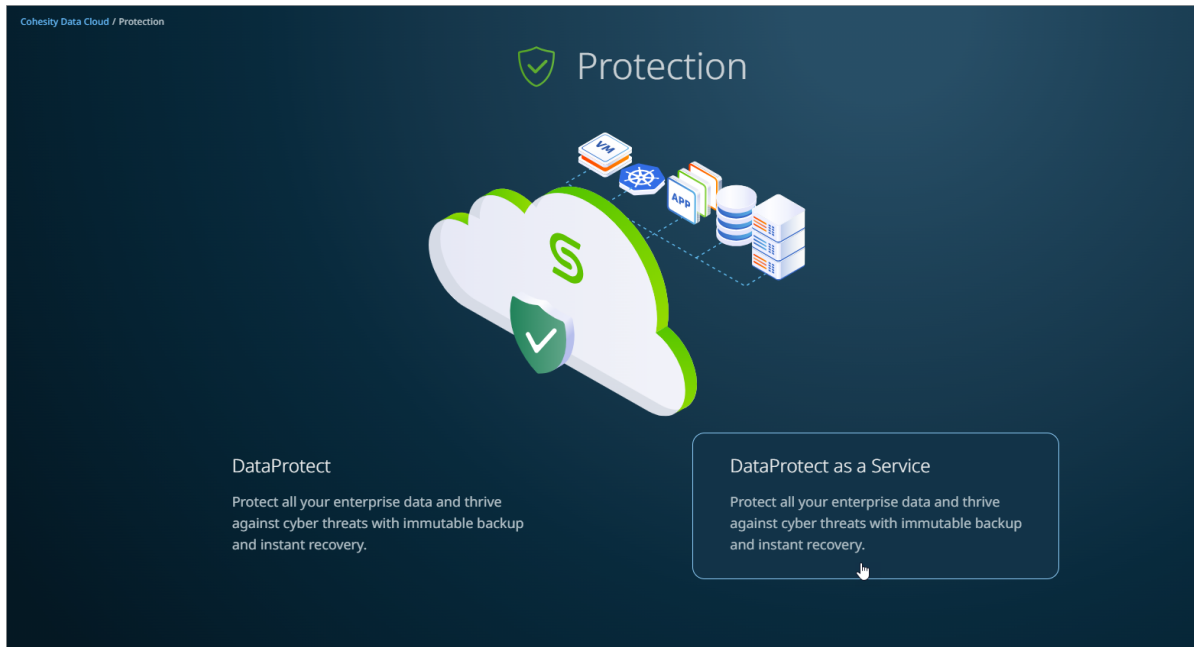
1. Log in to [Cohesity Helios for Government \(FedRAMP\)](#).

You must use the Salesforce credentials provided in your welcome email for your initial access to Cohesity Helios for Government (FedRAMP).

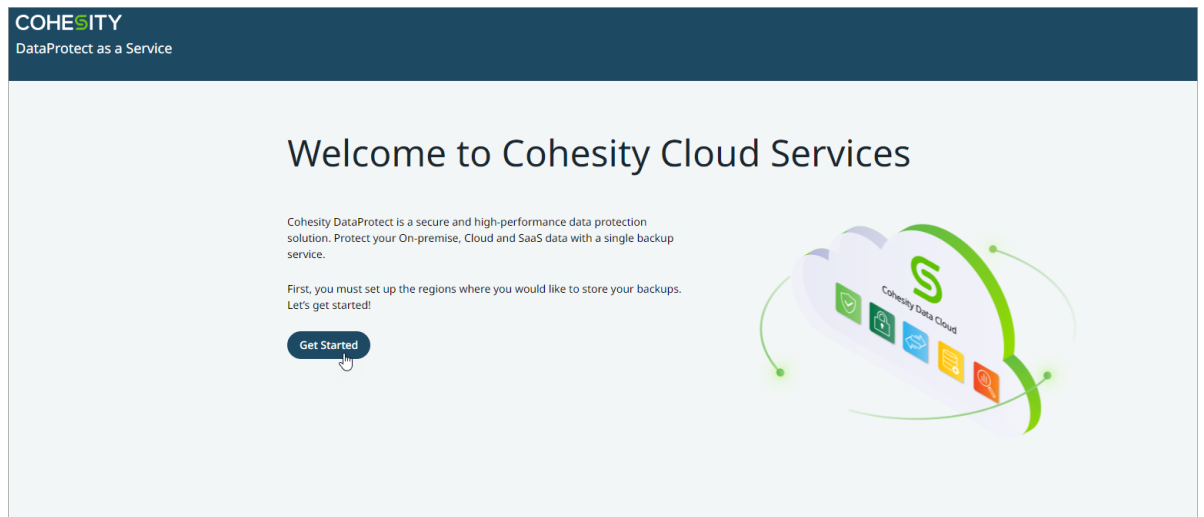
**Note:** Once logged in to Cohesity Helios for Government (FedRAMP) with your Salesforce credentials, configure Single-Sign-on (SSO) access for users using Identity Provider (IdP), such as AD FS, Okta, and Azure. Ensure to assign the Super Admin role to at least two SSO-configured users. Your Salesforce credentials will be deactivated after successfully configuring SSO for users with the Super Admin role. However, you can still utilize them to open Cohesity Support cases. For more information, see [Add Users](#).

You will be redirected to Cohesity Data Cloud.

2. On the **Cohesity Data Cloud** landing page, click the **Protection** solution area and then select **DataProtect as a Service**.



On the **Welcome to Cohesity Cloud Services** page, click **Get Started** to protect data sources from your data center and SaaS applications.

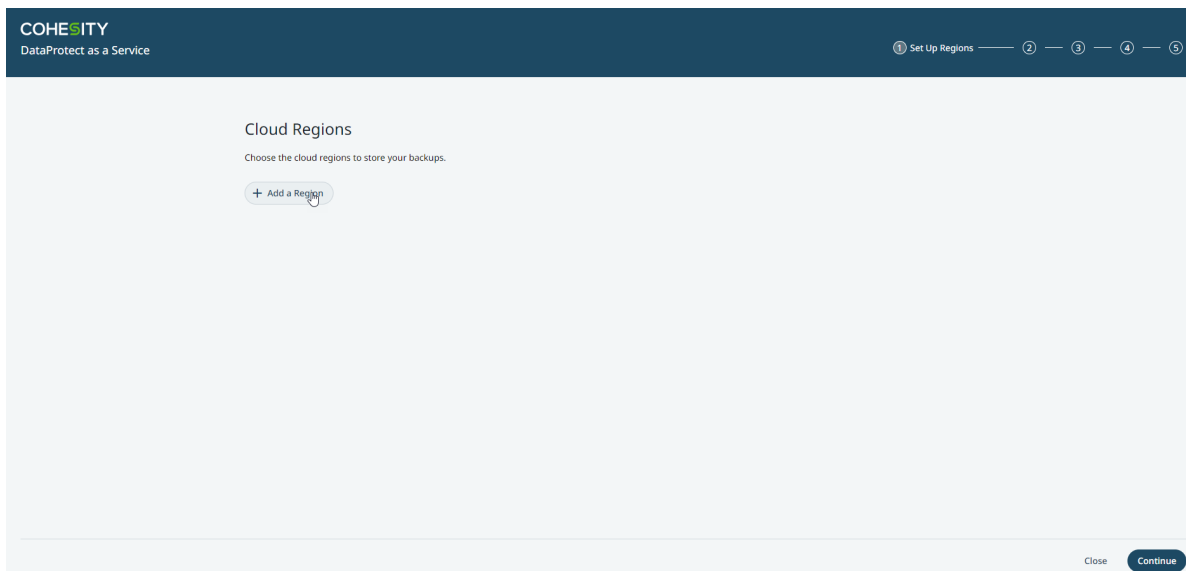


Select **No**, if you are protecting SaaS workloads like Microsoft 365. And, click **Continue**.

## Select Regions and Encryption Key Management System

Before you can use Cohesity DataProtect as a Service for Government (FedRAMP), you need to choose at least one cloud region for your data backups. Currently, Cohesity supports the US-Gov-East region.

1. On the **Cloud Regions** page, click **Add a Region**.



2. From the **Set Up Region** dialog, select the **US-Gov-East** as the region for your data backups and choose the **encryption option**. For more information on the encryption options, see [Select Regions and Encryption Key Management System](#).
3. Once the cloud region is provisioned, click **Continue**.

## Choose Key Management System (KMS)

In Cohesity DataProtect as a Service for Government (FedRAMP), all the data is encrypted both in flight and at rest. Cohesity uses AWS Key Management System for at-rest data encryption and provides customers a choice between Cohesity- and self-managed keys:

- **Cohesity KMS.** Cohesity generates and uses unique AWS encryption keys (known as Customer Master Keys in AWS) for each customer to encrypt their data.
- **Self-Managed KMS.** You can also use your own AWS encryption keys (Customer Master Keys) instead. To use your own AWS KMS:
  1. You provide the CMK Amazon Resource Name (ARN) for the cloud region you selected.
  2. Cohesity generates the JSON for a key policy document that allows the DCohesity DataProtect as a Service for Government (FedRAMP) to make API calls to your CMK.
  3. You add the generated JSON contents to your AWS CMK's Policy in your AWS account.

The permissions required by the Cohesity DataProtect as a Service for Government (FedRAMP) are:

- kms:Encrypt
- kms:Decrypt
- kms:ReEncrypt\*
- kms:GenerateDataKey\*
- kms:DescribeKey

**Important:** If you choose this option, you are responsible for ensuring that your CMK is not deleted, as that would lead to data stored in Cohesity DataProtect to become unrecoverable.

With this option, you can audit the access calls made to your CMK to find important information, including when the CMK was used, the operation that was requested, the identity of the requester, and the source IP address. For more, see [Logging AWS KMS API calls with AWS CloudTrail](#) and [What Is AWS CloudTrail?](#) in the AWS documentation.

Note that you can also revoke CMK access to Cohesity at any time, after which Cohesity cannot decrypt the data stored in Cohesity DataProtect and all backup & recovery operations will fail.

In both options, Cohesity uses AES-256 encryption keys called DEKs (Data Encryption Keys) to encrypt the data at rest. DEKs are generated using the AWS CMK and rotated every 4 hours. The Data Encryption Key is encrypted with AWS CMK and stored along with the data — it is never stored in plain text.

**Note:** Once you choose a KMS, you cannot change that choice.

**Next >** You're all set up and ready to [register your sources!](#)

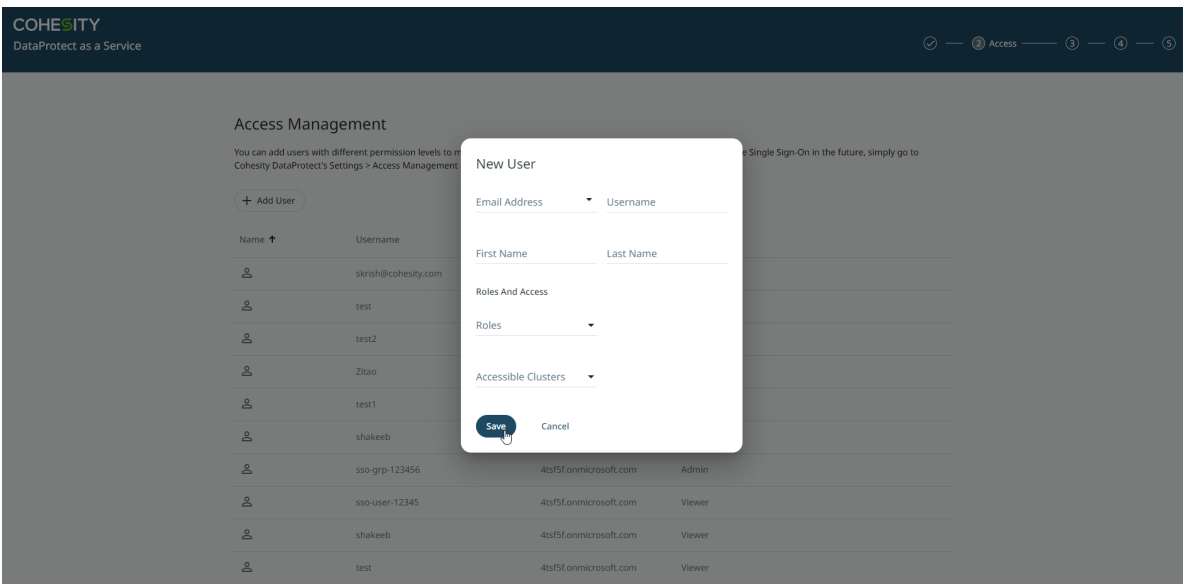
## Add Users

To manage user access to your DataProtect as a Service for Government (FedRAMP), we recommend that you add users. Once you create them, your users can start using your DataProtect as a Service for Government (FedRAMP) with their own logins. You can add users with different permission levels to manage your environment. For more information, see [Access Management](#).

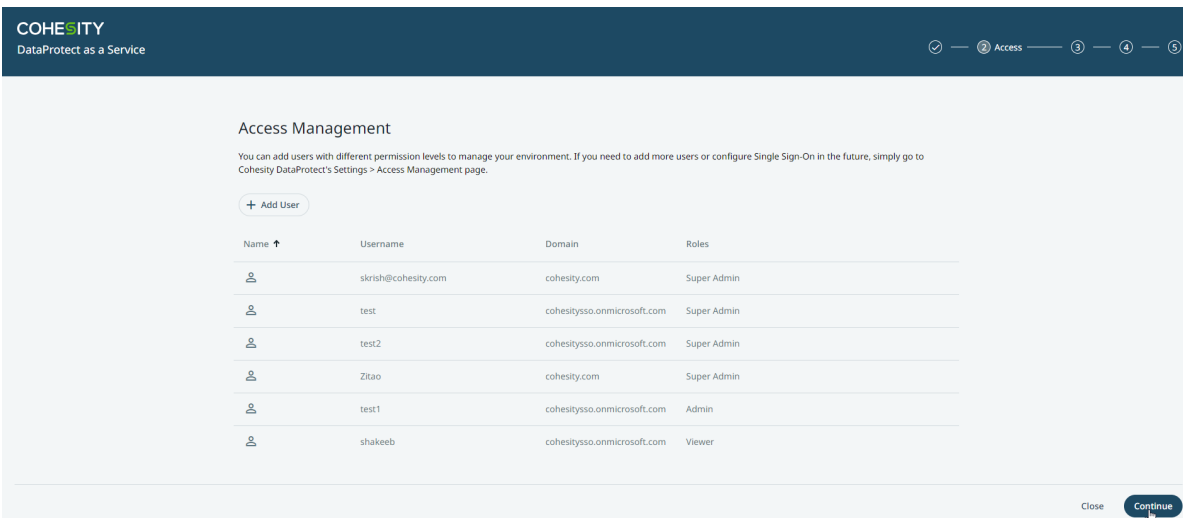
On the **Access Management** page, click **Add User** to add users.

On the **New User** dialog, perform the following:

1. Enter the following details:
  - **Username.** The user's email address.
  - **Email Address.** The user's email address again.
  - **First Name.** The user's first name in DataProtect as a Service for Government (FedRAMP).
  - **Last Name.** Typically, the domain of your email address.
2. Under **Roles and Access**, assign an appropriate **Role** to this user and select the **Clusters** that this user can access. See [Roles](#) for more information.
3. Click **Save**.



Once you have added the users, click **Continue**.



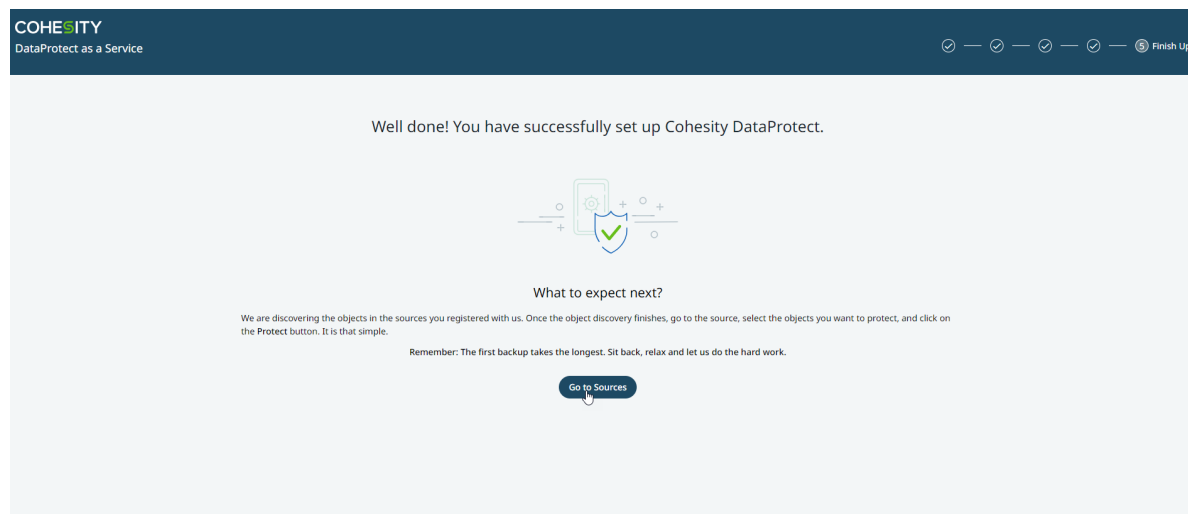
## Register a Source

To start protecting your data, register your data sources. On the **Sources** page, click **Register Source** to register your data sources.

Select your data source on the **Select Source** dialog, and click **Start Registration**.

Currently DataProtect as a Service for Government (FedRAMP) supports the protection [Microsoft 365](#).

After you have registered your data sources, click **Continue**. Then, click **Go to Sources** to start protecting your data sources.



## Protect a Source

Once you have registered a source in DataProtect as a Service for Government (FedRAMP), you can start protecting the objects, volumes, and files in that source. For detailed instructions, see the Workload Type: [Microsoft 365](#).

## Recovery Options

Depending on the Microsoft 365 applications you have protected, you can recover the following:

- [Recover User Mailboxes](#)
- [Recover Mailbox Items](#)
- [Mailbox Items Recovery Self-Service](#)
- [Recover User OneDrives](#)
- [Recover OneDrive Contents](#)
- [OneDrive Content Recovery Self-Service](#)

- [Recover SharePoint Sites](#)
- [Recover SharePoint Document Library Items](#)
- [Recover Microsoft 365 Teams](#)
- [Recover Microsoft 365 Teams Content](#)
- [Recover Groups](#)

# Access Management

On logging into DataProtect as a Service for Government (FedRAMP), the admin can add other users, define roles, specify cluster access, and generate API keys to access . To manage users, roles, and define their access, in the Helios dashboard, navigate to **Settings > Access Management**.

## Manage Users & Groups

To manage user access to your DataProtect as a Service for Government (FedRAMP), we recommend that you add users and groups. Once you create them, your users can start using your DataProtect as a Service for Government (FedRAMP) with their own logins.

### Add Users

To add a user:

1. In **DataProtect as a Service**, navigate to **Settings > Access Management** and click the **Users** tab.
2. Click **Add User**.

**Note:** Only the user with Admin privileges will be able to add a new user.

3. In the dialog, select **Add User** and enter:
  - **Username.** The user's email address.
  - **Email Address.** The user's email address again.
  - **First Name.** The user's first name in DataProtect as a Service for Government (FedRAMP).
  - **Last Name.** Typically, the domain of your email address.
4. Under **Roles and Access**, assign an appropriate **Role** to this user. See [Roles](#) for more information.
5. Click **Save**.

The new user receives a welcome email with a link to reset their password, and appears in the list on the **Users** tab. From there, you can edit or delete the user, or prompt them to reset their password.



## Roles

Roles	Description
Cohesity Support Admin	This role allows Cohesity Support to create a Super Admin user for the customer. Only Cohesity Support has access to this role, and it is typically used when the customer has lost access to a Super Admin user due to turnover and other events.
Data Security	Data Security users have Self Service Data Protection role privileges and can create DataLock Views and set DataLock expiration dates.
High Classified	User who has High classified role can fetch cluster details needed for specific API calls.
Operator	Operator users have Viewer role privileges and can run existing Protection Groups and create Recover Tasks.
SMB Backup Operator	SMB Backup Operators have privilege to perform SMB backup and SMB restore.
Super Admin	Super Admin users have full access to all actions and workflows within the Cohesity Dashboard. They can manage other Super admins and admins.
Viewer	Viewer users have read-only access for all workflows within the Cohesity Dashboard.

## Manage Users

To change a user's settings, click the Actions menu (: ) next to the user and select:

- **Edit.** To update their Email Address, First Name, and/or Last Name.
- **Delete.** To delete the user from your DataProtect as a Service for Government (FedRAMP).
- **Reset Password.** To send the user an email with a link to reset their password.

## Change Password

To change your DataProtect as a Service for Government (FedRAMP) password:

1. In **DataProtect as a Service**, navigate to **Settings > Access Management** and click the user to open the User Details page.
2. Click **Reset Password** and follow the prompts.

## Add SSO Users & Groups

If you have added Single Sign-on (SSO) to DataProtect as a Service for Government (FedRAMP), you can add users and groups from your SSO domain for additional user management.

To add SSO users and groups:

1. In **DataProtect as a Service**, navigate to **Settings > Access Management**.
2. Click **Add User** on the **Users** tab.
3. In the dialog, select **Add SSO Users & Groups** and enter:
  - **SSO Domain**. The domain you used to add SSO.
  - **SSO Users**. The users in your SSO domain who need access to DataProtect as a Service for Government (FedRAMP).
  - **SSO Groups**. The groups in your SSO domain who need access DataProtect as a Service for Government (FedRAMP).
4. Click **Save**.

The new SSO users and groups you entered appear in the list on the **Users** tab. To group them, click the **Domain** column sort them by your SSO domain.

Click the **Actions** menu (: ) next to the SSO user or group to **Edit** or **Delete** them.

## Add a Single Sign-on Provider

You can now configure DataProtect as a Service for Government (FedRAMP) to use an Identity Provider (IdP), such as Okta, for single sign-on (SSO) access. DataProtect as a Service for Government (FedRAMP) must be added as an application to your IdP such as Okta. The SSO must then be configured along with the SSO URL and certificate file in DataProtect as a Service for Government (FedRAMP). After the integration, users can sign in to DataProtect as a Service for Government (FedRAMP) using either the IdP sign in page or sign in with the SSO link in the DataProtect as a Service for Government (FedRAMP) login page.

The following identity providers are supported:

Identity Provider	Documentation Link
Active Directory Federation Services (AD FS)	<a href="#">Configure SSO with Active Directory Federation Services (AD FS)</a>
Azure	<a href="#">Configure SSO with Azure</a>
Duo Single Sign-on	<a href="#">Integration with Duo for SSO</a>

Identity Provider	Documentation Link
Ping Identity	<a href="#">Integration with Ping Identity for SSO</a>
Okta Single Sign-on	<a href="#">Configure SSO with Okta</a>

## Configure SSO

To configure SSO:

1. In **DataProtect as a Service**, navigate to **Settings > Access Management > Single Sign-On**.
2. Click **Configure SSO**.
3. Select one of the following options:
  - **SAML**: Security Assertion Markup Language (SAML) is an XML-based protocol used for SSO login.
  - **OpenID Connect**: OpenID Connect is an open authentication protocol that uses OAuth2.0 framework.
4. If you select **SAML**, then refer to the following table:

Name	Description
<b>SSO Domain</b>	<p>Unique domain name that will differentiate this IdP from others. As DataProtect as a Service for Government (FedRAMP) 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 <code>username@SSO_DOMAIN</code>.</p> <p>When a user logs in to DataProtect as a Service for Government (FedRAMP) using SSO and enters the email address as <code>foo@bar.com</code>, DataProtect as a Service for Government (FedRAMP) looks for the IdP that has the SSO Domain configured as <code>bar.com</code> and redirects this user <code>foo</code> to the matching IdP. This is how DataProtect as a Service for Government (FedRAMP) determines which IdP the user needs to be forwarded to.</p>
<b>SSO Provider</b>	<p>From the drop-down, select the SSO provider name of your choice. Select the <b>I have read the SSO documentation provided by &lt;SSO provider name&gt;</b> check box. Cohesity recommends reading the SSO documentation before proceeding to the next step.</p>
<b>Assign to Organization</b>	<p>Optional. In a multitenant-enabled cluster, you can configure SSO for an organization that has been added to the Cohesity cluster. Select an organization from the drop-down.</p>

Name	Description
<b>Single Sign-on URL</b>	Paste the URL that you copied from your IdP.
<b>Provider Issuer ID</b>	Paste the issuer ID that you copied from your IdP.
<b>X.509 Certificate</b>	Click <b>Select File</b> and browse to the location to select the file that you downloaded and renamed previously.

5. If you select **OpenID Connect (OIDC)**, perform the following steps and then refer to the table:

**Prerequisites:**

1. Create the OIDC app within your Identity Provider (IdP). For more information, see [Create OIDC app integrations](#).

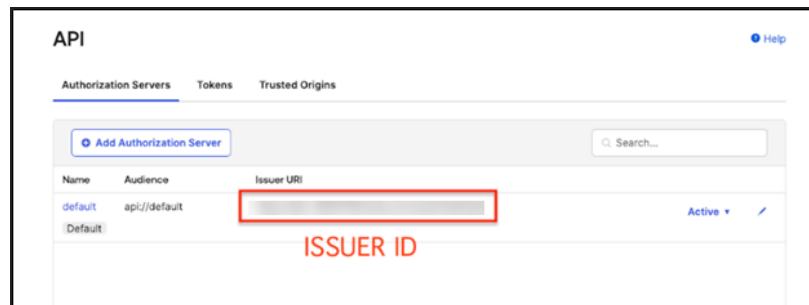
**Note:** OIDC is an open standard and Single-Sign On with DataProtect as a Service for Government (FedRAMP) is intended to work with any OpenID Connect supported Identity Provider. For setup details, refer to your Identity Provider's documentation.

2. Map the OIDC configuration details from Okta IDP to DataProtect as a Service for Government (FedRAMP) side configurations:

1. To get the Issuer ID:

1. Navigate to **Security > API**.
2. On the **API** page, click **Authorization Servers**.

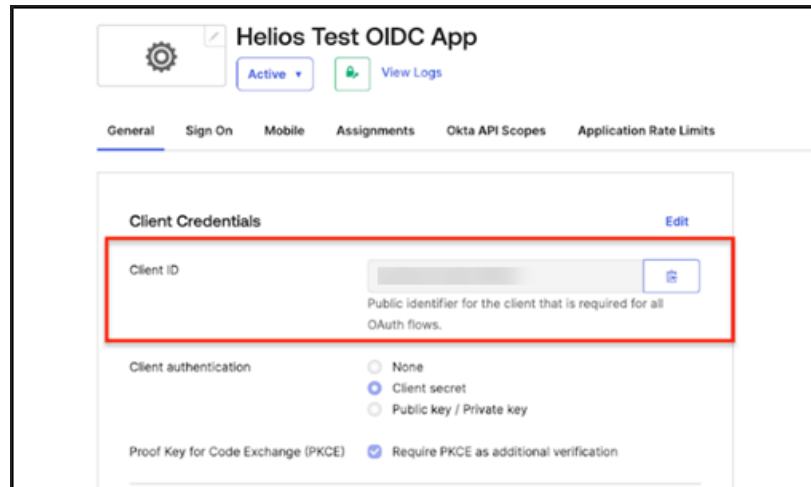
You can find the issuer ID in the Issuer URI section.



2. To get the Client ID:

1. Navigate to Applications.
2. On the Helios Test OIDC App page, click **General**.

You can find the Client ID in the Client Credentials window.



3. To generate the **JSON Web Key Set (JWKS)** URL:

1. Construct the URL as follows:

Format: <issuer ID>/well-known/openid-configuration

For example: `https://***-`

`00000000.okta.com/oauth2/default/.well-known/openid-configuration.`

2. Enter the constructed URL in the address bar of the browser and JSON output will be displayed.

Name	Description
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.

Name	Description
<b>Public Key Expiration (Seconds)</b>	Specifies the time in seconds before which Cohesity starts fetching for new public keys from the identity provider. The default value is 86400 seconds (24 hours).
<b>Public Key Refresh Interval (Seconds)</b>	Specifies the cache refresh interval in seconds to limit the requests to the OIDC server and also to refresh the public key, in case of token signature validation failure. The default value is 600 seconds (10 minutes).
<b>Token Validity (Seconds)</b>	Specifies the validity time in seconds for the token. The validity check is done only if the token is not expired. If it's expired, then the 401 unauthorized or invalid token error is displayed. The default value is 15 minutes.

6. Enter the following details:

Name	Description
<b>Default Role for all SSO Users</b>	Select a role to use as the default role for users signing on with SSO. Typically, you would select this option only during the initial SSO configuration. You can change this option later.
<b>Access to All Clusters or Limited Clusters</b>	Select if the identity provider users can have access to all clusters or limited clusters.

Name	Description
<p><b>Sign Auth Request</b></p>	<p>Optional. Enable this option if you want authorization requests to be signed with the DataProtect as a Service for Government (FedRAMP) public key. The DataProtect as a Service for Government (FedRAMP) public key must be uploaded to the IdP site.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> This option is not available if you select the OpenID Connect protocol.</p> </div> <p>Perform the following steps to obtain the DataProtect as a Service for Government (FedRAMP) public certificate:</p> <ol style="list-style-type: none"> <li>1. Log in to DataProtect as a Service for Government (FedRAMP).</li> <li>2. Start a browser and enter <a href="https://helios.cohesity.com/v2/mcm/sslCertificate">https://helios.cohesity.com/v2/mcm/sslCertificate</a> in the browser address bar.</li> <li>3. Copy-paste the certificate to Notepad or Word Processor.</li> <li>4. In the copied certificate, replace \n with a new line.</li> </ol> <p>Click to view a sample of the DataProtect as a Service for Government (FedRAMP) public certificate</p> <pre style="background-color: #f0f0f0; padding: 10px;"> -----BEGIN CERTIFICATE----- MIIG1zCCBb+gAwIBAgIJAiUz4iuB+NVMA0GCSqGSIb3DQEBCwUAMIG0MQswCQYD VQQGEwJVUzEQMA4GA1UECBMHQXJpem9uYTEtMBEgA1UEBxMKU2NvdHRzZGFsZTEa MBgGA1UEChMRR29EYWRkeS5jb20sIEluYy4xLTArBgNVBAsTJGh0dHA6Ly9jZXJ0 cy5nb2RhZGR5LmNvbS9yZXBvc210b3J5LzEzZmEzMDUyMDE1LjEzLjEzLjEzLjEz dXJlIENlcnRpb20sIEluYy4xLTArBgNVBAsTJGh0dHA6Ly9jZXJ0cy5nb2RhZGR5 LmNvbS9yZXBvc210b3J5LzEzZmEzMDUyMDE1LjEzLjEzLjEzLjEzLjEzLjEzLjEz DTIyMDcyOTIwMzYzNFowRjEhMB8GA1UECxMYRG9tYWluIENvbnRyb2wgVmFsaWRh dGVkMSEwHwYDQDExhoZWxpb3MtZGF0YS5jb2h1c210eS5jb20wggeiMA0GCSqG SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDSToInp3D+wBCvJuHfhQwfl8qFr2aWe5rA tu6TV5udPCq+ORqC2UZ05HtLnv9NTXLJtISpH208fJmMBIsmQL6u6LgQ3bA7B3w5 q9e+Q/nsvDUS1MI0wjJsdVb96UZJHU4hrFeFm2seMB1jhscOOaWBdcP3wEaSum80 oSqc7Gs1UGZImxJrNmC0ikCOH9kDK8qj9Bie05CQUM4nGhpzjr3zgGte1MvGBxji GOOW/dW/qB5lmScndAoXmzwyTQVWxHasXRpYCawGEuG0+V4iGVJs14dSvKT8o4b JOHFwXHcU8mesdfPvq9YTkH6TkYdl5S4WfYygr5rltwzDCC4NmH/AgMBAAGjggNX MIIDUzAMBgNVHRMBAf8EAAjAAMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcD                     </pre>

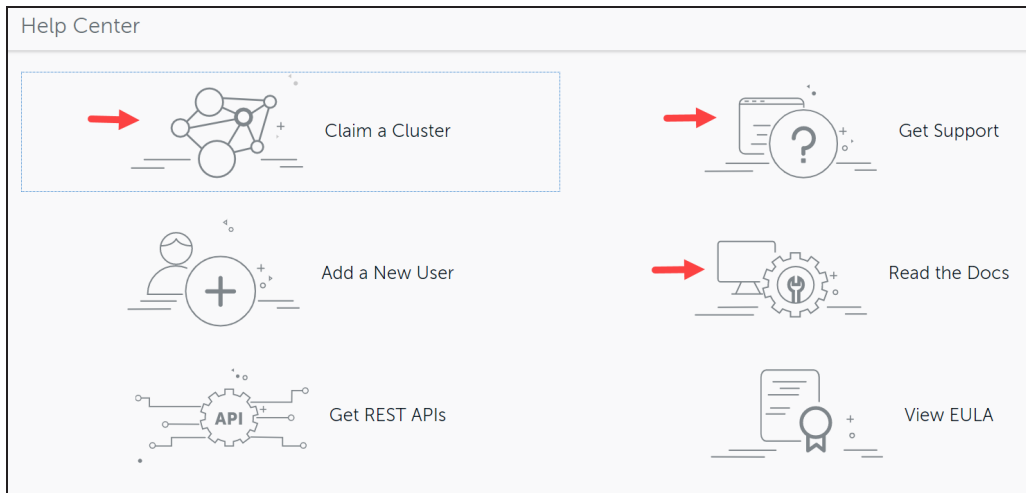
Name	Description
	<pre data-bbox="537 289 1382 533"> AjAObgNVHQ8BAf8EBAMCBaAwOAYDVR0fBDEwLzAtoCugKYYnaHR0cDovL2Nybc5n b2RhZGR5LmNvbS9nZGlhbnMmMxLTIxNjcuY3JsMF0GA1UdIARWMFQwSAYLYIZIAYb9 bQEhFwEwOTA3BggrBgEFBQcCARYraHR0cDovL2N1cnRpZmljYXR1cy5nb2RhZGR5 LmNvbS9yZXBvc210b3J5LzAIBgZngQw -----END CERTIFICATE-----                     </pre> <ol data-bbox="500 558 1377 674" style="list-style-type: none"> <li>5. Save the Notepad or Word Processor as .pem or .crt format.</li> <li>6. The DataProtect as a Service for Government (FedRAMP) public key must be uploaded to the IdP site.</li> </ol>

7. Click **Save**.

DataProtect as a Service for Government (FedRAMP) validates the connection to the IdP. If the connection succeeds, the SSO provider is added to the provider list and you can edit, delete or deactivate the provider. Users can start accessing DataProtect as a Service for Government (FedRAMP) through their IdP home page or the DataProtect as a Service for Government (FedRAMP) sign-in page by clicking the **Sign in with SSO** link.

**Considerations**

- If you have logged into DataProtect as a Service for Government (FedRAMP) using Okta credentials (or any other IdP), you will not be able to directly access some of the portals in the Help Center such as Claim a Cluster, Get Support, and Read the Docs as these portals require Cohesity Support portal credentials to log in.



- If no default role is assigned to a user in the IdP entry, then such users will be rejected. Users will need to have an explicit entry.



- If the SAML assertions are to be signed and encrypted, then the DataProtect as a Service for Government (FedRAMP) certificate must be used.

**Next** > Add Cohesity DataProtect as a Service **users and groups** from your SSO domain.

## Configure SSO with Active Directory Federation Services (AD FS)

This topic provides step-by-step instructions on configuring and using Active Directory Federation Services (AD FS) on Cohesity SSO.

### Prerequisites

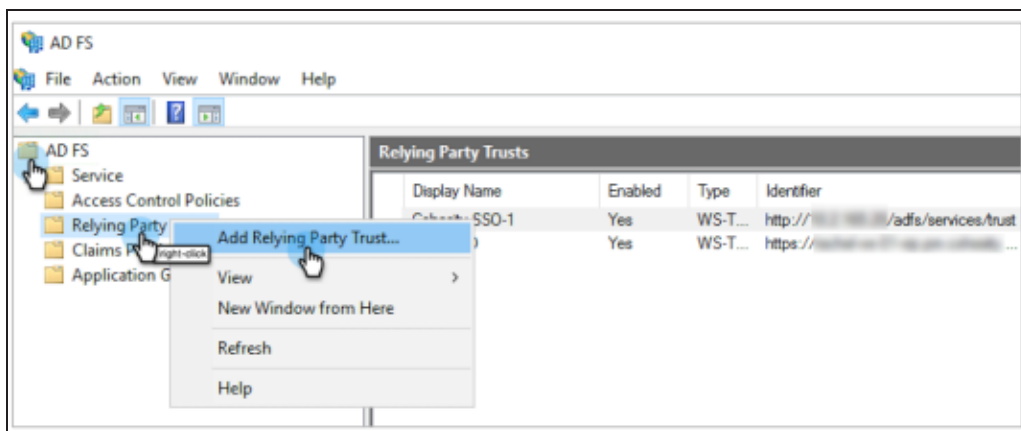
- Install AD FS on the server. For more information, see [Deploy and configure AD FS](#).
- An Active Directory instance where all users have an email address attribute.
- A server running Microsoft Server 2016, 2012, or 2008.
- An SSL certificate to sign your AD FS login page and the Signing Certificate for that certificate.
- An installed certificate for hosted SSL.

### Add a Relying Party Trust (RPT)

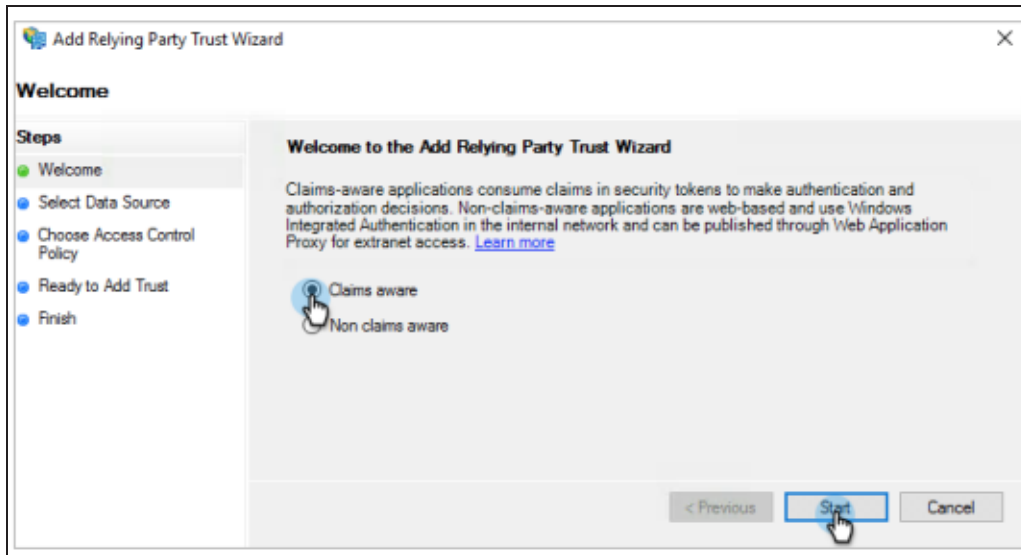
Perform the following steps to add a Relying Party Trust (RPT) to enter the Cohesity SSO authenticate URL via the SAML 2.0 WebSSO protocol.

1. Log in to the server and open **AD FS**.
2. Under **AD FS**, right-click **Relying Party Trusts** and select **Add Relying Party Trust**.

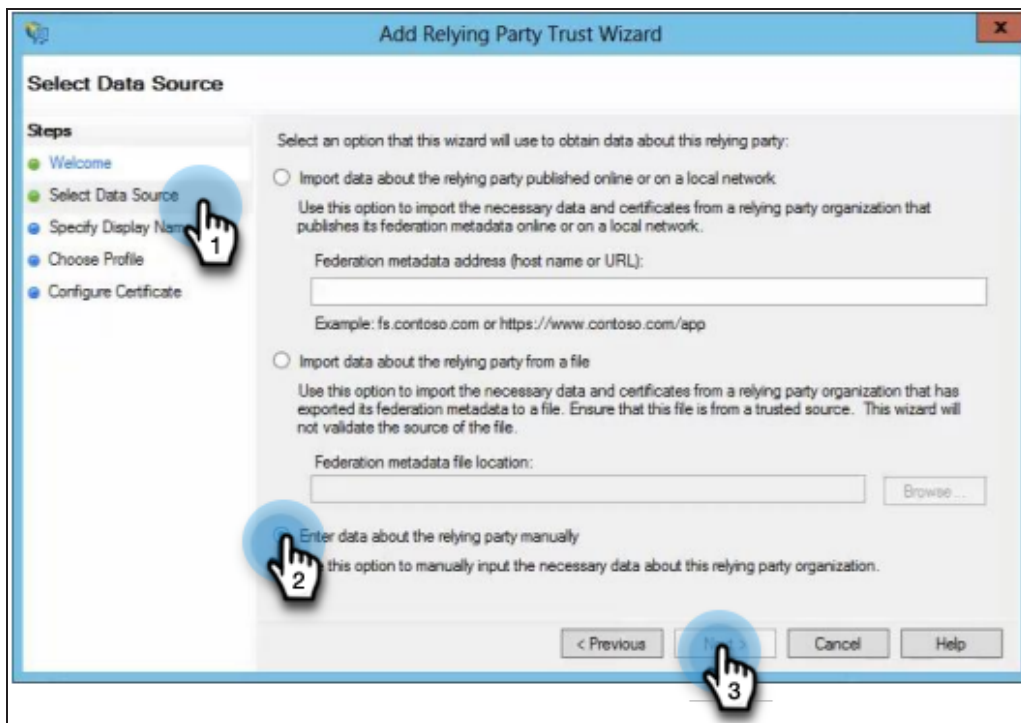
The **Add Relying Trust Party Wizard** page is displayed.



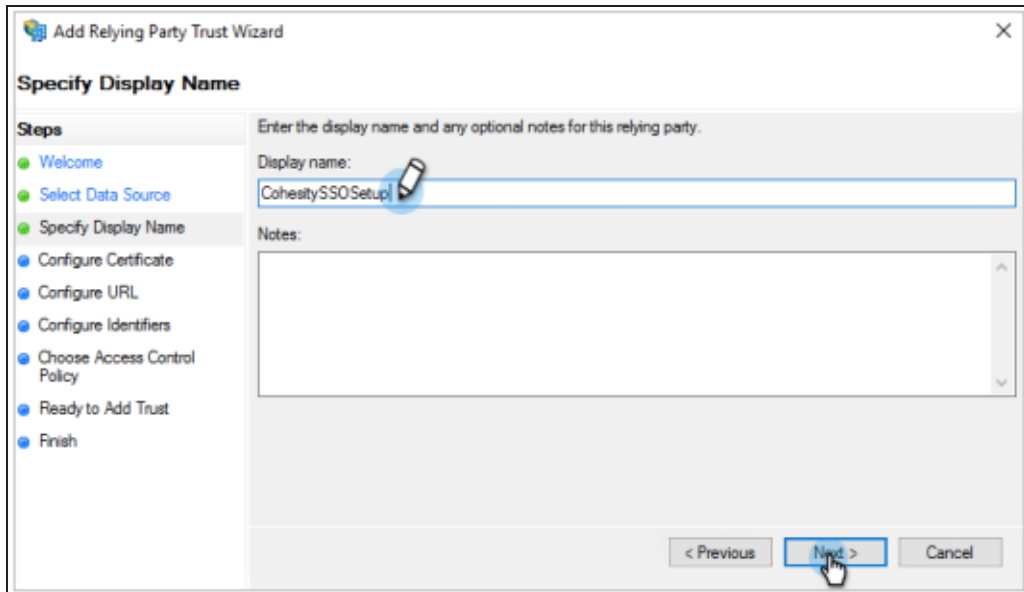
3. Select **Welcome**, select **Claims aware**, and then click **Start**.



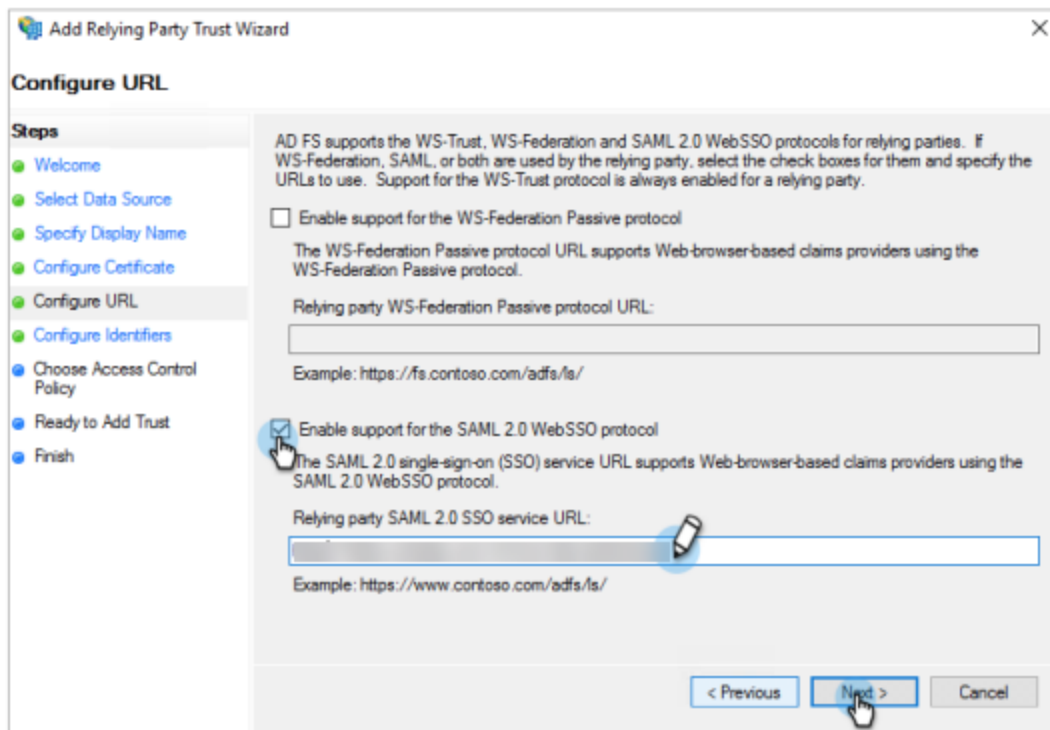
- 4. Under **Select Data Source**, select **Enter data about the relying party manually** and click **Next**.



- 5. Under **Specify Display Name**, in the **Display name** field, enter a display name and click **Next**.

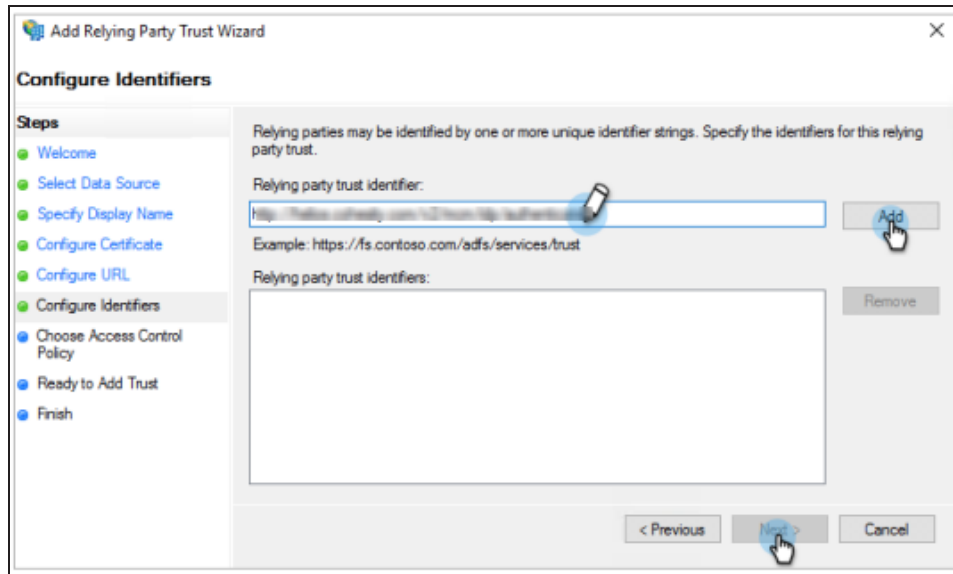


6. Under **Configure Certificate**, leave the default certificate settings and click **Next**.
7. Under **Configure URL**, do the following:
  1. Select the **Enable Support for the SAML 2.0 WebSSO protocol** check box.
  2. In the **Relying party SAML 2.0 SSO service URL** field, enter :  
**<https://helios.gov-cohesity.com/v2/mcm/idp/authenticate>**



8. Under **Configure Identifiers**, do the following:

1. In the **Relying party trust identifier** field, enter **https://helios.gov-cohesity.com/v2/mcm/idp/authenticate**
2. Click **Add** and then click **Next**.



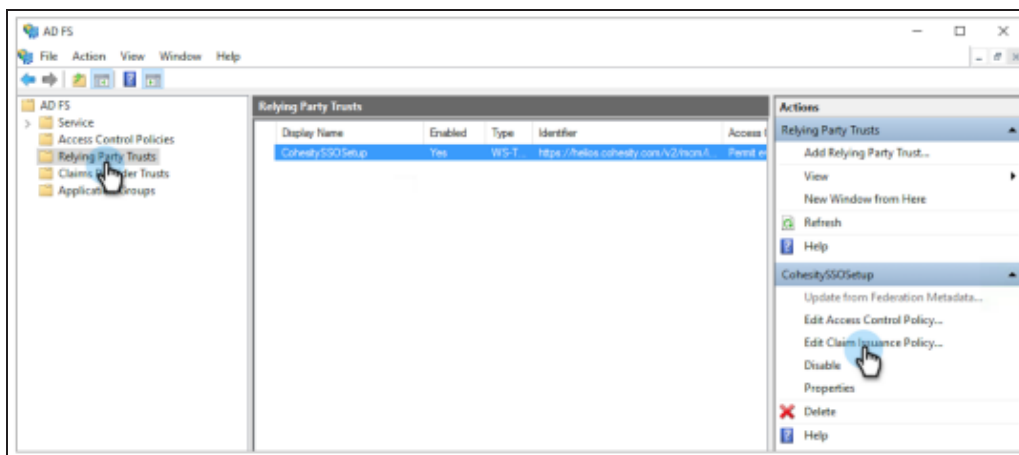
9. Under **Choose Access Control Policy**, you can optionally configure multi-factor authentication (MFA) and click **Next**. For more information, see [Configure Additional Authentication Methods for AD FS](#).
10. Under **Ready to Add Trust**, see an overview of the settings and click **Next**.
11. Under **Finish**, click **Close**.

### Create Claim Rules

Cohesity looks for SAML attributes to identify users and assign roles.

Perform the following steps to pass SAML attributes:

1. Log in to the server and open **AD FS**.
2. Under **AD FS**, select **Relying Party Trusts** and select the RPT that you added.
3. On the right, click **Edit Claim Issuance Policy**.

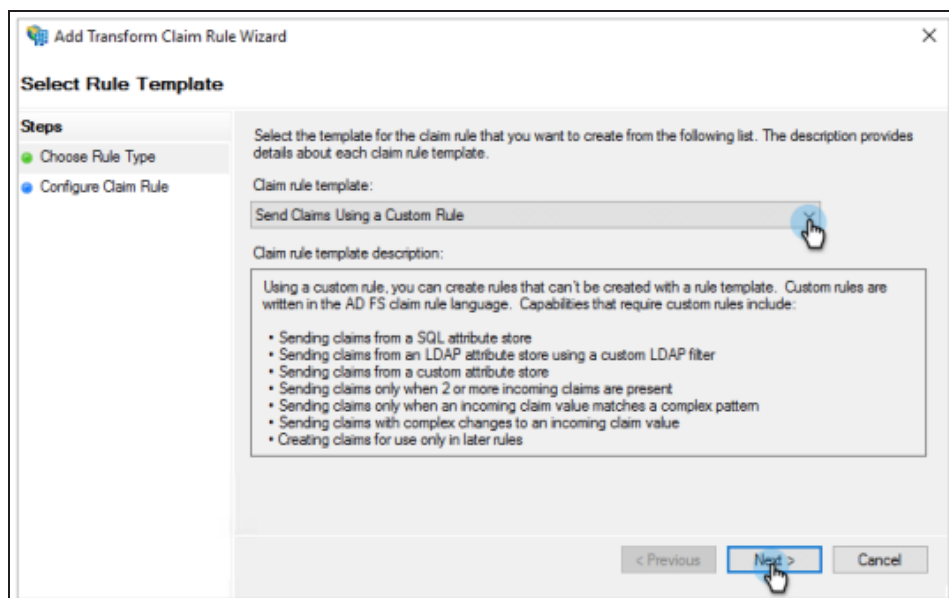


4. Click **Add Rule**.

The **Add Transform Claim Rule Wizard** page is displayed.

5. Under **Select Rule Template**, do the following:

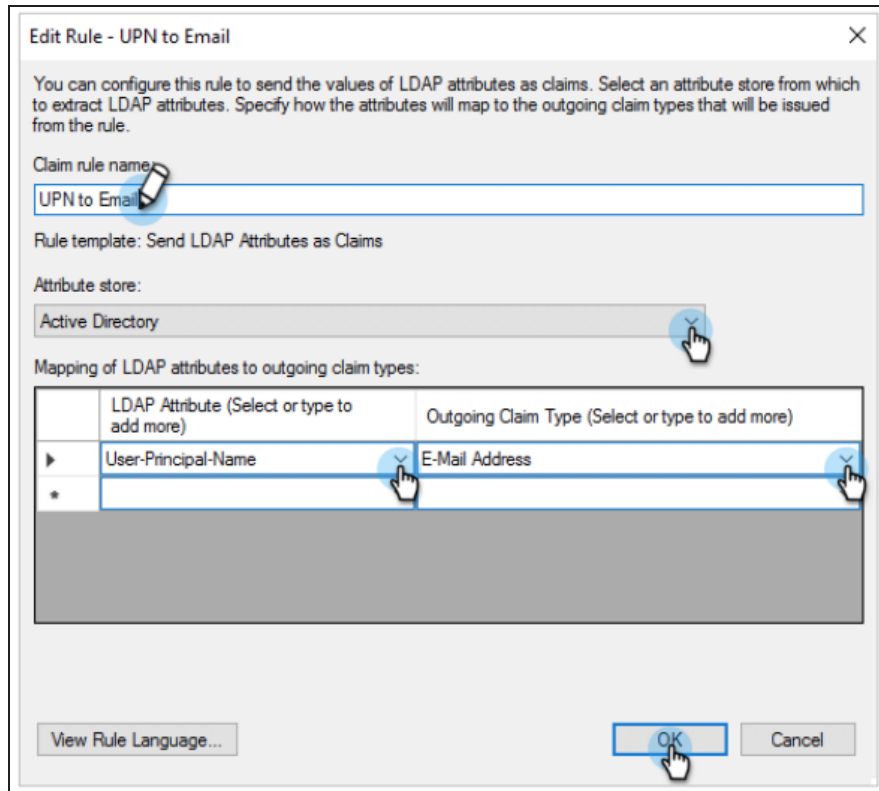
1. From the **Claim rule template** drop-down, select **Send LDAP Attributes as Claims**.
2. Click **Next**.



6. Under **Edit Rule**, do the following:

1. In the **Claim rule name** field, enter a name.
2. From the **Attribute store** drop-down, select **Active Directory**.
3. In the **Mapping of LDAP attributes to outgoing claim types** table:

1. Under **LDAP Attribute (Select or type to add more)**, from the drop-down, select **User-Principal-Name**.
2. Under **Outgoing Claim Type**, from the drop-down, select **E-Mail Address**.
3. Click **OK**.



7. Click **Add Rule** to create another rule.
8. From the **Claim rule template** drop-down, select **Transform an Incoming Claim**.
9. Click **Next**.
10. Under **Edit rule**, do the following:
  1. In the **Claim rule name** field, enter a name.
  2. From the **Incoming claim type** drop-down, select **E-Mail Address**.
  3. From the **Outgoing claim type** drop-down, select **email**.

4. Click **OK**.

**Edit Rule - Email address to Cohesity email Attribute** [X]

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

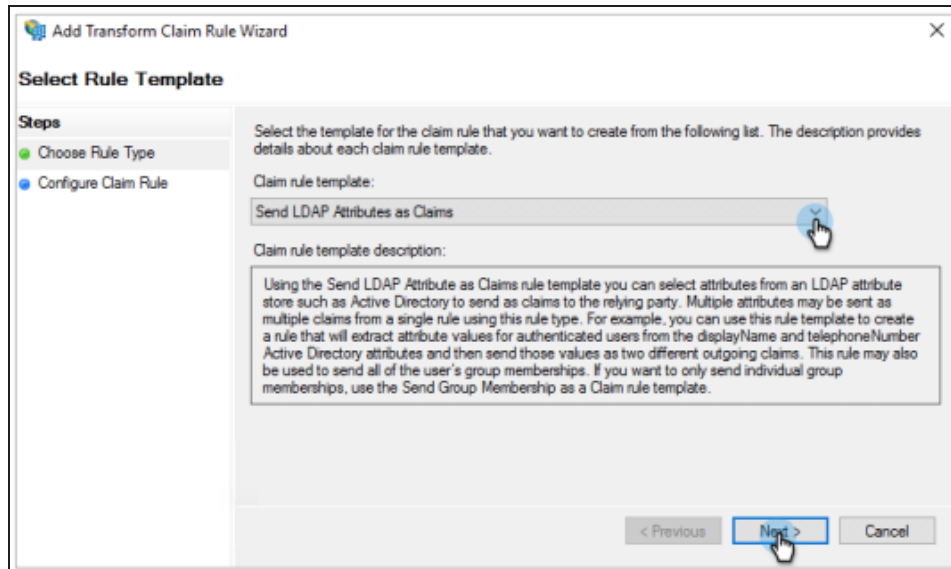
Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

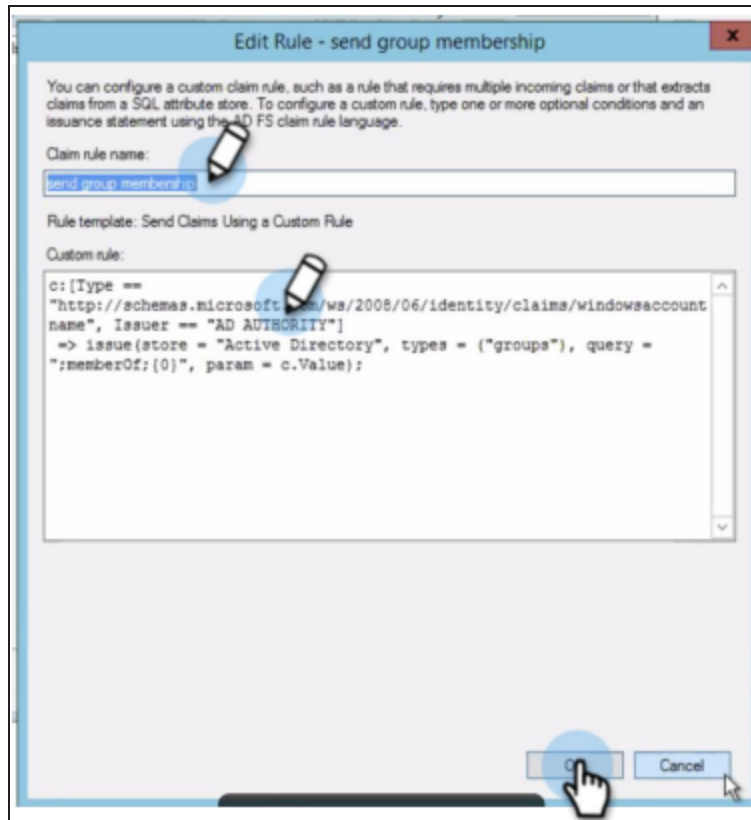
Pass through all claim values  
 Replace an incoming claim value with a different outgoing claim value  
     Incoming claim value:   
     Outgoing claim value:    
 Replace incoming e-mail suffix claims with a new e-mail suffix  
     New e-mail suffix:   
     Example: fabrikam.com

11. Follow the steps above to pass group SAML attributes.
12. To extract the user group name and send it to Cohesity, you need to create a custom rule in AD FS:
  1. Click **Add Rule** to create the custom rule.
  2. From the **Claim rule template** drop-down, select **Send Claims Using a Custom Rule**.
  3. Click **Next**.



4. Under **Edit rule**, do the following:
  1. In the **Claim rule** name field, enter a name.
  2. In the **Custom rule** field, create and enter a custom rule. For more information, see [Understanding Claim Rule Language in AD FS](#).
  3. Click **OK**.





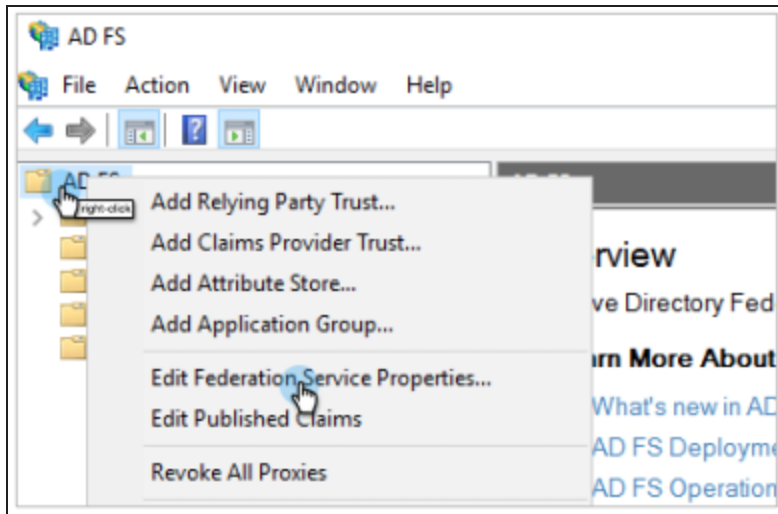
**Note:** This rule might be different for different AD FS configurations. Make sure to edit the custom rule accordingly. For more information, see [When to Use a Custom Claim Rule](#).

### Retrieve the SSO URL, Provider Issuer ID, and Certificate

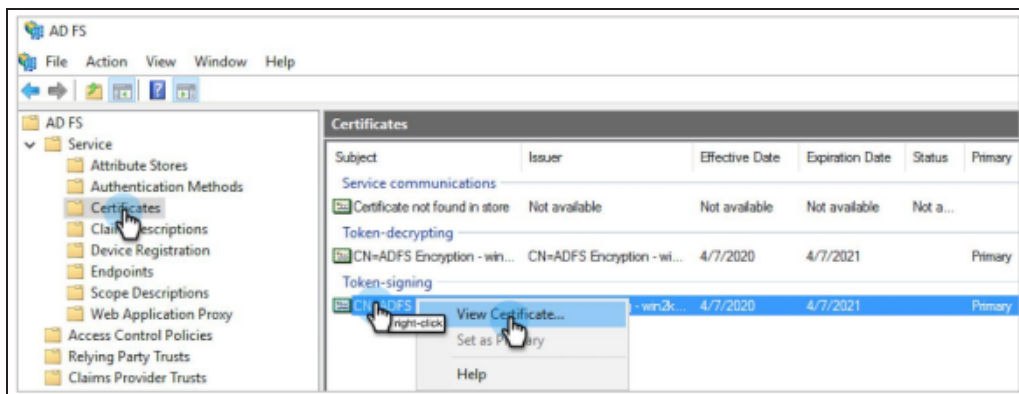
You need to retrieve the Federation Service name and Federation Service Identifier which is required when adding AD FS as an SSO provider to Cohesity.

Perform the following steps to retrieve the Federation Service name and Federation Service Identifier:

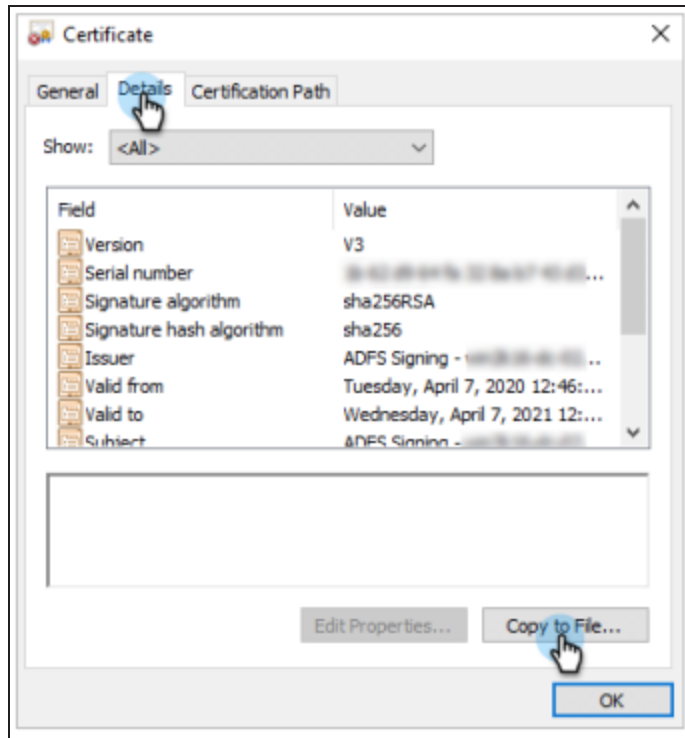
1. Log in to the server and open **AD FS**.
2. Right-click **AD FS** and select **Edit Federation Service Properties**.



3. Copy the **Federation Service name** and the **Federation Service Identifier** and save it for later use. You will need these when you [Configure SSO](#) to Cohesity.
4. To download the certificate, navigate to **AD FS > Service > Certificates**.
5. Under **Token-signing**, right-click the certificate and select **View Certificate**.



6. Click the **Details** tab and then click **Copy to File**.  
The **Certificate Export Wizard** page is displayed.



7. Select **Base-64 encoded X.509 (.CER)**, click **Next**, and follow the instructions to download the certificate (.cer).
8. Convert certificate file from the .cer to the .pem format.

To convert the file:

- On Mac/Linux, rename the file with the .pem filename extension.
- On Windows, run the following command:

```
openssl x509 -in mycert.crt -out mycert.pem -outform PEM
```

### Consideration

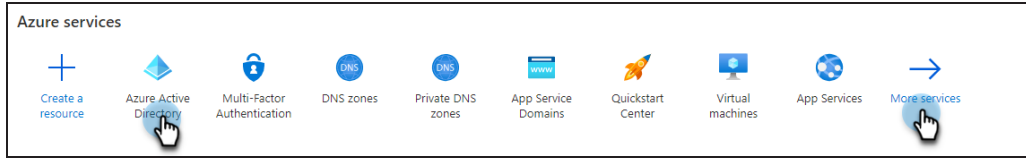
DataProtect as a Service for Government (FedRAMP) does not support **Sign Auth Requests** to sign the SAML requests to the ADFS server.

### Configure SSO with Azure

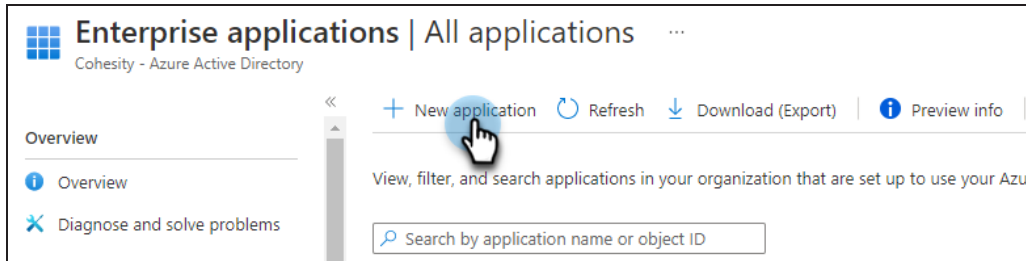
This topic provides step-by-step instructions on creating an Azure Active Directory application.

Perform the following steps to create an Azure AD SSO:

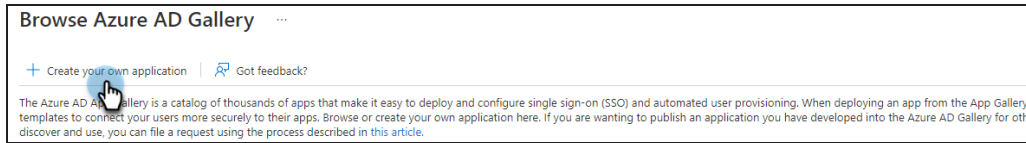
1. Log in to [Azure portal](#).
2. Under **Azure services**, click **Azure Active Directory**. If Azure Active Directory is not listed, click **More Services** and select **Azure Active Directory**.



- 3. On the left, click **Enterprise applications**.
- 4. Under **All applications**, click **New Application**.




- 5. On the **Browse Azure AD Gallery** page, click **Create your own application**.



- 6. In the **What's the name of your app**, enter a display name for your application.
- 7. Select **Integrate any other application you don't find in the gallery (Non-gallery)** and click **Create**.


## Create your own application ✕

 Got feedback?


---


If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?


What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Azure AD (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery) 


 [Create](#)

8. On the **<app> Overview** page, under **General Settings**, 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 user accounts in the application  
[Get started](#)

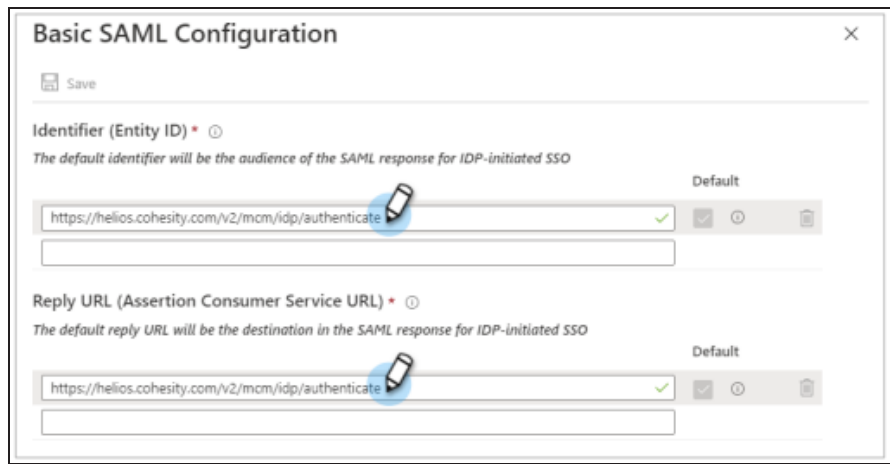



**4. Conditional Access**  
Secure access to this application with a customizable access policy.  
[Create a policy](#)

9. Under **Select a single sign-on method**, click the **SAML** tile.
10. Under **Set up Single Sign-On with SAML**, do the following:
  1. In the **Basic SAML Configuration** section, click the edit  icon and do the following:
    1. Under **Identifier (Entity ID)**, click **Add identifier**.  
For example,  
`https://helios.gov-cohesity.com/v2/mcm/idp/authenticate`
    2. Under **Reply URL (Assertion Consumer Service URL)**, click **Add reply URL**.  
For example,  
`https://helios.gov-cohesity.com/v2/mcm/idp/authenticate`
    3. Click **Save**.

**Note:** 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.



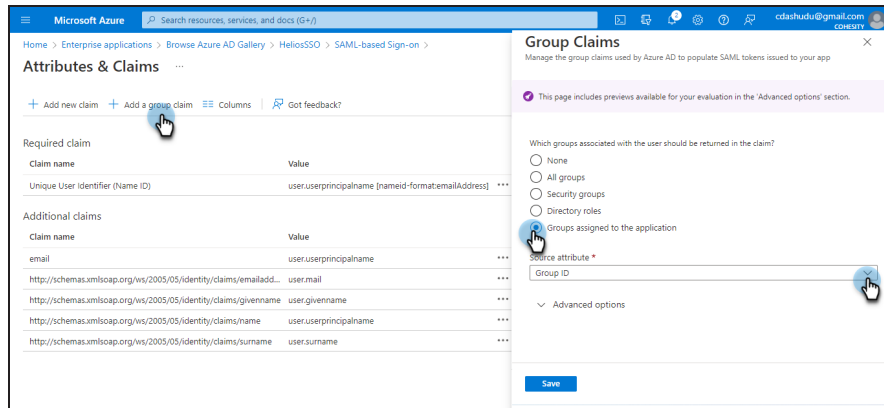
2. In the **Attributes & Claims** section, click the edit  icon and do the following:
  1. Click **Add new claim**.  
The **Manage claim** page is displayed.
  2. **Name**: Enter a name for the attribute.
  3. **Source**: Select Attribute.
  4. **Namespace**: Optional. Enter a namespace URI.
  5. **Source attribute**: From the drop-down, select the source attribute.
  6. Click **Save**.



3. If you plan to use user groups-based RBAC, you need to pass the "Groups" SAML attribute to Cohesity. Perform the following steps:
  1. Under **User Attributes & Claims**, click **Add a group claim**.
  2. For **Which groups associated with the user should be returned in the claim?**, select **Groups assigned to the application**.

**Note:** Groups must be directly assigned to the application. Azure will not send the groups attribute that are a subgroup of a group which is assigned to the application.

3. From the **Source attribute** drop-down, select the source attribute.



4. Under **Advanced options**:

- a. Select the **Customize the name of the group claim** check box.
- b. **Name:** Enter a name as groups.
- c. **Namespace:** Enter the namespace URI. This is optional.



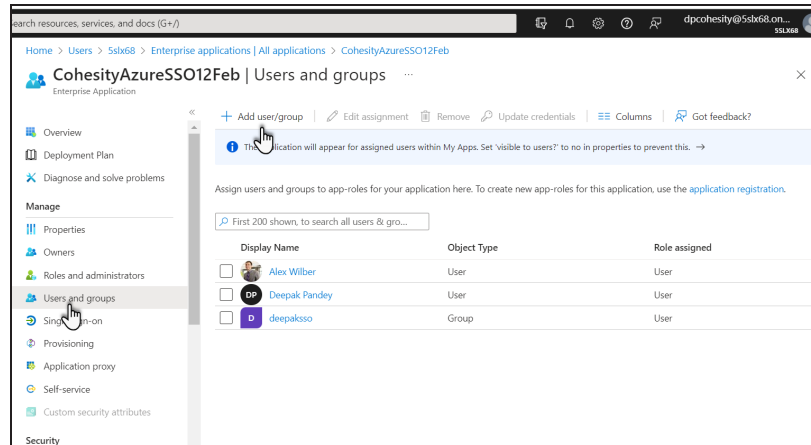
d. Click **Save**.

**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](#).

If you don't have an on-prem Active Directory synced with Azure AD, in the **Source** attribute drop-down, select **Group ID**.

4. Depending on the value of the Source attribute you selected, you need to create the corresponding . For example, if you use:
  1. **sAMAccountName**, you need to create groups with the SSO Group value as the AD groups name.
  2. **Group ID**, you need to create SSO groups using **Azure AD's Group ID**. To obtain the Azure AD's Group ID:

- a. Click the application name
- b. Under **Manage**, click **Users and groups**.





- c. Click **Add user/group** to assign a user or a group who should be able to access DataProtect as a Service for Government (FedRAMP) using this Azure AD application.
- d. From the list of users, click a user.

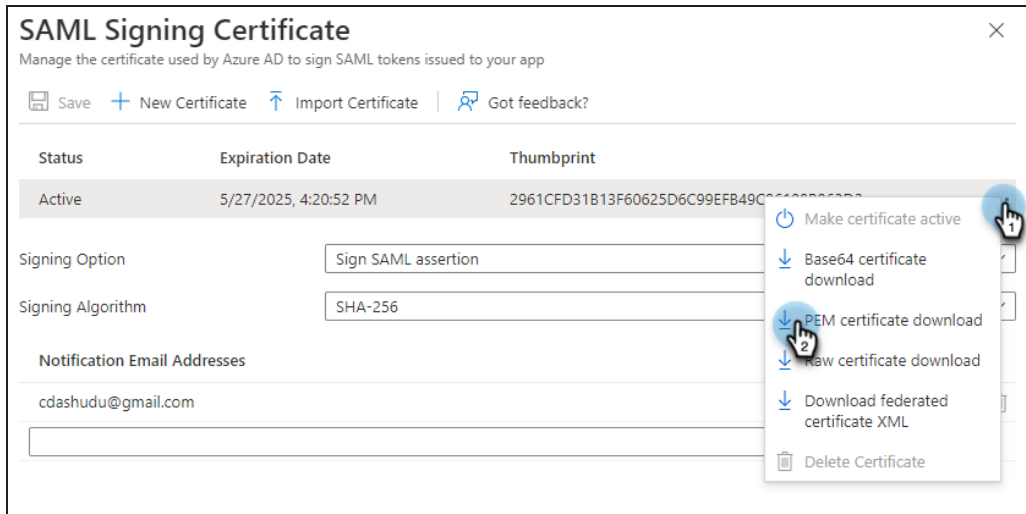
**Note:** Nested groups are not supported and will not be passed under the Groups SAML attributes.

### Retrieve the SSO URL, Provider Issuer ID, and Certificate

You need to retrieve Azure AD information to configure SSO on DataProtect as a Service for Government (FedRAMP) for the IdP (Azure AD).

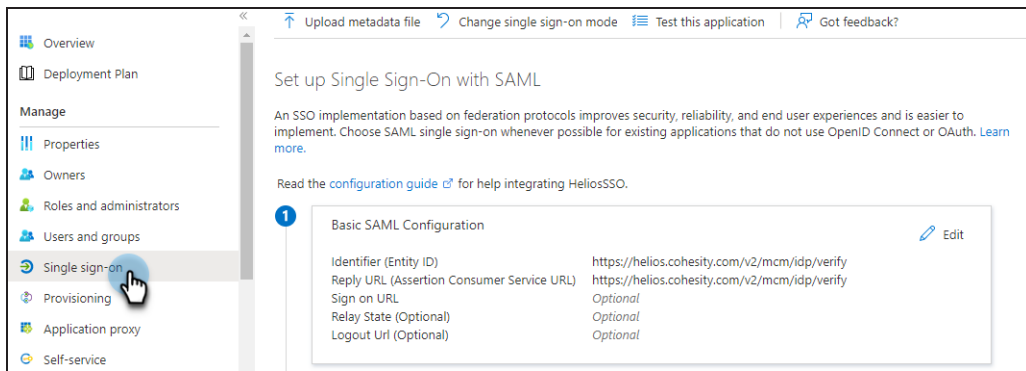
Perform the following steps to retrieve the SSO URL, Entity ID, and certificate from the Azure AD application:

1. Log in to [Azure portal](#).
2. Under **Azure services**, click **Azure Active Directory**. If Azure Active Directory is not listed, click **More Services** and select **Azure Active Directory**.
3. On the left, click **Enterprise applications**.
4. Click the application name and under **Manage**, click **Single sign-on**.
5. Under **Set up Single Sign-On with SAML**, in the **SAML Signing Certificate** section, click the edit  icon.
6. On the **SAML Signing Certificate**, click the ellipsis (  ) icon and select **PEM certificate download**.



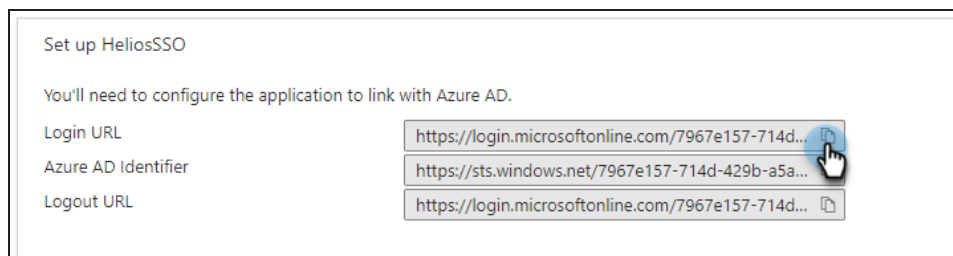
**Note:** Cohesity SSO only accepts \*.pem format certificate.

7. Under **Manage**, click **Single sign-on**.



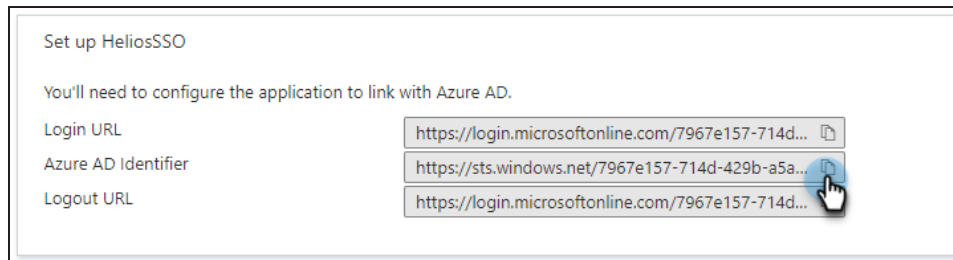
8. Under **Set up Single Sign-On with SAML**, in the **Set up <application name>** section, do the following:

1. Copy the **Login URL** and save it for later use. You will use this URL to enter the Cohesity Single-Sign-On URL when you **Configure SSO** to Cohesity.



2. Copy the **Azure AD Identifier** URL and save it for later use. You will use this URL to enter the Cohesity Provider Issuer ID when you **Configure SSO** to

Cohesity.



You need to add the SSO provider in DataProtect as a Service for Government (FedRAMP). For more information, see [Configure SSO](#).

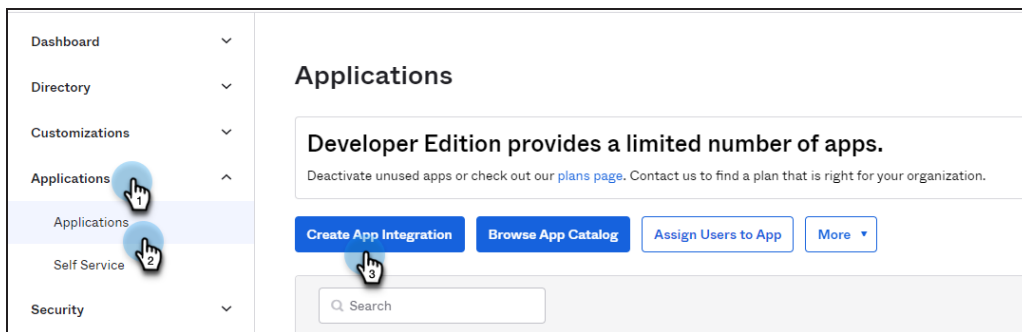
### Configure SSO with Okta

This topic provides step-by-step instructions on adding DataProtect as a Service for Government (FedRAMP) as an application to Okta.

Perform the following steps to add DataProtect as a Service for Government (FedRAMP) as an application to Okta:

1. Log in to Okta as an Okta administrator.
2. Navigate to **Applications > Applications** and click **Create App Integration**.

The **Create a New Application Integration** page is displayed.



3. For the **Sign on method**, select **SAML 2.0** and click **Next**.

The **Create SAML Integration** page is displayed.

4. Click the **General** tab and for **General Settings** do the following:

1. **App Name**: Specify an app name of your choice to display in the DataProtect as a Service for Government (FedRAMP) tile on the SSO page.

2. **App logo (optional)**: Click  > **Browse files** and navigate to the location of the logo and select the logo. Click **Apply** to upload the logo. Click  to

delete the logo.

3. **App Visibility:** Leave the default settings for **Do not display application icon for users** and **Do not display application icon in the Okta Mobile app**.
4. Click **Next**.

**1 General Settings**

App name: CohesitySSO

App logo (optional): [Gear icon] [Trash icon]

App visibility:
 

- Do not display application icon to users
- Do not display application icon in the Okta Mobile app

Cancel [Next]

5. Click the **Configure SAML** tab and for **SAML Settings** do the following:

1. **Single sign on URL:** Specify the application URL followed by `/idps/authenticate`.

For example: `https://<cluster_fqdn>/idps/authenticate`.

For Cohesity Helios for Government (FedRAMP) use, `https://helios.gov-cohesity.com/v2/mcm/idp/authenticate`.


**Note:** To find the FQDN and VIP address, log in to Cohesity Data Cloud (Self-managed) and navigate to **Settings > Cluster > Networking > VIPs**.

The **Use this for Recipient URL and Destination URL** check box is selected by default.

2. **Audience URI (SP Entity ID):** Specify the same URL as above.
3. **Application username:** Select your preference.


**A 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 ?  

- 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 <small>(optional)</small>	Value
<input type="text" value="email"/> 	<input type="text" value="Unspecified"/>	<input type="text" value="user.email"/> 
<input type="text" value="login"/> 	<input type="text" value="Unspecified"/>	<input type="text" value="user.login"/>  <span style="float: right;">×</span>

- Under **Group Attribute Statements (Optional)**, 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.) If you want

to use an existing group, use a regex to pass all groups.

**Note:** You should enter "groups" in the name field to map the groups attribute to the Okta Filter attribute.

**Group Attribute Statements (optional)**

Name	Name format (optional)	Filter
groups	Unspecified ▾	Matches regex ▾ (.*)
<div style="border: 1px solid #ccc; border-radius: 5px; padding: 5px 15px; display: inline-block; color: #0070c0; text-decoration: none;">Add Another</div>		

6. Click **Next**.
7. Click **Finish** to add the application.
6. Click the **Sign On** tab and do the following:
  1. Under **SAML Setup**, located at the right side, click **View SAML setup instructions**.

The **How to Configure SAML 2.0 for <application name>** page is displayed.

**SAML Signing Certificates**

[Generate new certificate](#)

Type	Created	Expires	Status	Actions
SHA-1	Today	Sep 2028	Inactive ⚠	<a href="#" style="color: #0070c0;">Actions ▾</a>
SHA-2	Today	May 2032	Active	<a href="#" style="color: #0070c0;">Actions ▾</a>

**SAML Setup**

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

2. Copy the **Identity Provider Single Sign On URL** and save it for later use. You will use this URL to enter the Cohesity Single Sign-On URL when you [Configure SSO](#) to Cohesity.

A sample URL is shown below.

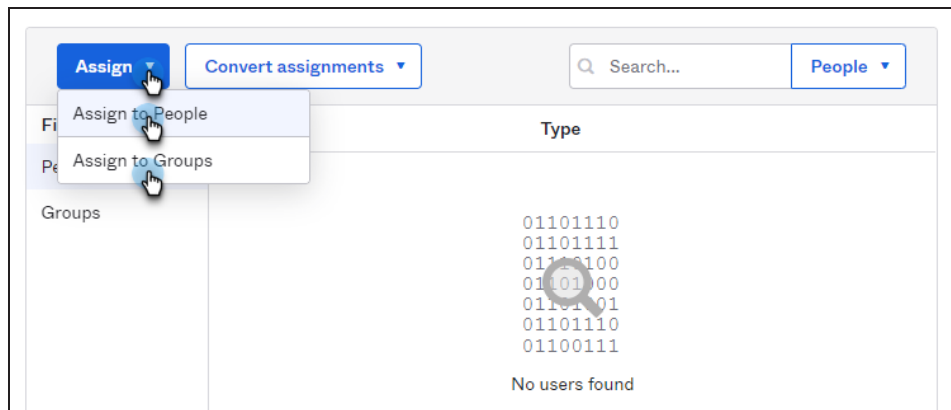
```
https://mycompany.okta.com/app/cohesitymycompany_heliosapp/exkhhbyzrgu0YvJFk0h7/sso/saml
```

3. Copy the **Identity Provider Issuer** and save it for later use. You will use this URL to enter the Cohesity Provider Issuer ID when you [Configure SSO](#) to Cohesity.

A sample URL is shown below.

`http://okta.com/exkhhbyzrgu0YvJFk0h7`

4. Click **Download certificate** to download the `okta.cert` file and note its download location.
5. Convert the downloaded `okta.cert` file to `okta.pem`. You will upload this file to DataProtect as a Service for Government (FedRAMP) later.
7. Click the **Assignments** tab and do the following:
  1. From the **Assign** drop-down, select **Assign to People** to assign users to your Cohesity Okta application.
  2. From the **Assign** drop-down, select **Assign to Groups** to assign groups to the app.



You have now configured the Okta application for Cohesity. You need to add the SSO provider in DataProtect as a Service for Government (FedRAMP). For more information, see [Configure SSO](#).

## Add API Keys

You can add your Cohesity API keys to your DataProtect as a Service for Government (FedRAMP) to:

- Authenticate an application or script for reporting and workflow automation via Cohesity's REST API calls for Cohesity DataProtect.

To add your API key:

1. In **DataProtect as a Service**, navigate to **Settings > Access Management**, and click the **API Keys** tab.
2. Click **Add API Key**.
3. Enter a **Name** for the API key.
4. Click **Save** to advance to the **API Key Details** page, where you can:



- **View or Copy API Key Token.** To use with the application or script you wish to authenticate.
- **Scan QR Code.** Scan the QR code that is displayed with your Helios Mobile App to monitor your Cohesity DataProtect as a Service in the mobile app.

When you return to the **API Keys** tab, your new key appears in the list.

**Note:** The API keys you add are available only to you.

Click the **Actions** menu (: ) next to the API key to **Delete** it.

### Sample API Keys



Once you have [added an API Key](#), you can start making API calls.

Below is a sample API key,

#### API Key Details

The API Key Token will be available only once on creation. Please store it in a secure location.

Use API Keys to authenticate an application or script to Helios for management by APIs. Refer to Helios REST API documentation for details about using these keys.

Name	Sample
API Key Token	*****  

The API Key Token is only available once upon creation. Make sure to store it in a secure location. Use this key to authenticate an application or script to Helios for API management. For the detailed list of APIs, see <https://api.cohesity.com>.

# Policies

In DataProtect as a Service for Government (FedRAMP), a policy is a reusable collection of settings that define how and when the objects & files in a source are protected. You can create as many policies with specific settings for different use cases as you need.

In a policy, you set the frequency (**Backup every**) and retention period (**Keep for**) for each protection run. You can also add a Periodic Full Backup, Quiet Times, and Log Backup schedules — see [More Options](#).

## Create a Policy

To create a policy:

1. In **DataProtect as a Service**, navigate to **Policies**.
2. Click **Create Policy**.
3. Enter a **Policy Name**, choose a **Backup every** interval and a **Keep for** retention period.
4. If you wish to add a DataLock, Periodic Full Backup, Quiet Times, or schedule database Log Backups, click **More Options**.
5. Click **Create**.

## More Options

Settings	Descriptions
<b>DataLock</b>	<p>Typically used for compliance and regulatory purposes, DataLock is a protection policy option that can only be enabled by a user with the Data Security role. Use it when you need to prevent the deletion of backup snapshots for a specified duration. You can set the DataLock duration to the same period as your backup retention, or to a shorter period.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p><b>Note:</b> Only a user with the <b>Data Security</b> role can enable or disable DataLock on a policy, or delete or edit a DataLocked policy. Disabling a DataLock does not unlock any previously DataLocked snapshots.</p> </div>
<b>Periodic Full Backup</b>	<p>After the first Protection Run, Cohesity DataProtect as a Service backs up only the data that changed with <i>incremental</i> backups. Use this option to add a <i>full</i> backup run at regular intervals.</p>

Settings	Descriptions
<b>Quiet Times</b>	<p>If there are times you need to protect your network from too much traffic, add a Quiet Time period to define the times when new Protection Runs do not start. (Note that those already running at the beginning of a Quiet Time will still complete the run.) By default, a Quiet Time period is set in your browser's time zone.</p> <p><b>Tip:</b> To add more Quiet Time periods, click <b>Quiet Times</b> again.</p>
<b>Log Backup</b>	<p>If you are protecting databases, you can set a separate frequency and retention period for your log backups.</p>

# Microsoft 365

Microsoft 365 is a subscription service that bundles the traditional office productivity applications and delivers them as SaaS applications. Microsoft 365 includes Exchange Online, OneDrive for Business, SharePoint Online, Teams, and other applications. DataProtect as a Service for Government (FedRAMP) provides simple, fast, and cost-effective data protection solution for the following Microsoft 365 applications:

- [Exchange Online Mailboxes](#)
- [OneDrive for Business](#)
- [SharePoint Online](#)
- [Microsoft Teams](#)
- [Microsoft Groups](#)

## Microsoft 365 Requirements

Before you register your Microsoft 365 sources with DataProtect as a Service for Government (FedRAMP) to protect your Microsoft 365 data, ensure you have met the following prerequisites:

1. In the Exchange admin center, [add these roles to the Microsoft 365 user account](#) you will use to register your Microsoft 365 sources with DataProtect as a Service for Government (FedRAMP):
  - `ApplicationImpersonation`
  - `View-Only Configuration`
  - `View-Only Recipients`
  - `MailboxSearch`
  - `MailRecipients`
2. Update [Microsoft Organization setting](#) for Mailbox size reporting.
3. [Register a custom Azure app](#) (for manual Microsoft 365 source registration).
4. [Set additional permissions for SharePoint Online](#).

Finally, review the considerations for each supported Microsoft 365 application:

- [Exchange Online Mailboxes](#)
- [OneDrive](#)
- [SharePoint Online](#)
- [Teams](#)
- [Groups](#)

**Note:** For information on the supported cloud regions where you can back up this source, see [Supported Workloads and Cloud Regions](#).

## Add Roles to Microsoft 365 User Account

DataProtect as a Service for Government (FedRAMP) accesses your Microsoft 365 domain with a user account to back up your Microsoft Exchange Online data. You can either add these roles to an existing user account or create a new user account with these roles.

**Important:** Ensure that multi-factor authentication is not enabled for the user account.

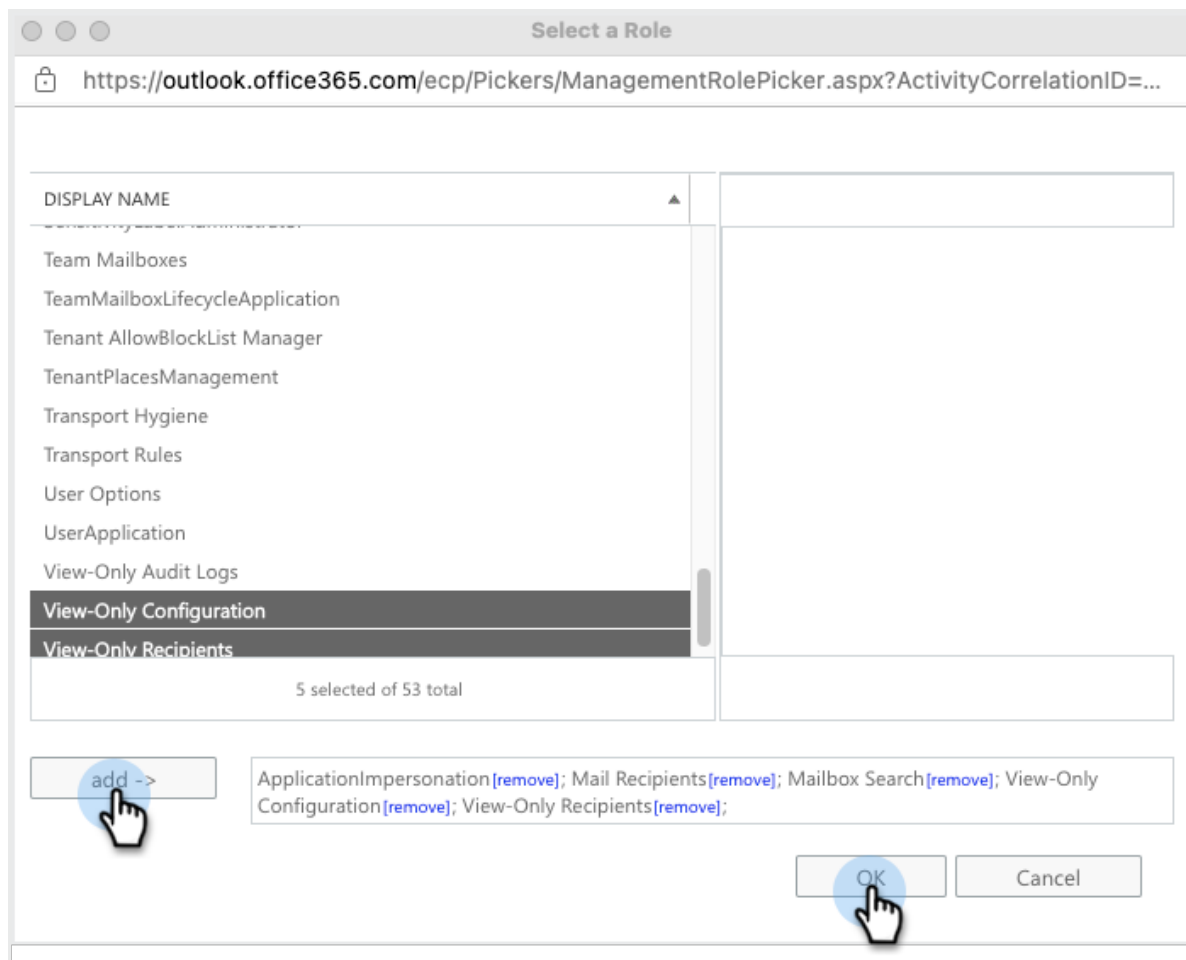
To add roles to the Microsoft 365 user account:

1. Log in to [Microsoft 365](#).
2. In the **Office 365** page, click **Admin**.
3. In the **Microsoft 365 admin center** page, select **Admin centers**, and then click **Exchange**.

Follow the steps for Classic Exchange admin center in [Step 4](#) next, or skip to Step 5 if you are in the new Exchange admin center page.

**Tip:** TIP: If you see a message prompting you to switch to New Exchange, you are still in classic Exchange.

4. To add roles from the Classic Exchange admin center page:
  1. Click **Permissions** and then select the **Admin roles** tab.
  2. In the **Admin roles** tab, click **+** to create a new role group.
  3. In the **new role group** page, enter a **Name** and **Description**, and under **Roles**, click **+**.
  4. In the **Write scope** drop-down, select **Default** and click **Next**.
  5. In the **Select a Role** page, select the following roles, click **Add**, and then **OK**:
    - Mail Recipients
    - Mailbox Search
    - View-Only Configuration
    - View-Only Recipients



6. Under **Members**, click **+** to add the user account you plan to use to register the Microsoft 365 domain with DataProtect as a Service for Government (FedRAMP), then click **OK**.
7. Click **Save** to create the Role Group.

**Role Group**

https://outlook.office365.com/ecp/UsersGroups/NewAdminRoleGroup.a...

new role group

\*Name:

Description:

Write scope:

Roles:  
+ -

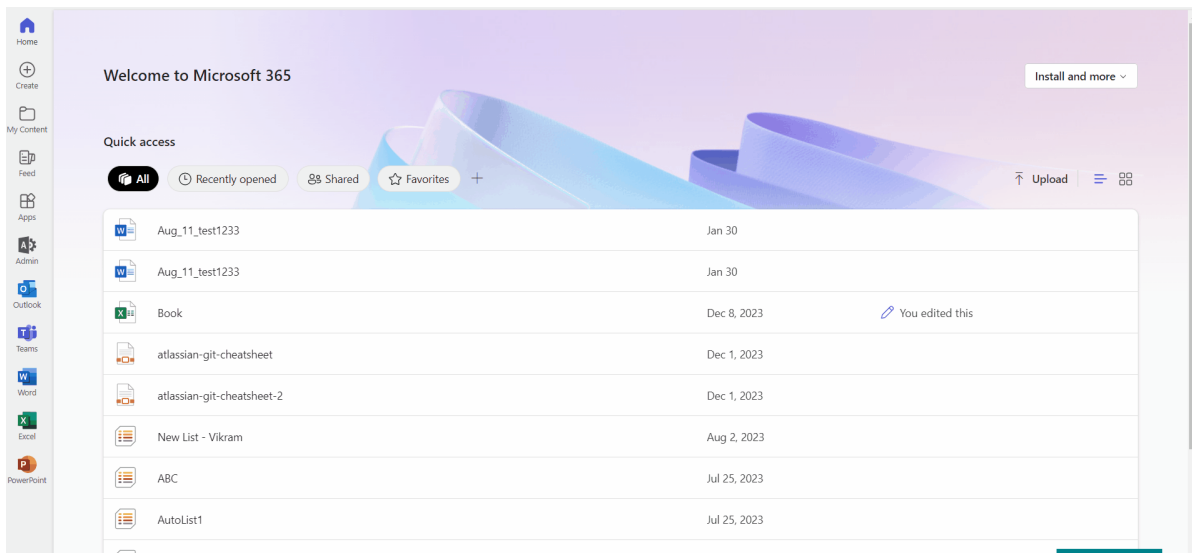
NAME
ApplicationImpersonation
Mail Recipients
Mailbox Search
View-Only Configuration
View-Only Recipients

Members:  
+ -

NAME	DISPLAY NAME
backupadmin	Backup Admin

You are ready to [update your Microsoft 365 Org setting](#) for Mailbox size reporting.

5. To add roles from the new Exchange admin center page:
  1. Select **Roles > Admin roles**.
  2. In the **Admin roles** page, click **Add role group**.
  3. Under **Basics**, enter a **Name** and **Description** for the admin role.
  4. In the **Write scope** drop-down, select **Default** and click **Next**.
  5. Under **Permissions**, select the following and click **Next**:
    - Mail Recipients
    - Mailbox Search
    - View-Only Configuration
    - View-Only Recipients
  6. Under **Admins**, search and select the user account you plan to use to register the Microsoft 365 domain with CDataProtect as a Service for Government (FedRAMP), then click **Next**.
  7. Under **Review and finish**, review the configuration and click **Add role group**.
6. After the role group is added, click **Done**.



You are ready to [update your Microsoft 365 Org setting](#) for Mailbox size reporting.

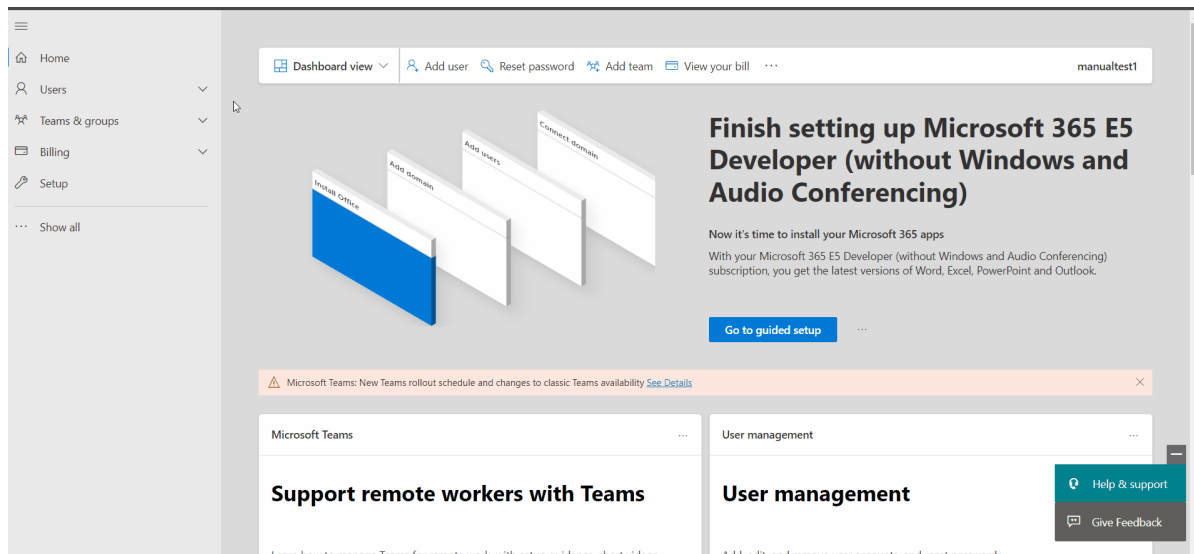
## Update Microsoft Organization Setting for Mailbox Size Reporting

By default, Microsoft reports, using Graph API, display information as de-identified names for users, groups, and sites. However, for Mailbox size reporting to work in Cohesity, you need to have identifiable information in the Email activity reports. To do that, you need to disable de-identified names for users, groups, and sites in Microsoft 365 reports.



Update the following organization setting in your Microsoft 365 admin center:

1. Log in to your [Microsoft 365 admin center](#) as a Microsoft 365 tenant administrator.
2. Go to **Settings > Org settings > Services > Reports**.
3. In **Reports**, ensure the information is identifiable by deselecting **Display concealed user, group, and site names in all reports**.
4. Click **Save**.



To continue, if you are using:

- Cohesity's [express registration](#) for Microsoft 365 sources, you are ready to add those sources to DataProtect as a Service for Government (FedRAMP).
- The [manual registration](#) for Microsoft 365 sources, you must first [register your custom Azure app](#).

**Note:** For SharePoint Online data protection, ensure that you also set the required [add-in permissions](#) and [tenant permissions](#) on the Azure application.

## Register Custom Azure App

To get started, you'll register a custom Azure app below to add the necessary permissions.

Go to the Azure portal, register a new app, add the permissions, and capture the App ID and Access Key. For more on registering and configuring Azure apps, see [Register an application with the Microsoft identity platform](#) and [Configure a client application to access a web API](#) in the Microsoft documentation.

**Note:** Make sure that you make note of the App ID and Access Key while registering the app. You'll need them to [register your Microsoft 365 domain as a source](#) in DataProtect as a Service for Government (FedRAMP).

To register your custom app for DataProtect as a Service for Government (FedRAMP):

1. Open Microsoft Entra ID
  1. To manage Microsoft Entra ID using the Azure Portal:
    1. Log in to the [Azure portal](#) with your Microsoft 365 administrator user credentials.
    2. Click the main menu (≡) in the top left corner and select **Microsoft Entra ID**.
  2. To manage Microsoft Entra ID using Microsoft 365:
    1. Log in to [Microsoft 365](#).
    2. On the **Microsoft 365** page, click **Admin**.
    3. On the **Microsoft 365 admin center** page, select **Admin centers** and then click **Microsoft Entra**.
2. Create a new custom app.
  1. Under the **Manage** section, select **App Registrations**, then click **New Registration**. In the **Register an application** page:
    1. Enter a **Name** for your app.
    2. Select the **Supported account types** that can access the app,
    3. In the **Redirect URI** drop-down, select **Web** and enter `https://localhost`.

4. Click **Register**.

### Register an application ...

**\* Name**  
The user-facing display name for this application (this can be changed later).

**Supported account types**  
Who can use this application or access this API?

Accounts in this organizational directory only (cohesitydmas only - Single tenant)  
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)  
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)  
 Personal Microsoft accounts only

[Help me choose...](#)

**Redirect URI (optional)**  
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

[By proceeding, you agree to the Microsoft Platform Policies](#)

**Register**

3. After the custom app has been created, click **Overview** and copy the **Application (client) ID**. You need to use **Application (client) ID** to register Microsoft 365 as a source in DataProtect as a Service for Government (FedRAMP).

Cohesity DataProtect App

[Delete](#)
[Endpoints](#)
[Preview features](#)

**Overview**

[Quickstart](#)

[Integration assistant](#)

**Manage**

[Branding](#)

[Authentication](#)

**Essentials**

Display name : Cohesity DataProtect App

Application (client) ID : 36744479-4114-4c50-8799-f588472f8e4f

Object ID : e25393d3-0cbc-4f6a-b7a0-9b754afd1566

Directory (tenant) ID : 942464e4-30bd-40a1-b631-cac735352ef6

Supported account types : My organization only

Client credentials : [Add a certificate or secret](#)

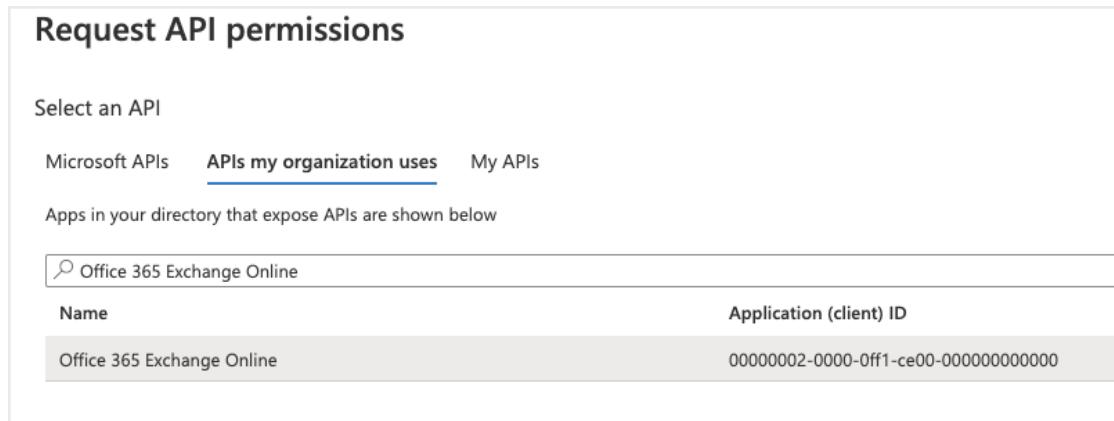
Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : [Add an Application ID URI](#)

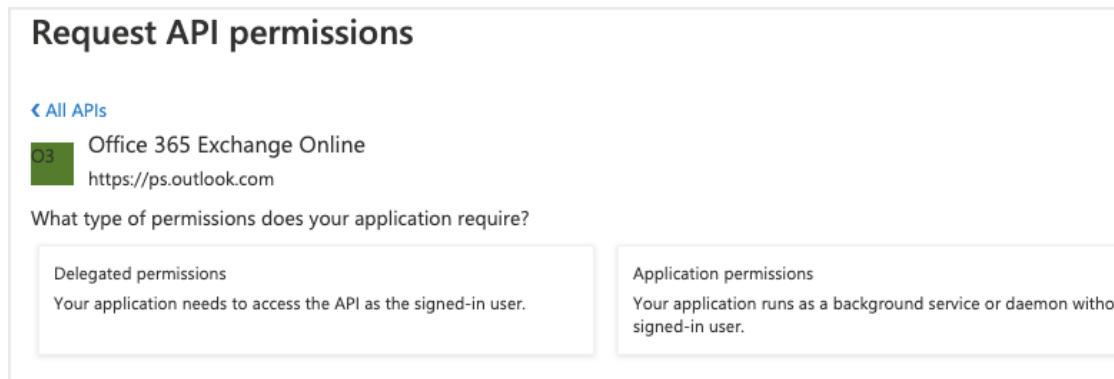
Managed application in I... : Cohesity DataProtect App

4. Add API permissions to the custom app:

1. **Add OAuth API permission** if the Microsoft 365 source tenant has OAuth enabled for secure communication:
  1. Under the **Manage** section, select **App Registrations** and click **Add a permission**.
  2. In the **Request API permissions** page, click the **APIs my organization uses** tab.
    - a. In the search bar, enter **Office 365 Exchange Online** then **click the API**. (Use the complete app name.)

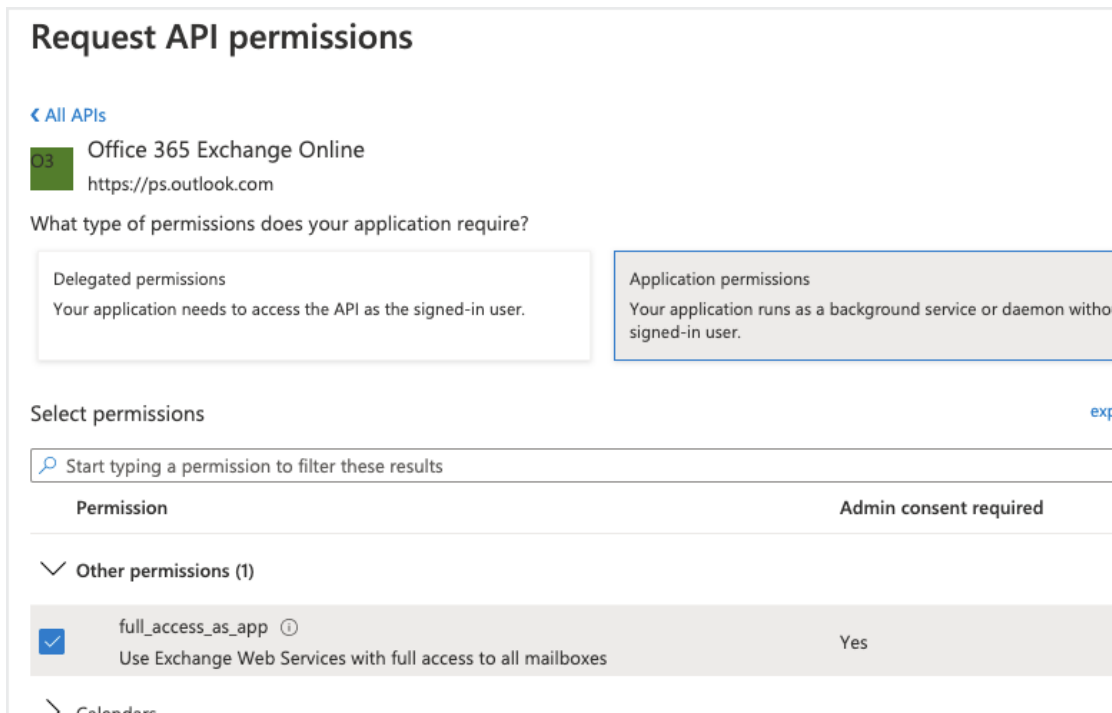


- b. In the Office 365 Exchange Online API, click **Application Permissions**.

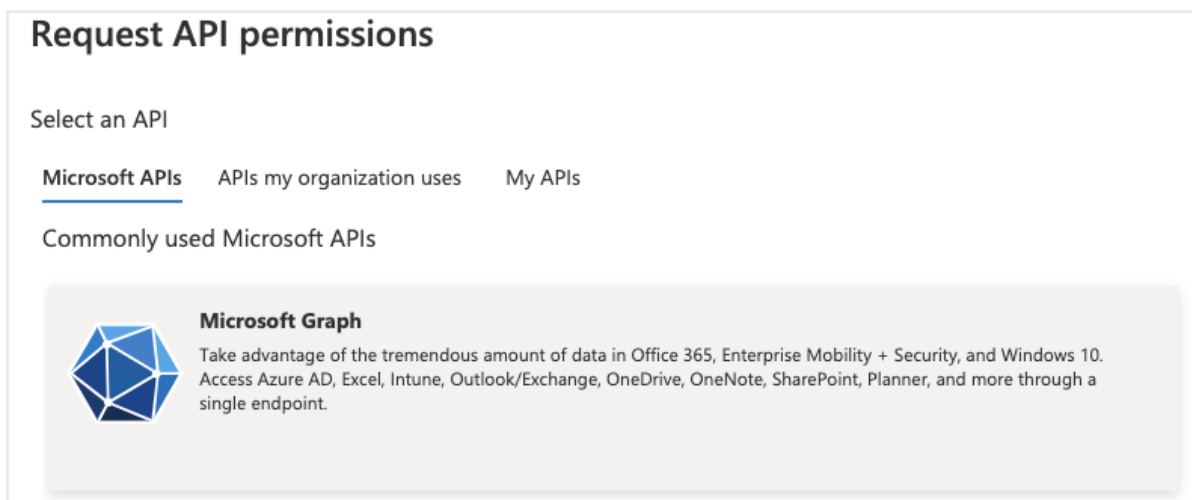


- c. Under **Other Permissions**, select `full_access_as_app` to enable OAuth and click **Add Permissions**.

App Permissions	Permission Type	Mailboxes
full_access_as_app	Application	Y






2. Add Graph API permissions:
  1. Under the **Manage** section, select **App Registrations**, and then click **Add a permission**.
  2. In the **Request API permissions** page, select **Microsoft Graph API**.



3. Click **Application Permissions** and add the permissions listed below for your Microsoft 365 application.

App Permissions	Permission Type	Mailboxes	OneDrive	SharePoint Online Sites	MS Teams
Channel.Create	Application	N/A	N/A	N/A	✔
Channel.ReadBasic.All	Application	N/A	N/A	N/A	✔
ChannelMember.ReadWrite.All	Application	N/A	N/A	N/A	✔
Directory.ReadWrite.All	Application	✔	✔	✔	✔
Files.ReadWrite.All	Application	N/A	✔	✔	✔
Group.Create	Application	N/A	N/A	N/A	✔
Group.ReadWrite.All	Application	N/A	✔	✔	✔
Reports.Read.All	Application	✔	✔	✔	✔
Sites.ReadWrite.All	Application	✔	✔	✔	✔
Sites.FullControl.All	Application	N/A	N/A	✔	✔
User.Read.All	Application	✔	✔	✔	✔
User.ReadWrite.All	Application	N/A	✔	✔	✔

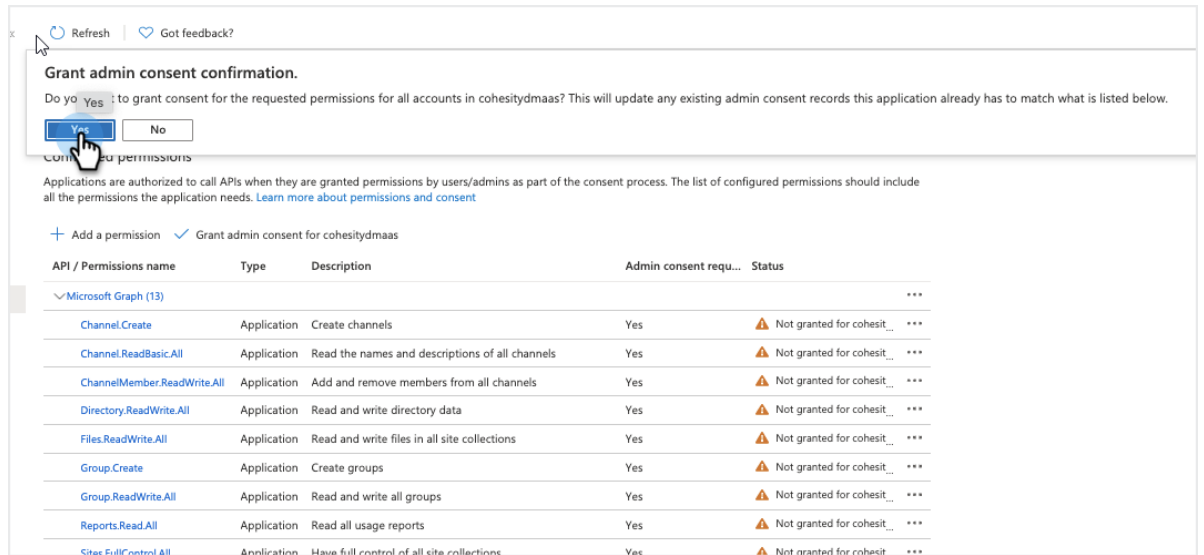
App Permissions	Permission Type	Mailboxes	OneDrive	SharePoint Online Sites	MS Teams
ChannelMessage.Read.All	Application	N/A	N/A	N/A	
Chat.Read.All	Application		N/A	N/A	N/A
Mail.ReadWrite	Application		N/A	N/A	N/A

4. Click **Add permissions**.
3. Add SharePoint permissions to the custom app:
  1. Under the **Manage** section, select **App Registrations** and click **Add a permission**.
  2. In the **Request API permissions** page, select **SharePoint**. (If you don't see it, scroll further down.)
    - a. Click **Delegated Permissions** and add the permissions listed below, then click **Add permissions**.
    - b. Click **Application Permissions** and add the permissions listed below, then click **Add permissions**.

Permission Type	Permissions Name
<b>Delegated</b>	AllSites.FullControl
	AllSites.Manage
	AllSites.Read
	MyFiles.Read
	MyFiles.Write
	Sites.Search.All
	TermStore.ReadWrite.All
	User.ReadWrite.All
<b>Application</b>	Sites.FullControl.All
	Sites.Manage.All
	Sites.ReadWrite.All
	TermStore.ReadWrite.All
	User.ReadWrite.All

5. Grant admin consent for the API permissions.
  1. Under **Configured permissions**, click **Grant admin consent**.
  2. On the Grant admin consent confirmation, click **Yes**.





6. Create a new client secret that will be used to register Microsoft 365 as a source in DataProtect as a Service for Government (FedRAMP).
  1. Under the **Manage** section, select **Certificates & secrets**.
    1. In the Client secrets section, click **New client secret**. Enter a **Description**.
    2. In the **Expires** drop-down, select how long the secret key will be valid.

- 3. Click **Add**.

**Add a client secret**

Description: Cohesity DataProtect Secret Key

Expires: Recommended: 6 months



- Recommended: 6 months
- 3 months
- 12 months
- 18 months
- 24 months
- Custom

- 2. Under **Client secrets**, click the **Copy** button next to the string under **VALUE**. You need the Value key of the client secret to register Microsoft 365 as a source in DataProtect as a Service for Government (FedRAMP).
- 3. Store the Value key in a secure location. After you exit this page, you will not be able to see the Value key again. If you lose your value key, you will need to create a new client secret.

**Client secrets**

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Cohesity DataProtect Secret Key	10/14/2023	[REDACTED]	aa0d893d-08d7-44df-a42b-2090bde65c43  

When you finish, your custom Azure app should include the permissions as shown below.

API / Permissions name	Type	Description	Admin consent requi...	Status
<span>▼</span> Microsoft Graph (13) <span style="float: right;">***</span>				
<a href="#">Channel.Create</a>	Application	Create channels	Yes	Granted for cohesi... <span>***</span>
<a href="#">Channel.ReadBasic.All</a>	Application	Read the names and descriptions of all channels	Yes	Granted for cohesi... <span>***</span>
<a href="#">ChannelMember.ReadWrite.All</a>	Application	Add and remove members from all channels	Yes	Granted for cohesi... <span>***</span>
<a href="#">Directory.ReadWrite.All</a>	Application	Read and write directory data	Yes	Granted for cohesi... <span>***</span>
<a href="#">Files.Read.All</a>	Application	Read files in all site collections	Yes	Granted for cohesi... <span>***</span>
<a href="#">Files.ReadWrite.All</a>	Application	Read and write files in all site collections	Yes	Granted for cohesi... <span>***</span>
<a href="#">Group.Create</a>	Application	Create groups	Yes	Granted for cohesi... <span>***</span>
<a href="#">Group.ReadWrite.All</a>	Application	Read and write all groups	Yes	Granted for cohesi... <span>***</span>
<a href="#">Reports.Read.All</a>	Application	Read all usage reports	Yes	Granted for cohesi... <span>***</span>
<a href="#">Sites.FullControl.All</a>	Application	Have full control of all site collections	Yes	Granted for cohesi... <span>***</span>
<a href="#">Sites.ReadWrite.All</a>	Application	Read and write items in all site collections	Yes	Granted for cohesi... <span>***</span>
<a href="#">User.Read.All</a>	Application	Read all users' full profiles	Yes	Granted for cohesi... <span>***</span>
<a href="#">User.ReadWrite.All</a>	Application	Read and write all users' full profiles	Yes	Granted for cohesi... <span>***</span>
<span>▼</span> Office 365 Exchange Online (1) <span style="float: right;">***</span>				
<a href="#">full_access_as_app</a>	Application	Use Exchange Web Services with full access to all mailboxes	Yes	Granted for cohesi... <span>***</span>
<span>▼</span> SharePoint (13) <span style="float: right;">***</span>				
<a href="#">AllSites.FullControl</a>	Delegated	Have full control of all site collections	Yes	Granted for cohesi... <span>***</span>
<a href="#">AllSites.Manage</a>	Delegated	Read and write items and lists in all site collections	No	Granted for cohesi... <span>***</span>
<a href="#">AllSites.Read</a>	Delegated	Read items in all site collections	No	Granted for cohesi... <span>***</span>
<a href="#">MyFiles.Read</a>	Delegated	Read user files	No	Granted for cohesi... <span>***</span>
<a href="#">MyFiles.Write</a>	Delegated	Read and write user files	No	Granted for cohesi... <span>***</span>
<a href="#">Sites.FullControl.All</a>	Application	Have full control of all site collections	Yes	Granted for cohesi... <span>***</span>
<a href="#">Sites.Manage.All</a>	Application	Read and write items and lists in all site collections	Yes	Granted for cohesi... <span>***</span>
<a href="#">Sites.ReadWrite.All</a>	Application	Read and write items in all site collections	Yes	Granted for cohesi... <span>***</span>
<a href="#">Sites.Search.All</a>	Delegated	Run search queries as a user	Yes	Granted for cohesi... <span>***</span>
<a href="#">TermStore.ReadWrite.All</a>	Delegated	Read and write managed metadata	Yes	Granted for cohesi... <span>***</span>
<a href="#">TermStore.ReadWrite.All</a>	Application	Read and write managed metadata	Yes	Granted for cohesi... <span>***</span>
<a href="#">User.ReadWrite.All</a>	Delegated	Read and write user profiles	Yes	Granted for cohesi... <span>***</span>
<a href="#">User.ReadWrite.All</a>	Application	Read and write user profiles	Yes	Granted for cohesi... <span>***</span>

## Set Additional Permissions for SharePoint Online

For SharePoint Online data protection, ensure that you set the required add-in permissions and tenant permissions below.

When you finish, your custom Azure app should include the permissions as shown below.

### Add-In Permissions in SharePoint Online

Make sure that you assign the following add-in permissions to the custom app. For more information, see [Add-in permissions in SharePoint](#) in the Microsoft documentation.

Scope URI	Required Rights
http://sharepoint/content/tenant	FullControl
http://sharepoint/content/sitecollection	FullControl
http://sharepoint/content/sitecollection/web	FullControl
http://sharepoint/content/sitecollection/web/list	FullControl
http://sharepoint/taxonomy	Read,Write

### Tenant Permissions

After you have [registered the custom app](#), configure the tenant permissions on the custom app.

To configure the tenant permissions:

1. Launch the **SharePoint Admin Center** using the URL: `https://<your-tenant>-admin.sharepoint.com/_layouts/15/AppInv.aspx`
2. In the **SharePoint Admin Center**, log in as the tenant admin.
3. In the **App ID and Title** section, perform the following:
  1. In the **App Id** field, enter the **AppID** of the custom app you have created and click **Lookup** to search for the custom app.
  2. In the **App Domain** field, enter `www.localhost.com` as the app domain.

**Important:** Do not enter any other string other than `www.localhost.com` in the **App Domain** field.

3. In the **Redirect URL** field, enter `https://localhost.com/` as the redirect URL.

**Important:** Do not enter any other URL other than `https://localhost.com/` in the **Redirect URL** field.

4. In the **Permission Request XML** field, enter the following values:

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
<AppPermissionRequest Scope="http://sharepoint/content/tenant"
Right="FullControl" />
</AppPermissionRequest
```

```

Scope="http://sharepoint/content/sitecollection"
Right="FullControl" />
<AppPermissionRequest
Scope="http://sharepoint/content/sitecollection/web"
Right="FullControl" />
<AppPermissionRequest
Scope="http://sharepoint/content/sitecollection/web/list"
Right="FullControl" />
<AppPermissionRequest Scope="http://sharepoint/taxonomy"
Right="Read,Write" />
</AppPermissionRequests>
    
```

### App Configuration for SharePoint Online

**App Id and Title**  
 App Id:    
 Title:   
 App Domain:   
 Example: "www.contoso.com"  
 Redirect URL:   
 Example: "https://www.contoso.com/default.aspx"

**App's Permission Request XML**  
 The permission required by the app.  
 Permission Request XML:  

```

<AppPermissionRequests AllowAppOnlyPolicy="true">
  <AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="FullControl" />
  <AppPermissionRequest Scope="http://sharepoint/content/sitecollection" Right="FullControl" />
  <AppPermissionRequest Scope="http://sharepoint/content/sitecollection/web" Right="FullControl" />
  <AppPermissionRequest Scope="http://sharepoint/content/sitecollection/web/list" Right="FullControl" />
  <AppPermissionRequest Scope="http://sharepoint/taxonomy" Right="Read,Write" />
</AppPermissionRequests>
    
```

4. Click **Create**.
5. In the **Do you trust <app\_title>?** page, perform the following:
  - a. From the drop-down, select **DO\_NOT\_DELETE\_SPLIST\_TENANTADMIN\_AGGREGATED\_SITECOLLECTIONS**.
  - b. click **Trust It**.

**Important:** If you have created your Microsoft 365 tenant on or after Sep 20, 2020, you must install SharePoint Online PowerShell. Using the global administrator account, run the following commands in an administrator PowerShell session:

```
Get-Module -Name Microsoft.Online.SharePoint.PowerShell -
ListAvailable | Select Name,Version
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
Install-Module -Name Microsoft.Online.SharePoint.PowerShell -Scope
AllUsers
Connect-SPOService -Url 'https://<tenant>-admin.sharepoint.com'
Set-SPOTenant -DisableCustomAppAuthentication $False
```

**Note:** Custom scripts setting is not supported in SharePoint.

## Enhance Backup of Large Microsoft 365 Data

When it comes to ingesting Microsoft 365 data, the size can vary from hundreds of terabytes (TBs) to a few petabytes (PBs) in some cases. One of the issues that may arise while performing the initial full backup of such large data is throttling from the Microsoft 365 APIs.

Cohesity recommends using only one application ID for Microsoft 365 backups. However, when you back up a large amount of data, using only one application ID may result in a prolonged ETA for the first full backup. Contact your Cohesity account team to determine the appropriate number of application IDs to optimize the performance while ensuring that the Microsoft Tenant Level Throttling limits are not exceeded, which may cause service failures for Microsoft 365.

After completing the first full backup, using multiple application IDs is not usually required. However, in certain situations, a single application ID may be inadequate. For guidance on the appropriate number of application IDs for incremental backups following the initial full backup, Contact your Cohesity account team.

Cohesity also supports Microsoft paid APIs to perform the first full backups faster. These APIs come with higher limits, ensuring the backups are performed faster at a higher API rate. The paid APIs are configured to be used in addition to the existing backup capacity allocated by Microsoft, rather than as a substitute, to help minimize additional costs.

## Register Microsoft 365 Sources

To start protecting Microsoft 365 applications, you need to register the Microsoft 365 domain as a source in DataProtect as a Service for Government (FedRAMP).

DataProtect as a Service for Government (FedRAMP) uses the [Microsoft Graph API](#) for object discovery, backup, and recovery in Microsoft 365. To use the Graph API, DataProtect as a Service for Government (FedRAMP) uses an Azure application created and registered on the Azure portal with necessary permissions. You can either let Cohesity [create the Azure application](#) or [manually enter Azure application](#) details while registering your Microsoft 365 domain as a source in DataProtect as a Service for Government (FedRAMP).

## Express Registration for Microsoft 365 Sources

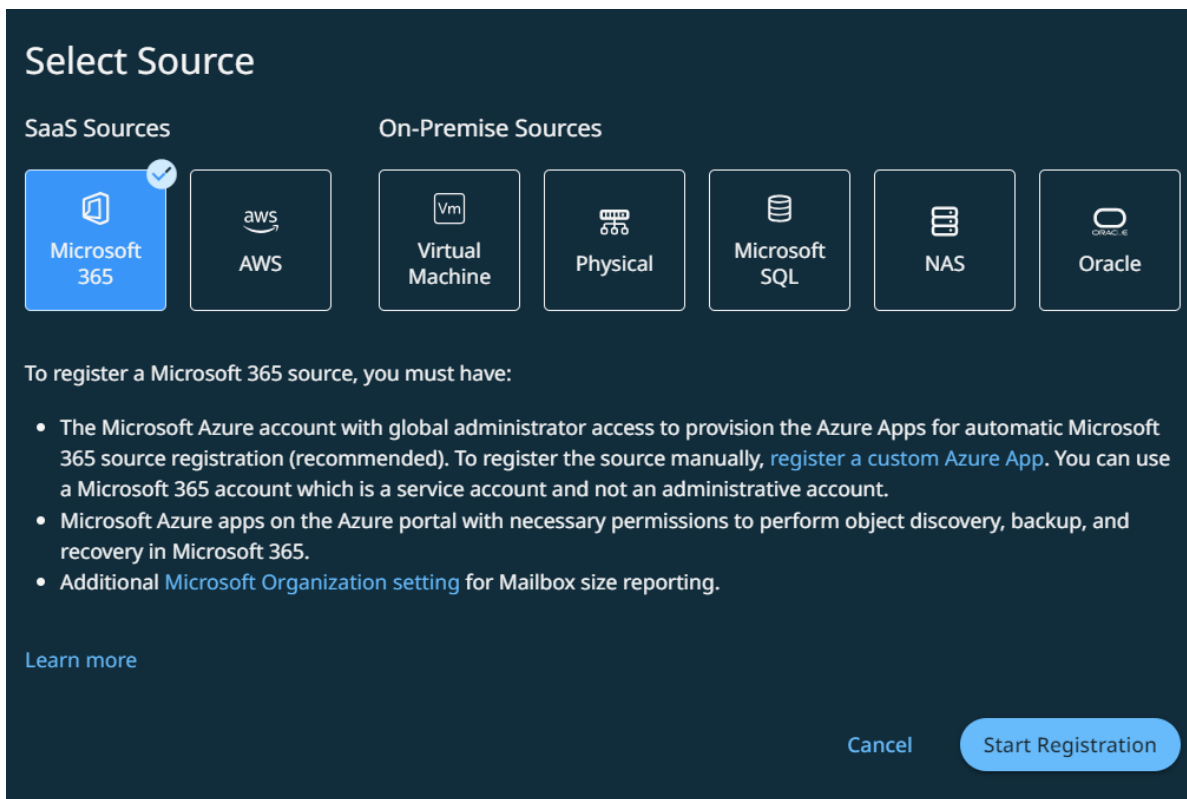
Before you register your Microsoft 365 domain, ensure that you have:

- [Added roles to the Microsoft 365 user account.](#)
- [Updated your Microsoft Organization setting for Mailbox size reporting.](#)

**Note:** Basic Auth is not supported for Microsoft 365 source registration.

To register your Microsoft 365 domain:

1. In **DataProtect as a Service**, navigate to the **Sources** page and click **+ Register Source** in the upper-right corner of the page.
2. In the **Select Source** dialog box, select **Microsoft 365** and click **Start Registration**.



3. In the **Source Details** section, select a cloud region for your data backups.
4. Choose the **Microsoft 365 Applications** to discover.

**Note:** Discovery selection change is not allowed for applications with protected objects.

**Note:** If the **Private Chats** and **Teams Posts** option is enabled under the **Mailbox** and **Teams** apps respectively, the Private Chats and Teams Posts will be backed up along with the corresponding Users and Teams respectively.

Private Chats and Teams Posts backup APIs are charged separately by Microsoft. All Azure apps configured by Cohesity must be linked to an [Azure subscription for billing](#). Backups of Mailboxes and Teams may fail if the Azure subscription configuration is not set appropriately.

This is an Early Access feature. Contact your Cohesity account team to enable the feature.

5. *[Optional]* You can enable the below options based on your requirement:



**Note:** Retaining the default values will speed up object discovery in the environment. The metadata required (which is fetched through these options) will be fetched during the backup of the objects and updated.

1. **Fetch Mailbox Info** to fetch and process the Mailbox information including the provisioning status, mailbox type, and in-place archival usage.

**Note:** You can enable this option to discover the Mailboxes of the users that were converted into Shared Mailboxes by revoking the user Exchange Online licenses.

2. **Fetch OneDrive Info** to fetch and process the OneDrive information including the provisioning status and storage quota.
3. **Include Users without MySite** to include users who have unprovisioned OneDrive or do not have MySite.
4. **Enable Site Tagging** to tag SharePoint Sites whether they are a Group Site or a Teams Site.

**Note:** Any Site that is tagged as a Group or Team will not be visible in the Sites section and these sites will be protected through the corresponding Group or Team protection.

6. In the **Account Credentials** section, enter the full **Username** of the Microsoft 365 user account with a valid SharePoint and Mailbox license.
7. In the **Azure Applications** section, enter the number of Azure applications that you want to create based on your requirements and click **Create**.

**Register Microsoft 365 Source**

- Fetch Mailbox Info ⓘ
- Fetch OneDrive Info ⓘ
- Include Users without MySite ⓘ
- Enable Site Tagging ⓘ

**Account Credentials**

Username  
dmasa-ai-automation4-rv2@cohesity.com ✓  
Enter full UPN (Eg: username@company.com)

**Azure Applications**

Number of Azure Apps to be created 1 **Create**

Cancel Register

**Note:** By default, an Azure application will be created. To better manage Microsoft 365 throttling, Cohesity recommends at least one Azure app.

- In the **Add Azure Application** form, copy the device code and click the **Microsoft Azure App** link to open the Microsoft Azure App authorization service in a new tab.

**Note:** If you prefer to create your Azure apps manually, see [Manual Registration for Microsoft 365 Sources](#).

- In the **Microsoft Azure App authorization** service, paste the copied code and click **Next**.
- Log in to Microsoft Azure, enter the **Username** and **Password** of your Microsoft 365 account and click **Sign in**.

**Note:** Ensure that your Microsoft 365 account has global administrator access.

- Follow the instructions to complete the authorization on the Microsoft Azure portal.
- Wait for Microsoft Azure Authorization to complete and then click **Register**.

For SharePoint Online data protection, ensure that you set the required add-in permissions and tenant permissions on the Azure application. For more information, see [Set additional permissions for SharePoint Online](#).

You can follow the Microsoft 365 source discovery and registration progress on the **Sources** page.

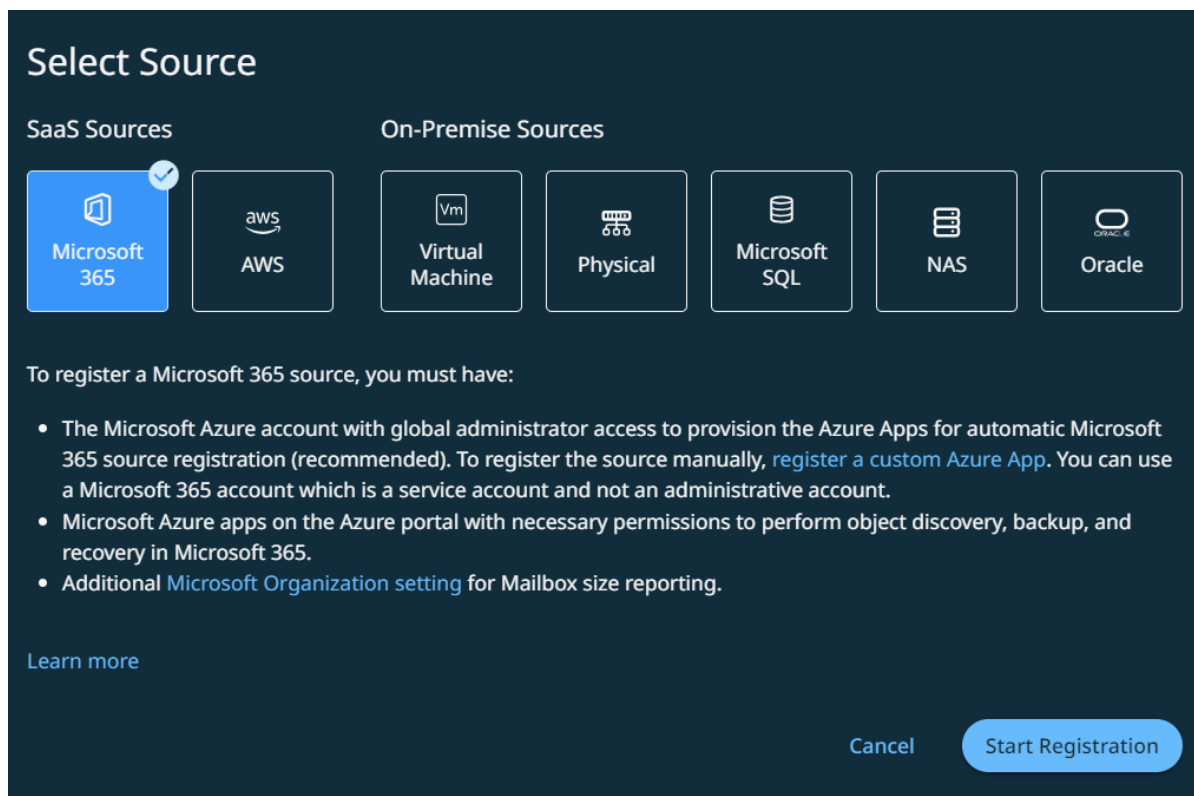
**Next** > You are now ready to protect your Microsoft 365 [Mailboxes](#), [OneDrives](#), [SharePoint Online Sites](#), and [Teams](#)!

## Manual Registration for Microsoft 365 Sources

**Note:** Basic Auth is not supported for Microsoft 365 source registration.

To register your Microsoft 365 domain manually, make sure you've met all the [Microsoft 365 Requirements](#) and then:

1. In **DataProtect as a Service**, navigate to the **Sources** page and click **+ Register Source** in the upper-right corner of the page.
2. In the **Select Source** dialog box, select **Microsoft 365** and click **Start Registration**.



3. In the **Source Details** section, select a cloud region for your data backups.

4. Choose the **Microsoft 365 Applications** to discover.

**Note:** Discovery selection change is not allowed for applications with protected objects.

**Note:** If the **Private Chats** and **Teams Posts** option is enabled under the **Mailbox** and **Teams** apps respectively, the Private Chats and Teams Posts will be backed up along with the corresponding Users and Teams respectively.

Private Chats and Teams Posts backup APIs are charged separately by Microsoft. All Azure apps configured by Cohesity must be linked to an [Azure subscription for billing](#). Backups of Mailboxes and Teams may fail if the Azure subscription configuration is not set appropriately.

This is an Early Access feature. Contact your Cohesity account team to enable the feature.

5. *[Optional]* You can enable the below options based on your requirement:

**Note:** Retaining the default values will speed up object discovery in the environment. The metadata required (which is fetched through these options) will be fetched during the backup of the objects and updated.

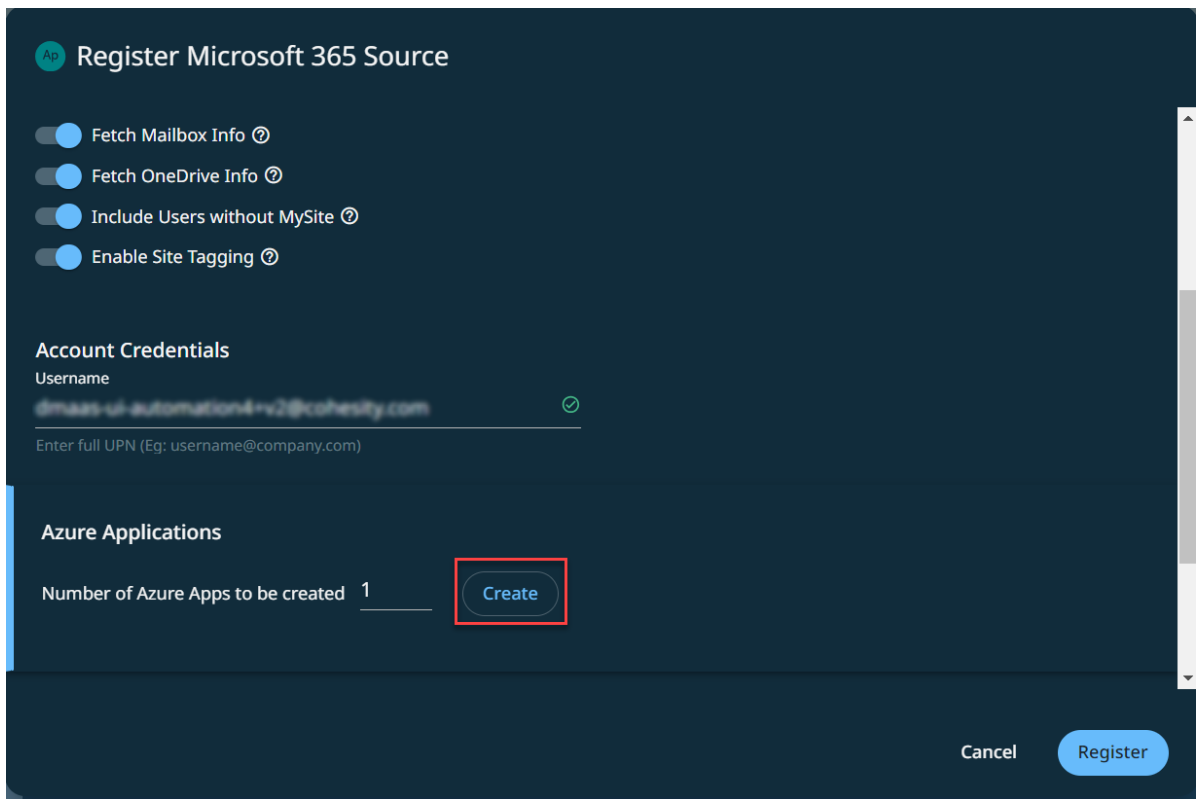
1. **Fetch Mailbox Info** to fetch and process the Mailbox information including the provisioning status, mailbox type, and in-place archival usage.

**Note:** You can enable this option to discover the Mailboxes of the users that were converted into Shared Mailboxes by revoking the user Exchange Online licenses.

2. **Fetch OneDrive Info** to fetch and process the OneDrive information including the provisioning status and storage quota.
3. **Include Users without MySite** to include users who have unprovisioned OneDrive or do not have MySite.
4. **Enable Site Tagging** to tag SharePoint Sites whether they are a Group Site or a Teams Site.

**Note:** Any Site that is tagged as a Group or Team will not be visible in the Sites section and these sites will be protected through the corresponding Group or Team protection.

- 6. In the **Account Credentials** section, enter the full **Username** of the Microsoft 365 user account with a valid SharePoint and Mailbox license.
- 7. In the **Azure Applications** section, enter the number of Azure applications that you want to create based on your requirements and click **Create**.



**Note:** By default, an Azure application will be created. To better manage Microsoft 365 throttling, Cohesity recommends at least one Azure app.

- 8. In the **Add Azure Application** form, click the **You can also add Azure App manually** link and then enter the **App ID** and **App Secret Key** that you noted down while registering your custom Azure app.

**Tip:** You can add multiple Azure apps for a Microsoft 365 source to load balance your backup and restore operations. Click **+** to add multiple Azure apps. When you do, ensure that you provide the valid **App ID** and **App Secret Key**.

9. Click **Register**.

For SharePoint Online data protection, ensure that you set the required add-in permissions and tenant permissions on the Azure application. For more information, see [Set additional permissions for SharePoint Online](#).

You can follow the Microsoft 365 source discovery and registration progress on the **Sources** page.

**Next** > You are now ready to protect your Microsoft 365 [Mailboxes](#), [OneDrives](#), [SharePoint Online Sites](#), and [Teams](#)!

## Manage Microsoft 365 Source Registration

After registering your Microsoft 365 domain as a source, you can:

- Update the Microsoft 365 source configuration.
- Refresh the source details.
- Unregister the Microsoft 365 domain from Cohesity.

### Update the Microsoft 365 Source Configuration

After registering your Microsoft 365 source on Cohesity, you might have changed the Microsoft 365 domain configuration by:

- Changing the credentials of Microsoft 365 user account credentials.
- Updating the app secret by adding more permissions to the custom app.
- Creating a new app ID.

You can update the Microsoft 365 details provided during the registration process with the latest Microsoft 365 configuration details.

To edit the Microsoft 365 source configuration:.

1. In **DataProtect as a Service**, navigate to **Sources**.
2. Click the actions menu ( **⋮** ) next to the Microsoft 365 source and select **Edit**.
3. In the **Register Microsoft 365 Source** page, update the required configurations.
4. Click **Register**.

To edit Azure App ID:

**Note:** Azure App ID permissions must be provided for successful Private Chats and Teams Posts backup.

1. In **DataProtect as a Service**, navigate to **Sources**.
2. Click the actions menu next to the Microsoft 365 source and select **Edit**.
3. Click **Update App Permission**. This button is displayed if the **Private Chats** or **Teams Posts** discovery is enabled under the **Mailbox** or **Teams** apps respectively.
4. Copy the displayed device code to link with Microsoft Azure automatically. The code is valid for 15 minutes.
5. Open the Microsoft Azure App authorization service in a new tab and paste the copied code to complete authorization. When prompted to log in to Microsoft Azure, ensure to use an account with global administrator access.
6. Complete the authorization and click **Update**.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

### Refresh the Microsoft 365 Source

You can refresh the Microsoft 365 domain configuration and fetch the latest changes on the Microsoft 365 domain.

To refresh the Microsoft 365 Source Configuration:

1. Navigate to **Sources**.
2. Click the actions menu (  ) next to the Microsoft 365 source and select **Refresh**.

### Unregister the Microsoft 365 Domain

If you plan to stop taking the backup of your Microsoft 365 domain, you can unregister the Microsoft 365 source from the DataProtect as a Service for Government (FedRAMP).

To unregister the Microsoft 365 domain:

1. Navigate to **Sources**.
2. Click the actions menu (  ) next to the Microsoft 365 source and select **Unregister**.

## Explore Microsoft 365 Sources

After you have registered your Microsoft 365 domain as a source, you can review the Users, Mailboxes, OneDrives, Sites, and Teams that DataProtect as a Service for Government (FedRAMP) discovered for the source.

## Overview

To explore your Microsoft 365 source details, under Sources, find the Microsoft 365 source and click it.

The discovered Mailboxes, OneDrives, Sites, and Teams are listed in their respective tabs on the Microsoft 365 source details page. In addition, the source details page also displays a glance bar that communicates:

- **Object Counts.** The number of Users, Mailboxes, OneDrives, Sites and Teams discovered from the source.
- **Protected/Unprotected Objects.** The protected and unprotected count of Microsoft 365 objects in the source. For example, the number of protected and unprotected Mailboxes in the source.
- **Size.** The size (FETB) of protected and unprotected Microsoft 365 application data. For example, the amount of protected and unprotected Mailboxes data in the source.
- **Cross-App Counts.** Summary of protected and unprotected objects across all the Microsoft 365 applications in the source.

## Interpret the Numbers

Every Microsoft 365 licensed user is counted as a User in Cohesity. A User might have both a Mailbox and a OneDrive. Or a User can have either a Mailbox or a OneDrive. In addition, Shared Mailboxes and Resource Mailboxes are not counted as Users. That means that the count of Mailboxes, OneDrives, and Users is not expected to be the same.

For example, in the source details page below, the right side of the glance bar lists **17** Users but the number of Mailboxes listed on the left side of the glance bar is **22**.

The screenshot shows the DataProtect interface for a Microsoft 365 source. At the top, there is a search bar and navigation icons. Below the search bar, the source name is displayed. The interface has tabs for Mailbox, OneDrive, Site, and Teams. A summary bar shows the following data:

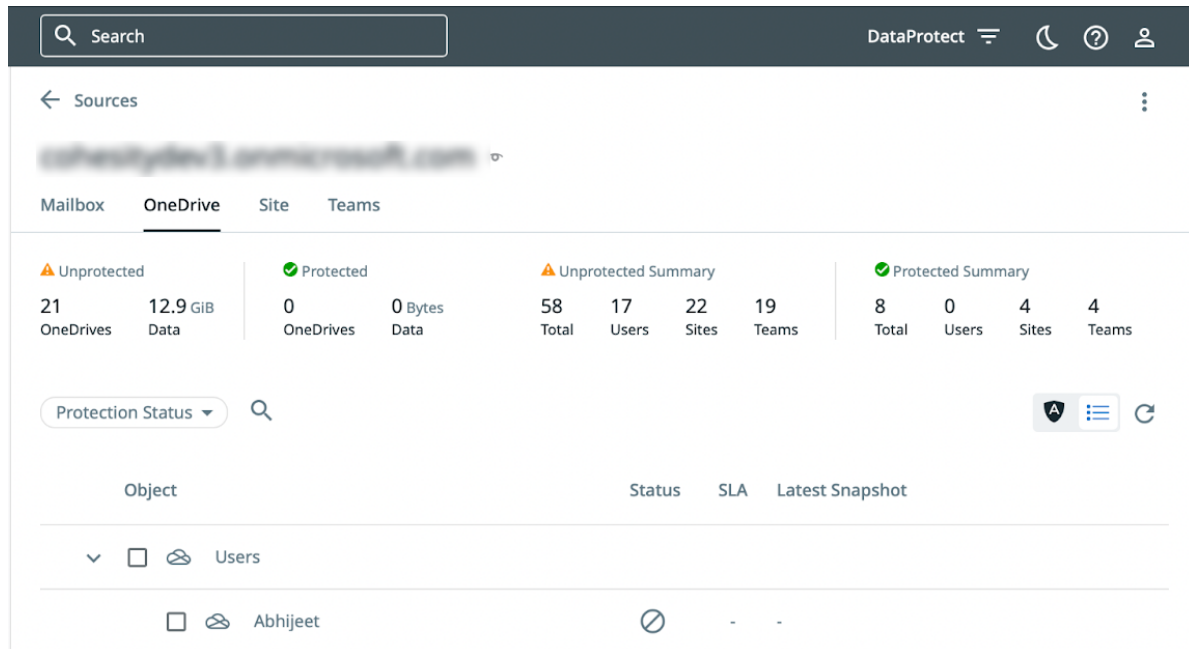
Unprotected		Protected		Unprotected Summary				Protected Summary			
22	0 Bytes	0	0 Bytes	58	17	22	19	8	0	4	4
Mailboxes	Data	Mailboxes	Data	Total	Users	Sites	Teams	Total	Users	Sites	Teams

Below the summary bar, there is a filter for Protection Status and a search icon. A table of objects is displayed with the following columns: Object, Status, SLA, and Latest Snapshot.

Object	Status	SLA	Latest Snapshot
> [ ] [ ] Users			
[ ] [ ] Abhijeet	⊘	-	-



Similarly, in the following details page, the right side of the glance bar lists **17** users but the number of OneDrives listed on the left side of the glance bar is **21**.



**Next** > You are now ready to protect your Microsoft 365 Mailboxes, OneDrives, SharePoint Online Sites, and Teams!

## Exchange Online Mailboxes

Microsoft Exchange Online is a SaaS application that is bundled in your Microsoft 365 subscription service. It is a hosted messaging solution that delivers the capabilities of Microsoft Exchange Server as a cloud-based service. It gives users access to email, calendar, contacts, and tasks from PCs, the web, and mobile devices. Using the policy-based data protection solution from DataProtect as a Service for Government (FedRAMP), you can protect Exchange Online data on Microsoft 365.

### Considerations

- PST download is supported only for mailbox items and not entire mailboxes.
- The exported PST of the mailbox items is valid for 72 hours. Ensure that you download the PST file within 72 hours of the recovery task completion.
- PST recovery of emails with more than 2000 recipients is not supported.
- Backup and download of the following is not supported:
  - Self-message (messages sent to self)
  - Saved or pinned messages property in the conversation
  - Meeting recordings metadata from private chats

- In Recoverable Items,
  - only deletions, Purges, Discovery Holds, and SubstrateHolds folders are currently supported.

**Note:** SubstrateHolds folders support is a Private Preview feature. Private Preview was termed as Early Access in the earlier releases. Contact your Cohesity account team to enable the feature.

- Audits, Calendar Logging, and Versions folders are not supported.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- Granular recovery and search is not supported for Recoverable Items. The admin must recover the complete mailbox to recover the Recoverable Items.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- Converted-shared mailboxes are not backed up by default. To enable backup of converted-shared mailboxes, contact [Cohesity Support](#).
- The [Retirement of RBAC Application Impersonation in Exchange Online](#) does not impact the Microsoft 365 Exchange Online Mailboxes, Teams, and Groups protection workflow on the Cohesity cluster.
- Exchange Online Mailboxes protection is supported only for users present on Azure AD and not for users on the on-premises Active Directory.
- Exchange Online Mailboxes protection is supported for:
  - users present in Azure AD
  - hybrid setup with users present on Azure AD

It is not supported for:

- users on the on-premises Active Directory
- users natively on the on-premises Active Directory that are synchronized to Azure AD.
- By default, the Conversation History/Team Chat folder is excluded during Exchange Online backup.
- Following the Microsoft changes for EWS APIs, Cohesity no longer backs up mailbox items of the type **IPM.Teams.SkypeMessage**. For more details, see the [KB Article](#).

- [Microsoft 365 Backup Storage](#) service is supported for Mailboxes.

**Note:** This is a Private Preview feature. Private Preview was termed as Early Access in the earlier releases. Contact your Cohesity account team to enable the feature.

## Protect Microsoft 365 Mailboxes

Once you have [registered your Microsoft 365 domain](#) as a source, you're ready to protect the user Mailboxes in your domain.

To protect your Microsoft 365 Mailboxes:

**Note:** If the **Private Chats** option is enabled under Mailbox during app registration, the Private Chats will be backed up along with the corresponding Users.  
Mailboxes backup may fail if the Azure subscription configuration is not set appropriately.  
This is an Early Access feature. Contact your Cohesity account team to enable the feature.

1. In **DataProtect as a Service**, under **Sources**, find the Microsoft 365 source and click on it.
2. Click the **Mailbox** tab.
3. Select the individual Mailboxes you wish to protect or:
  - Click **Users > Select All Child Objects** to protect all the Mailboxes in this source.
  - Click **Users > Auto Protect This** to protect all the Mailboxes *plus any future additional Mailboxes* on that source.
  - Click the **Security Groups** icon and select the security group to protect the Mailboxes of the users in the security group. For more information, see [Security Groups](#).

Security groups based user import also supports nested security groups.

For example, if a security group (AA) includes members (X and Y) and security groups (BB and CC), the import process includes the members (X and Y) and the members of security groups (BB and CC).

Cohesity supports only users and not devices in Security Groups. This is an Early Access feature. Contact your Cohesity account team to enable the feature.

1. Click the **Protect** icon above the list.
2. Choose a policy to specify backup frequency and retention. If you don't have a policy, you can easily [create one](#).
3. Under **Settings**, edit the **Start Time** if necessary.
4. Under **Additional Settings**, you can enable **Indexing** and other [additional settings](#).

**Note:** Indexing is enabled by default. If you plan to [recover individual emails or folders](#), in addition to whole Mailboxes, you need to enable **Indexing** in this step. When you do, you can include or exclude specific Mailboxes from indexing.

5. Click **Protect**.

**Note:** The backups start immediately after you protect the objects, regardless of the time you set for the protection run.

**Next >** When the first protection run completes, you will be ready to [recover your protected Mailboxes](#) when and if you need to.

### Additional Settings

Advance Settings	Description
<b>Start Time</b>	Available only if the selected policy is set to <b>Backup Daily</b> . Indicates what time the protection run should start. Enter the <b>Start Time</b> and select <b>AM</b> or <b>PM</b> . The default time zone is the browser's time zone. You can change the time zone of the protection run by selecting a different time zone here.
<b>SLA</b>	The service-level agreement (SLA) defines how long the administrator expects a protection run to take. Enter: <ul style="list-style-type: none"> <li>• <b>Full</b>. The number of minutes you expect a full protection run, which captures all the blocks in an object, to take.</li> <li>• <b>Incremental</b>. The number of minutes you expect an incremental protection run, which captures only the changed blocks in an object, to take.</li> </ul>

Advance Settings	Description
<p><b>Cancel Runs at Quiet Time Start</b></p>	<p><i>(Available only if the selected policy has at least one <b>Quiet Time</b>)</i></p> <p>When enabled, all the protection runs that are currently executing will cancel when the Quiet Time period starts. By default, this setting is disabled, meaning that after a protection run starts, it continues to execute even when a Quiet Time period starts. However, new protection runs will not start during a Quiet Time.</p>
<p><b>Indexing</b></p>	<p>By default, indexing is enabled.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p><b>Note:</b> Indexing is mandatory for granular restore of an Exchange Online mailbox , such as restoring a folder or restoring an email.</p> </div>
<p><b>Exclusions</b></p>	<p>Select the folders that you plan to exclude from the backup or click <b>Add</b> to add custom folders that you want to exclude from the backup.</p> <p>To protect the Recoverable Items, ensure to deselect <b>Archive Recoverable Items</b> and <b>Recoverable Items</b>.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p><b>Note:</b> This is an Early Access feature. Contact your Cohesity account team to enable the feature.</p> </div>

### Manage Existing Protection

Edit protection settings, change the policy, and start, stop, & pause protection.


Once you have [applied protection](#) to the objects in your sources, DataProtect as a Service for Government (FedRAMP) makes it easy to make changes to that protection quickly. You can:

- Edit additional settings like **End Date, Exclusions, Alerts**, and more.
- Apply a different policy.
- Start an on-demand protection run, pause and resume it, or even remove protection.

#### Edit Protection Settings

To edit protection settings:

1. In **DataProtect as a Service**, navigate to **Sources**.
2. Click into the **Source** name.
3. Select **Show All > Protected** and use the other filters, search box, and views at the top to narrow your search.

4. Click the **Actions** menu (  ) next to the object and select **Edit Protection** to open the protection settings for that object.

**Apply a New Protection Policy**

To change the **Policy**, click the drop-down and select a different policy. To help you choose, each policy in the list shows the **Backup** frequency and the **Retain** period for each backup. If you don't have a policy that meets your needs, scroll to the bottom of the list and click **Create Policy** to create your own policy.

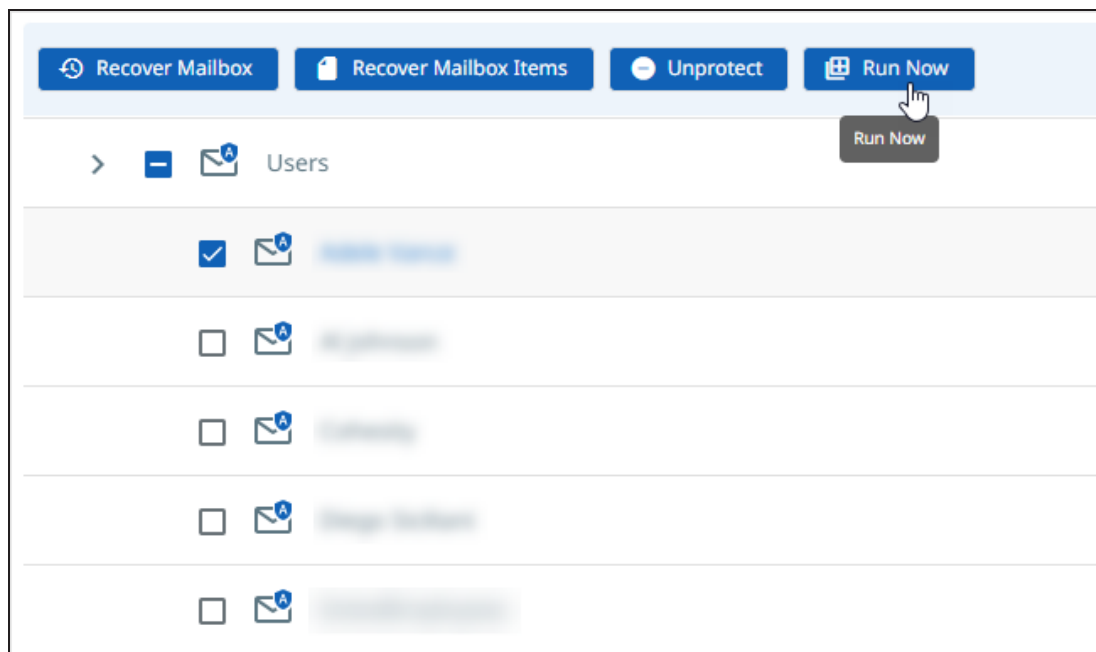
**Edit Additional Protection Settings**

In **DataProtect as a Service**, under **Settings**, you can change the protection **Start Time** (and select the **Time Zone**).

Click the drop-down next to **Additional Settings** to change more options. See [Additional Protection Settings](#) for details.

**Start, Stop, or Remove Protection**

When you select protected objects in one of your sources, DataProtect as a Service for Government (FedRAMP) presents buttons for the actions that are possible for those objects.



With the protected objects selected, you can click:

- **Recover Mailbox** to recover the mailbox.
- **Recover Mailbox Items** to recover the mailbox items.
- **Run Now** to start an on-demand protection run immediately.
- **Unprotect** to remove protection from the object.

**Tip:** If a protected object is deleted from the source, you can search the object using Global Search and unprotect it.

Additional Settings

Advance Settings	Description
<b>Start Time</b>	Available only if the selected policy is set to <b>Backup Daily</b> . Indicates what time the protection run should start. Enter the <b>Start Time</b> and select <b>AM</b> or <b>PM</b> . The default time zone is the browser's time zone. You can change the time zone of the protection run by selecting a different time zone here.
<b>SLA</b>	The service-level agreement (SLA) defines how long the administrator expects a protection run to take. Enter: <ul style="list-style-type: none"> <li>• <b>Full.</b> The number of minutes you expect a full protection run, which captures all the blocks in an object, to take.</li> <li>• <b>Incremental.</b> The number of minutes you expect an incremental protection run, which captures only the changed blocks in an object, to take.</li> </ul>
<b>Cancel Runs at Quiet Time Start</b>	<i>(Available only if the selected policy has at least one Quiet Time)</i> When enabled, all the protection runs that are currently executing will cancel when the Quiet Time period starts. By default, this setting is disabled, meaning that after a protection run starts, it continues to execute even when a Quiet Time period starts. However, new protection runs will not start during a Quiet Time.
<b>Indexing</b>	By default, indexing is enabled.  <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-left: 20px;"> <p><b>Note:</b> Indexing is mandatory for granular restore of an Exchange Online mailbox , such as restoring a folder or restoring an email.</p> </div>
<b>Exclusions</b>	Select the folders that you plan to exclude from the backup or click <b>Add</b> to add custom folders that you want to exclude from the backup.  To protect the Recoverable Items, ensure to deselect <b>Archive Recoverable Items</b> and <b>Recoverable Items</b> .  <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-left: 20px;"> <p><b>Note:</b> This is an Early Access feature. Contact your Cohesity account team to enable the feature.</p> </div>

## Recover Microsoft 365 Mailboxes and Mailbox Items

After you [protect your users' Microsoft 365 Mailboxes](#), you can recover them — as [whole Mailboxes](#) or [individual mailbox items](#) — from DataProtect as a Service for Government (FedRAMP).

**Note:** You can recover Mailboxes to a target Mailbox as long as the Microsoft 365 domain for the target Mailbox is registered within the same [cloud region](#) as the Microsoft 365 domain of the Mailbox being recovered.

You can recover:

- [Whole Mailboxes](#)
- [Individual Mailbox Items](#)

### Recover User Mailboxes

To recover protected Microsoft 365 user Mailboxes:

1. In **DataProtect as a Service**, go to **Sources** to set up your recovery task.
2. Click on the **Source** name and select the **Mailbox** tab.
3. Above the tree, select **Show All > Protected**.
4. Find the Mailbox you need and click the **Recover** icon on that row to open the **New Recovery** form with the Latest snapshot (protection run).
5. In the **New Recovery** form, if you need to add more Mailboxes and/or recover from an earlier backup, click the **Edit** icon in the top right of the form.
  - To add **Mailboxes**, enter a **Search** term on the left, locate the other Mailboxes, and select them.
  - To use a different **Recovery Point** for a Mailbox, click the **Edit** icon on the tile for that Mailbox. Find the recovery point you need and click **Select Recovery Point**.

Click **Next: Recover Options** to return to the form.

6. Under **Recover To**, select **Original Location** or **New Location**.  
If you choose **New Location**, select a **Registered Source** and the **Target Mailbox**.
7. Select your **Recovery Options**:
  - **Continue on Error**. Enable to recover even if errors occur when recovering Mailboxes. For example, if one of the Mailboxes cannot be recovered, Cohesity will still attempt to recover the other selected Mailboxes.
  - **Task Name**. Change the default name of the recovery task.
  - **Include Recoverable Items**. Toggle ON to **Recover Recoverable Items**.



**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- **Include Archive Recoverable Items.** Toggle ON to **Recover Archive Recoverable Items**.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

8. Click **Start Recovery**.

**Next** > Protect your Microsoft 365 [OneDrives](#), [SharePoint Online Sites](#), and [Teams](#) so you can recover them easily when you need to, as well!

### Recover Mailbox Items

After you [protect your users' Microsoft 365 Mailboxes](#), you can recover the Mailbox items such as [individual emails](#), [folders](#), [calendar invites](#), [contacts](#), [notes](#), or [tasks](#) — from DataProtect as a Service for Government (FedRAMP).

#### Recover Emails

To recover specific emails from a protected Microsoft 365 user Mailbox:

1. In **DataProtect as a Service**, go to **Sources** to set up your recovery task.
2. Click into the **Source** name and select the **Mailbox** tab.
3. Use the search or filter options, find and select the user you need, and click the **Recover Mailbox Items** icon above the list to open the **New Recovery** form.

**Tip:** You can also use Global Search to locate, filter, and select the Mailbox you need. Click the Global Search box at the top or type slash (/) anywhere to start your search.

4. Select **Emails & Folders** from the **Item Type** drop-down.
5. Use the '\*' wildcard character or enter the text to search for emails with a matching subject in the **Search** bar. Select the emails to recover from the search results.

**Or**

Click **Advanced Search** and select **Emails** to search based on these filters:

Filters	Description
<b>Subject</b>	Subject line in the email.
<b>From</b>	Mail sender email address.
<b>To</b>	Mail recipient email address. Use a comma or space separator to enter multiple addresses.
<b>Date Range</b>	Using the calendar, select a specific date range to search the emails.
<b>Email Type</b>	Select one of the email types: <ul style="list-style-type: none"> <li>• All Emails</li> <li>• Only emails with attachments</li> <li>• Only emails without attachments</li> </ul>
<b>cc</b>	The email address in the Cc: line of the email. Use a comma or space separator to enter multiple addresses.
<b>bcc</b>	The email address in the Bcc: line of the email. Use a comma or space separator to enter multiple addresses.
<b>Search in Folder</b>	Search for the email within the specified folder. For example, Inbox, Drafts, and so on. Use a comma or space separator to enter multiple folder names.

To use a different **Recovery Point** for a Mailbox, click the **Edit** icon on the tile for that Mailbox. Find the recovery point you need and click **Select Recovery Point**.

- Click **Next: Recover Options** to return to the form.
- Under **Recover To**, select **Original Location** or **New Location**.

If you choose **New Location**, select a **Registered Source** and the **Target Mailbox**, and specify the **Folder** name to which you plan to recover.

**Note:** If a folder with the specified name does not exist, Cohesity creates the folder and recovers the emails to that folder.

Select **Export as PST** to export the backed up emails as a PST file, and provide a password for the exported PST file.

**Note:** Once the recovery task is completed, the exported PST file is valid for 72 hours. Ensure that you download the PST within 72 hours. For more information, see [Download Exported PST File](#).

This is an Early Access feature. Contact your Cohesity account team to enable the feature.

**Note:** PST recovery of emails with more than 2000 recipients is not supported.

8. Select your **Recovery Options**:
  - **Continue on Error**. Enable to recover even if errors occur when recovering Mailboxes. For example, if one of the emails cannot be recovered, Cohesity will still attempt to recover the other selected emails.
  - **Task Name**. Change the default name of the recovery task.
9. Click **Start Recovery**.

#### Recover Mailbox Folders

To recover specific folders from a protected Microsoft 365 user Mailbox:

1. Go to **Sources** to set up your recovery task.
2. Click into the **Source** name and select the **Mailbox** tab.
3. Use the search or filter options, find and select the user you need, and click the **Recover Mailbox Items** icon above the list to open the **New Recovery** form.

**Tip:** You can also use Global Search to locate, filter, and select the Mailbox you need. Click the Global Search box at the top or type slash (/) anywhere to start your search.

4. On the **New Recovery** page, select **Emails & Folders** from the **Item Type** dropdown
5. Click **Advanced Search** and select **Folders**.
6. Enter the **Folder Name** and click **Apply**. Select the folders to recover from the search results.

To use a different **Recovery Point** for a Mailbox, click the **Edit** icon on the tile for that Mailbox. Find the recovery point you need and click **Select Recovery Point**.
7. Click **Next: Recover Options** to return to the form.

- Under **Recover To**, select **Original Location** or **New Location**.

If you choose **New Location**, select a **Registered Source** and the **Target Mailbox**, and specify the **Folder** name to which you plan to recover.

**Note:** If a folder with the specified name does not exist, Cohesity creates the folder and recovers the data to it.

Select **Export as PST** to export the backed up mailbox folders as a PST file, and provide a password for the exported PST file.

**Note:** Once the recovery task is completed, the exported PST file is valid for 72 hours. Ensure that you download the PST within 72 hours. For more information, see [Download Exported PST File](#).

This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- Select your **Recovery Options**:

- **Continue on Error.** Enable to recover even if errors occur when recovering Mailboxes. For example, if one of the emails cannot be recovered, Cohesity will still attempt to recover the other selected emails.
- **Task Name.** Change the default name of the recovery task.

- Click **Start Recovery**.

#### Recover Calendar Invites

You can recover specific calendar invites from a protected Microsoft 365 user Mailbox. However, if you plan to recover the entire calendar, then [recover the mailbox folder](#) called **Calendar**.

To recover calendar Invites:

- Go to **Sources** to set up your recovery task.
- Click into the **Source** name and select the **Mailbox** tab.
- Use the search or filter options, find and select the user you need, and click the **Recover Mailbox Items** icon above the list to open the **New Recovery** form.

**Tip:** You can also use Global Search to locate, filter, and select the Mailbox you need. Click the Global Search box at the top or type slash (/) anywhere to start your search.

- On the **New Recovery** page, select **Calendars** from the **Item Type** drop-down.

- Use the '\*' wildcard character or enter the text to search for calendar items with a matching subject of the calendar invite in the **Search** bar. Select the calendar invite to recover from the search results.

**Or**

Click **Advanced Search** and search calendar invite based on these filters and click **Apply**:

Filters	Description
<b>Subject of Event</b>	Subject line in the calendar invite.
<b>Organizer</b>	The email address of the event organizer.
<b>Invitee</b>	Event recipients' email addresses. Use a comma or space separator to enter multiple addresses.
<b>Invitation Date</b>	Using the calendar, select a specific date range to search the calendar invites.

To use a different **Recovery Point** for a Mailbox, click the **Edit** icon on the tile for that Mailbox. Find the recovery point you need and click **Select Recovery Point**.

- Click **Next: Recover Options** to return to the form.
- Under **Recover To**, select **Original Location** or **New Location**.

If you choose **New Location**, select a **Registered Source** and the **Target Mailbox**, and specify the **Folder** name to which you plan to recover.

**Note:** If a folder with the specified name does not exist, Cohesity creates the folder and recovers the calendar invite(s) to that folder.

Select **Export as PST** to export the backed up calendar invites as a PST file, and provide a password for the exported PST file.

**Note:** Once the recovery task is completed, the exported PST file is valid for 72 hours. Ensure that you download the PST within 72 hours. For more information, see [Download Exported PST File](#).  
This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- Select your **Recovery Options**:

- **Continue on Error.** Enable to recover even if errors occur when recovering calendar invites. For example, if one of the calendar invites cannot be recovered, Cohesity will still attempt to recover the other selected calendar invite.
- **Task Name.** Change the default name of the recovery task.

9. Click **Start Recovery**.

### Recover Contacts

You can recover specific contacts from a protected Microsoft 365 user Mailbox. However, if you plan to recover the complete contacts, then [recover the mailbox folder](#) called **Contacts**.

To recover specific contacts:

1. Go to **Sources** to set up your recovery task.
2. Click into the **Source** name and select the **Mailbox** tab.
3. Use the search or filter options, find and select the user you need, and click the **Recover Mailbox Items** icon above the list to open the **New Recovery** form.

**Tip:** You can also use Global Search to locate, filter, and select the Mailbox you need. Click the Global Search box at the top or type slash (/) anywhere to start your search.

4. On the **New Recovery** page, select **Contacts** from the **Item Type** drop-down.
5. Use the '\*' wildcard character or enter the text to search for contacts with a matching contact name in the **Search** bar. Select the contact to recover from the search results.

**Or**

Click **Advanced Search** and search the contact based on these filters and click **Apply**:

Filters	Description
<b>First Name</b>	The first name of the contact.
<b>Last Name</b>	The last name of the contact.
<b>Email Address</b>	The email address of the contact.
<b>Invitation Date</b>	Using the calendar, select a specific date range to search the calendar invites.

To use a different **Recovery Point** for a Mailbox, click the **Edit** icon on the tile for that Mailbox. Find the recovery point you need and click **Select Recovery Point**.

6. Click **Next: Recover Options** to return to the form.
7. Under **Recover To**, select **Original Location** or **New Location**.

If you choose **New Location**, select a **Registered Source** and the **Target Mailbox**, and specify the **Folder** name to which you plan to recover.

**Note:** If a folder with the specified name does not exist, Cohesity creates the folder and recovers the contact(s) to that folder.

Select **Export as PST** to export the backed up contacts as a PST file, and provide a password for the exported PST file.

**Note:** Once the recovery task is completed, the exported PST file is valid for 72 hours. Ensure that you download the PST within 72 hours. For more information, see [Download Exported PST File](#).

This is an Early Access feature. Contact your Cohesity account team to enable the feature.

8. Select your **Recovery Options**:
  - **Continue on Error**. Enable to recover even if errors occur when recovering the contacts. For example, if one of the contacts cannot be recovered, Cohesity will still attempt to recover the other selected contacts.
  - **Task Name**. Change the default name of the recovery task.
9. Click **Start Recovery**.

#### Recover Notes

You can recover specific notes from a protected Microsoft 365 user Mailbox. However, if you plan to recover the complete set of notes in the user Mailbox, then [recover the mailbox folder](#) called **Notes**.

To recover specific notes:

1. Go to **Sources** to set up your recovery task.
2. Click into the **Source** name and select the **Mailbox** tab.
3. Use the search or filter options, find and select the user you need, and click the **Recover Mailbox Items** icon above the list to open the **New Recovery** form.

**Tip:** You can also use Global Search to locate, filter, and select the Mailbox you need. Click the Global Search box at the top or type slash (/) anywhere to start your search.

4. On the **New Recovery** page, select **Notes** from the **Item Type** drop-down.
5. Use the '\*' wildcard character or enter the text to search for notes with a matching subject of the note in the **Search** bar. Select the note(s) to recover from the search results.

**Or**

Click **Advanced Search** and search the note based on these filters and click **Apply**:

Filters	Description
<b>Subject</b>	The subject of the note.
<b>Creation Date</b>	Using the calendar, select a specific date range to search the notes based on the creation date.
<b>Modification Date</b>	Using the calendar, select a specific date range to search the notes based on the modification date.

To use a different **Recovery Point** for a Mailbox, click the **Edit** icon on the tile for that Mailbox. Find the recovery point you need and click **Select Recovery Point**.

6. Click **Next: Recover Options** to return to the form.
7. Under **Recover To**, select **Original Location** or **New Location**.

If you choose **New Location**, select a **Registered Source** and the **Target Mailbox**, and specify the **Folder** name to which you plan to recover.

**Note:** If a folder with the specified name does not exist, Cohesity creates the folder and recovers the note(s) to that folder.

Select **Export as PST** to export the backed up notes as a PST file, and provide a password for the exported PST file.



**Note:** Once the recovery task is completed, the exported PST file is valid for 72 hours. Ensure that you download the PST within 72 hours. For more information, see [Download Exported PST File](#).

This is an Early Access feature. Contact your Cohesity account team to enable the feature.

8. Select your **Recovery Options**:

- **Continue on Error.** Enable to recover even if errors occur when recovering the notes. For example, if one of the notes cannot be recovered, Cohesity will still attempt to recover the other selected note.
- **Task Name.** Change the default name of the recovery task.

9. Click **Start Recovery**.

### Recover Tasks

You can recover specific tasks from a protected Microsoft 365 user Mailbox. However, if you plan to recover the complete set of tasks in the user Mailbox, then [recover the mailbox folder](#) called **Tasks**.

To recover specific notes:

1. Go to **Sources** to set up your recovery task.
2. Click into the **Source** name and select the **Mailbox** tab.
3. Use the search or filter options, find and select the user you need, and click the **Recover Mailbox Items** icon above the list to open the **New Recovery** form.

**Tip:** You can also use Global Search to locate, filter, and select the Mailbox you need. Click the Global Search box at the top or type slash (/) anywhere to start your search.

4. On the **New Recovery** page, select **Tasks** from the **Item Type** drop-down.
5. Use the '\*' wildcard character or enter the text to search for notes with a matching subject of the task in the Search bar. Select the task(s) to recover from the search results.

**Or**

Click **Advanced Search** and search the tasks based on these filters and click **Apply**:

Filters	Description
<b>Subject</b>	The subject of the task.
<b>Creation Date</b>	Using the calendar, select a specific date range to search the tasks based on their creation date.
<b>Due Date</b>	Using the calendar, select a specific date range to search the tasks based on their due date.
<b>Status</b>	The status of the task.

To use a different **Recovery Point** for a Mailbox, click the **Edit** icon on the tile for that Mailbox. Find the recovery point you need and click **Select Recovery Point**.

- Click **Next: Recover Options** to return to the form.
- Under **Recover To**, select **Original Location** or **New Location**.

If you choose **New Location**, select a **Registered Source** and the **Target Mailbox**, and specify the **Folder** name to which you plan to recover.

**Note:** If a folder with the specified name does not exist, Cohesity creates the folder and recovers the task(s) to that folder.

Select **Export as PST** to export the backed up tasks as a PST file, and provide a password for the exported PST file.

**Note:** Once the recovery task is completed, the exported PST file is valid for 72 hours. Ensure that you download the PST within 72 hours. For more information, see [Download Exported PST File](#).

This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- Select your **Recovery Options**:
  - Continue on Error.** Enable to recover even if errors occur when recovering the tasks. For example, if one of the tasks cannot be recovered, Cohesity will still attempt to recover the other selected tasks.
  - Task Name.** Change the default name of the recovery task.
- Click **Start Recovery**.

### Download Exported PST File

After the recovery task is completed, within 72 hours you can download the exported PST file of the mailbox items that you choose to recover.

To download the PST file:

1. Navigate to **Activity**.
2. Locate and click on the recovery task from which you want to download the exported PST file.
3. Click **Download Files**.

The PST file is downloaded to your local system.

**Note:** The PST file is protected with a password; you must contact the admin user and obtain the password to open the downloaded PST file. This is an Early Access feature. Contact your Cohesity account team to enable the feature.

### Download Private Chats

To download the Private Chats of a user:

1. Navigate to **Sources**.
2. Click on the required source and click the **Mailbox** tab.
3. Select **Show All > Protected** and use the other filters, search box, and views at the top to narrow your search.
4. Click the **Actions** menu next to the object and click **Download Private Chats**.
5. In the **Download Private Chats** page, select the required snapshot, provide the task name, and click **Recover**.

**Note:** Attachments in the Private Chats will not be downloaded.

6. Click the **View Progress** button in the pop-up message or click the **Activity** menu.
7. Once the recovery is successful, click **Download**. The Private Chats will be downloaded.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

**Next >** Protect your Microsoft 365 [OneDrives](#), [SharePoint Online Sites](#), and [Teams](#) so you can recover them easily when you need to, as well!

## Mailbox Items Recovery Self-Service

Cohesity provides a self-service workflow to help the end users recover the Microsoft 365 Mailbox items by leveraging the Microsoft Entra ID (Azure Active Directory) login for user authentication.

Administrators can authorize the self-service workflow for users through the Security Groups.

**Note:** You can access the self-service portal through <https://helios.cohesity.com/#/self-service-portal/auth>.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

### Mailbox Items Recovery

To recover Microsoft 365 Mailbox items from the Cohesity Self-Service Portal:

1. In the Cohesity Data Cloud login page, log in through Microsoft using the **Cohesity Self-Service Portal** link.
2. Choose **Microsoft 365 Mailbox** to recover your Emails and folders, Calendars, Contacts, Tasks, and Notes.
3. In the **Recover** page, select the required **Item Type** in the drop-down. The options include:
  - Emails & Folders
  - Calendars
  - Contacts
  - Tasks
  - Notes
4. Use the '\*' wildcard character or enter the text to search for Mailbox items with a matching subject in the **Search** bar. Select the items to recover from the search results.

**Or**

Click **Advanced Search** and select the items to search based on the filters.

5. To use a different **Recovery Point** for a Mailbox item, click the **Edit** icon on the tile for that item. Find the recovery point you need and click **Select Recovery Point**.
6. Click **Recover**.
7. Under **Recover Type**, select the following:

- **Recover to Original Location** to recover all the items directly to your Mailbox.
- **Export as PST** to export all the items in the PST format. Provide a password for the exported PST file.

**Note:** You can download the PST file and use an agent to migrate the PST content.

Once the recovery task is completed, the exported PST file is valid for 72 hours. Ensure that you download the PST within 72 hours. For more information, see [Download Exported PST File](#).

8. Click **Finish**. You can view the recovery progress from the **Welcome** page under the **Recoveries** section or on the **Activity** page.
9. Click the action icon on the required task and click **Show Recovered Items** to view the name and size of the recovered items.

#### Download Exported PST File

After the recovery task is completed, within 72 hours you can download the exported PST file of the mailbox items that you choose to recover.

To download the PST file:

1. Navigate to **Activity**.
2. Locate and click on the recovery task from which you want to download the exported PST file.
3. Click **Download Files**. The PST file is downloaded to your local system.

**Note:** The PST file is protected with a password; you must contact the admin user and obtain the password to open the downloaded PST file.

## OneDrive for Business

OneDrive for Business is a SaaS application that is bundled in your Microsoft 365 subscription service. It is an intelligent files app for Microsoft 365 connecting you to all your files so you can share and work together from anywhere while protecting your work. It enables you to easily store, access, and discover your individual and shared work files in Microsoft 365. Using the policy-based data protection solution from DataProtect as a Service for Government (FedRAMP), you can protect OneDrive for Business data on Microsoft 365.

## Considerations

Review and understand the following considerations before you protect your Microsoft 365 OneDrive data:

- From the recovery workflow, you cannot download an empty folder.
- Backup and restore of OneNote files in OneDrive are not supported.
- Restoring shared permissions for files in the Preservation Hold Library (PHL) drive is not supported.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- PHL data can only be recovered using full OneDrive recovery. Granular level recovery is not supported for the PHL data.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- Data from PHL is not searchable.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- OneDrive protection is supported only for users present on Azure AD or Hybrid setup with users present on Azure AD and not for users on the on-premises Active Directory.
- File/folder permissions with no role will not be recovered since Microsoft does not allow adding such permissions via Graph APIs. For example, no role will be assigned when a Restricted View permission is added to a user from Advanced Setting.
- [Microsoft 365 Backup Storage](#) service is supported for OneDrive.

**Note:** This is a Private Preview feature. Private Preview was termed as Early Access in the earlier releases. Contact your Cohesity account team to enable the feature.

- OneDrive does not support item permissions from applications and devices.

## Protect Microsoft 365 OneDrives

Once you have [registered your Microsoft 365 domain](#) as a source, you're ready to use DataProtect as a Service for Government (FedRAMP) to protect the user OneDrives in your

domain.

To protect your Microsoft 365 OneDrives:

1. In **DataProtect as a Service**, under **Sources**, find the Microsoft 365 source and click on it.
2. Click the **OneDrive** tab.
3. Select the individual OneDrives you wish to protect or:
  - Click **Users > Select All Child Objects** to protect all the OneDrives in this source.
  - Click **Users > Auto Protect This** to protect all the OneDrives *plus any future additional OneDrives* on that source.
  - Click the **Security Groups** icon and select the security group to protect the OneDrives of the users in the security group. For more information, see [Security Groups](#).

Security groups based user import also supports nested security groups.

For example, if a security group (AA) includes members (X and Y) and security groups (BB and CC), the import process includes the members (X and Y) and the members of security groups (BB and CC).

Cohesity supports only users and not devices in Security Groups.

This is an Early Access feature. Contact your Cohesity account team to enable the feature.

4. Click the **Protect** icon above the list.
5. Choose a policy to specify backup frequency and retention. If you don't have a policy, you can easily [create one](#).
6. Under **Settings**, edit the **Start Time** if necessary.
7. Under **Additional Settings**, you can enable **Indexing** and other [additional settings](#).

**Note:** Indexing is enabled by default.

8. Click **Protect**.

**Note:** The backups start immediately after you protect the objects, regardless of the time you set for the protection run.

**Next >** When the first protection run completes, you will be ready to [recover your protected OneDrives](#) when and if you need to.

## Additional Settings

Advance Settings	Description
<b>Start Time</b>	Available only if the selected policy is set to <b>Backup Daily</b> . Indicates what time the protection run should start. Enter the <b>Start Time</b> and select <b>AM</b> or <b>PM</b> . The default time zone is the browser's time zone. You can change the time zone of the protection run by selecting a different time zone here.
<b>SLA</b>	The service-level agreement (SLA) defines how long the administrator expects a protection run to take. Enter: <ul style="list-style-type: none"> <li>• <b>Full</b>. The number of minutes you expect a full protection run, which captures all the blocks in an object, to take.</li> <li>• <b>Incremental</b>. The number of minutes you expect an incremental protection run, which captures only the changed blocks in an object, to take.</li> </ul>
<b>Cancel Runs at Quiet Time Start</b>	<i>(Available only if the selected policy has at least one <b>Quiet Time</b>)</i> When enabled, all the protection runs that are currently executing will cancel when the Quiet Time period starts. By default, this setting is disabled, meaning that after a protection run starts, it continues to execute even when a Quiet Time period starts. However, new protection runs will not start during a Quiet Time.
<b>Indexing</b>	By default, indexing is enabled.  <div style="border-left: 2px solid #0070C0; padding-left: 10px; background-color: #F0F0F0;"> <p><b>Note:</b> Indexing is mandatory to search for files or folders in a OneDrive.</p> </div>
<b>Exclusions</b>	Click <b>Add</b> to add custom folders that you want to exclude from the backup.

## Manage Existing Protection

Edit protection settings, change the policy, and start, stop, & pause protection.


Once you have [applied protection](#) to the objects in your sources, DataProtect as a Service for Government (FedRAMP) makes it easy to make changes to that protection quickly. You can:

- Edit additional settings like **End Date**, **Exclusions**, **Alerts**, and more.
- Apply a different policy.
- Start an on-demand protection run, pause and resume it, or even remove protection.

### Edit Protection Settings

To edit protection settings:



1. In **DataProtect as a Service**, navigate to **Sources**.
2. Click into the **Source** name.
3. Select **Show All > Protected** and use the other filters, search box, and views at the top to narrow your search.
4. Click the **Actions** menu (  ) next to the object and select **Edit Protection** to open the protection settings for that object.

**Apply a New Protection Policy**

To change the **Policy**, click the drop-down and select a different policy. To help you choose, each policy in the list shows the **Backup** frequency and the **Retain** period for each backup. If you don't have a policy that meets your needs, scroll to the bottom of the list and click **Create Policy** to create your own policy.

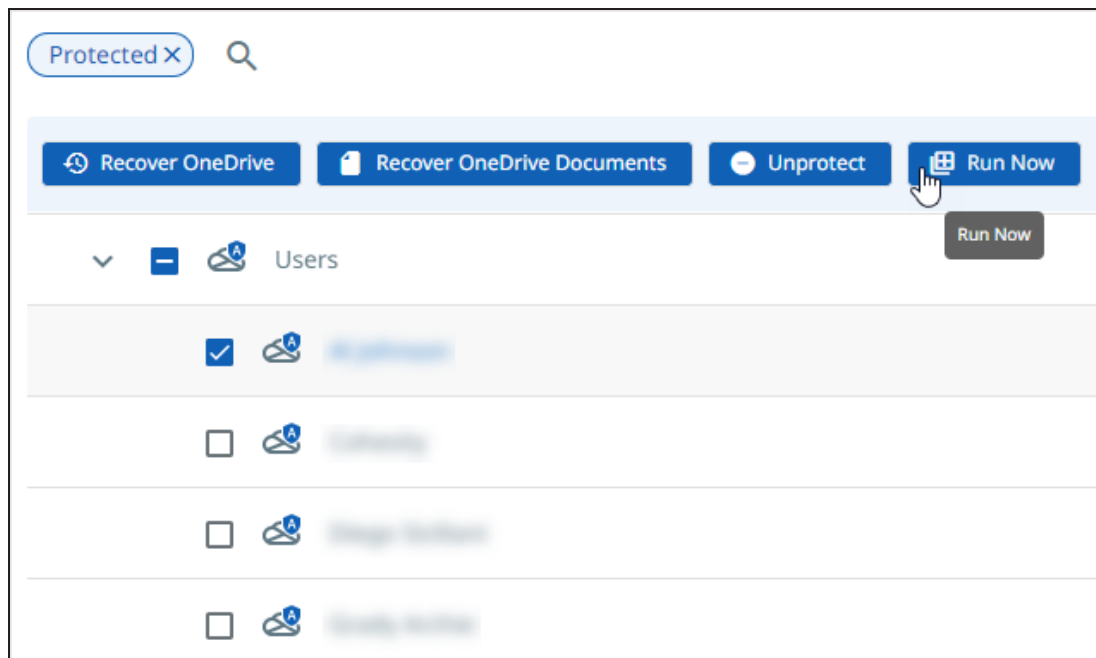
**Edit Additional Protection Settings**

In **DataProtect as a Service**, under **Settings**, you can change the protection **Start Time** (and select the **Time Zone**).

Click the drop-down next to **Additional Settings** to change more options. See [Additional Protection Settings](#) for details.

**Start, Stop, or Remove Protection**

When you select protected objects in one of your sources, DataProtect as a Service for Government (FedRAMP) presents buttons for the actions that are possible for those objects.



With the protected objects selected, you can click:

- **Recover OneDrive** to recover the OneDrive.
- **Recover OneDrive Documents** to recover the OneDrive documents.
- **Run Now** to start an on-demand protection run immediately.
- **Unprotect** to remove protection from the object.

**Tip:** If a protected object is deleted from the source, you can search the object using Global Search and unprotect it.

Additional Settings

Advance Settings	Description
<b>Start Time</b>	Available only if the selected policy is set to <b>Backup Daily</b> . Indicates what time the protection run should start. Enter the <b>Start Time</b> and select <b>AM</b> or <b>PM</b> . The default time zone is the browser's time zone. You can change the time zone of the protection run by selecting a different time zone here.
<b>SLA</b>	The service-level agreement (SLA) defines how long the administrator expects a protection run to take. Enter: <ul style="list-style-type: none"> <li>• <b>Full</b>. The number of minutes you expect a full protection run, which captures all the blocks in an object, to take.</li> <li>• <b>Incremental</b>. The number of minutes you expect an incremental protection run, which captures only the changed blocks in an object, to take.</li> </ul>
<b>Cancel Runs at Quiet Time Start</b>	<i>(Available only if the selected policy has at least one Quiet Time)</i> When enabled, all the protection runs that are currently executing will cancel when the Quiet Time period starts. By default, this setting is disabled, meaning that after a protection run starts, it continues to execute even when a Quiet Time period starts. However, new protection runs will not start during a Quiet Time.
<b>Indexing</b>	By default, indexing is enabled.  <div style="background-color: #f0f0f0; padding: 5px; border-left: 2px solid #0070c0;"> <p><b>Note:</b> Indexing is mandatory to search for files or folders in a OneDrive.</p> </div>
<b>Exclusions</b>	Click <b>Add</b> to add custom folders that you want to exclude from the backup.

## Recover OneDrives

After you protect your users' Microsoft 365 OneDrives, you can recover them — as whole OneDrives or just specific contents in a user's Microsoft 365 OneDrive — from DataProtect as a Service for Government (FedRAMP), to the same location, alternate location, or across Microsoft 365 domains.

**Note:** You can recover a OneDrive to a target OneDrive as long as the Microsoft 365 domain for the target OneDrive is registered within the same cloud region as the Microsoft 365 domain of the OneDrive being recovered. the same cloud region.

You can recover:

- User OneDrives
- User OneDrive Contents

### Recover User OneDrives

To recover protected Microsoft 365 user OneDrives:

1. In **DataProtect as a Service**, go to **Sources** to set up your recovery task.
2. Click into the **Source** name and select the **OneDrive** tab.
3. Above the tree, select **Protection Status > Protected**.
4. Use the search and filter options to find and select the OneDrive you need, click the **Actions (:)** menu on that row, and select **Recover OneDrive** to open the **New Recovery** form with the **Latest** snapshot (protection run).
5. In the **New Recovery** form, if you need to add more OneDrives and/or recover from an earlier backup, click the **Edit** icon in the top right of the form.
  - To add OneDrives, enter a **Search** term on the left, locate the other OneDrives, and select them.
  - To use a different **Recovery Point** for a OneDrive, click the **Edit** icon on the tile for that OneDrive. Find the recovery point you need and click **Select Recovery Point**.

Click **Next: Recover Options** to return to the form.

6. Under **Recover To**, select **Original Location** or **New Location**.  
If you choose **New Location**, select a **Registered Source** and the **Target OneDrive**.
7. Select your **Recovery Options**:

- **Continue on Error.** Enable to recover even if errors occur when recovering OneDrives. For example, if one of the OneDrives cannot be recovered, Cohesity will still attempt to recover the other selected OneDrives.
- **Include Preservation Hold Library.** Enable to recover the Preservation Hold Library that is part of the Cohesity snapshot. Recovering the Preservation Hold Library data may increase the recovery time substantially as it can include a large amount of data. The recovery will fail if the Target Location does not have sufficient space.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- **Task Name.** Change the default name of the recovery task.

8. Click **Start Recovery**.

**Next** > Protect your Microsoft 365 [Mailboxes](#), [SharePoint Online Sites](#), and [Teams](#) so you can recover them easily when you need to, as well!

### Recover OneDrive Contents

**Important:** Before you can recover a user's OneDrive contents, you need to set up [Microsoft 365 OneDrive protection](#) with **Indexing** enabled.

To recover specific OneDrive contents from a protected Microsoft 365 OneDrive:

1. In **DataProtect as a Service**, go to **Sources** to set up your recovery task.
2. Click into the **Source** name and select the **OneDrive** tab.
3. Above the tree, select **Protection Status** > **Protected**.
4. Use the search and filter options to find and select the OneDrive you need, click the **Actions** (: ) menu on that row, and select **Recover OneDrive Documents** to open the **New Recovery** form.
5. On the **New Recovery Microsoft 365 - OneDrive** page, in the **Recovery Type**, select any one of the following tabs to search for the file or folder:
  - **Browse OneDrive and Recover.** You can browse the individual user OneDrive to navigate and select the files or folders to be restored.
  - **Search Files and Recover.** You can use the global search to find the files and folders that need to be restored.
6. To *browse* and recover:

1. In the **Recovery Type** section, select **Browse OneDrive and Recover**.
  2. Select the file or folder you plan to restore. Do any one of the following based on your requirements:
    - To recover the file(s) or folder(s), click **Next**.
    - To download the file(s) or folder(s), click **Download Files**.

A new recovery task is created to download the file(s) or folder(s). When the task completes, from the **Activity** page, click the task name and then click **Download Files** to download the generated zip file.
  3. Click **Next: Recover Options** to return to the form and skip to **step 8**.
7. To *search* and recover:
- a. In the **Recovery Type** section, select **Search Files and Recover**.
  - b. Use the '\*' wildcard character and/or enter text to search for the folders or files with a matching folder name or file name in the **Search** bar. Select the folders or files to recover from the search results.

**Or**

Click **Advanced Search** and select **Both**, **Files**, or **Folder** and search based on the available filters and click **Apply**.
  - c. To use a different **Recovery Point** for a folder or file, click the **Edit** icon on the tile for that folder or file. Find the recovery point you need and click **Select Recovery Point**.
  - d. Click **Next: Recover Options** to return to the form.
8. Under **Recover To**, select **Original Location** or **New Location**.
- If you choose **Original Location**, the existing document library is overwritten.
  - If you choose **New Location**, select a **Registered Source** and the **Target Site**, and specify the **Document Library** name to which you plan to recover the document library items. Optionally, you can also enter a **new prefix for the Document Library**.

**Note:** If a folder with the specified name does not exist in the OneDrive, Cohesity creates the folder and recovers the OneDrive contents to that folder.

9. Select your **Recovery Options**:
- **Continue on Error**. Enable to recover even if errors occur when recovering the document library items. For example, if a document cannot be recovered, will

still attempt to recover the other selected documents from that document library.

- **Task Name.** Change the default name of the recovery task.

10. Click **Start Recovery**.

**Next** > Protect your Microsoft 365 [Mailboxes](#), [SharePoint Online Sites](#), and [Teams](#) so you can recover them easily when you need to, as well!

### OneDrive Content Recovery Self-Service

Cohesity provides a self-service workflow to help the end users recover the Microsoft 365 OneDrive content by leveraging the Microsoft Entra ID (Azure Active Directory) login for user authentication.

Administrators can authorize the self-service workflow for users through the Security Groups.

**Note:** You can access the self-service portal through <https://helios.gov-cohesity.com/#/self-service-portal/auth>.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

#### OneDrive Content Recovery

To recover OneDrive content from the Cohesity Self-Service Portal:

1. In the Cohesity Data Cloud login page, log in through Microsoft using the **Cohesity Self-Service Portal** link.
2. Choose **Microsoft 365 OneDrive** to recover your OneDrive Files and Folders.
3. In the **Recover** page, browse the OneDrive or search for the OneDrive content.
4. Use the '\*' wildcard character or enter the text to search for the folders or files with a matching subject in the **Search** bar. Select the folders or files to recover from the search results.

#### **Or**

Click **Advanced Search**, select **Both**, **Files**, or **Folder**, search based on the available filters, and click **Apply**.

5. To use a different **Recovery Point** for a folder or file, click the **Edit** icon on the tile for that folder or file. Find the recovery point you need and click **Select Recovery Point**.
6. Under **Recover Type**, select **Recover to Original Location** to recover all the items directly to your Mailbox.

7. Click **Finish**. You can view the recovery progress from the **Welcome** page under the **Recoveries** section or on the **Activity** page.
8. Click the action icon on the required task and click **Show Recovered Items** to view the name and size of the recovered items.

## SharePoint Online

SharePoint Online is a SaaS application bundled with the Microsoft 365 service. It provides an extensive range of collaborative and creative capabilities enabling organizations to share, manage, and access information from almost any device.

Using the policy-based data protection solution from DataProtect as a Service for Government (FedRAMP), you can backup and recover the SharePoint Online site templates. Thus enabling you to backup and recover the SharePoint Online sites or subsites and its contents such as document libraries and so on.

### Considerations

Review and understand the following considerations before you protect your Microsoft 365 SharePoint Online data:

- Document libraries enabled with the ForceCheckout option are not recovered.
- Recovery of sites with the out-of-the-box (OOTB) modern theme or composed look is not supported.
- Backup and recovery of the site or subsite URLs with non-ANSI characters are not supported.
- Recovery of a site collection is not supported if the site URL has changed after the backup.
- From the recovery workflow, you cannot download an empty folder.
- DataProtect as a Service for Government (FedRAMP) discovers and protects the SharePoint Online sites created in the central storage location of your Microsoft 365 tenant.
- SharePoint Online sites created in satellite storage locations of your Microsoft 365 tenant can be discovered and protected. You can recover to the same tenant and same location or an alternate tenant and default location. For more details, see [Multi-Geo Capabilities in SharePoint Online](#).

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- Cohesity currently does not support Geo-Stretched Microsoft 365 tenants.
- Recovering shared permissions for files in the PHL drive is not supported.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- Data from PHL is not searchable.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- Backup of checked-out files in SharePoint is not supported.
- Custom scripts setting is not supported in SharePoint.
- Granular recovery of Team and Group sites is not supported when Site Tagging is enabled.
- During SharePoint granular recovery, you cannot browse or download files from the document libraries that contain a slash (/) in its name. As a workaround, you can perform a full recovery.
- File/folder permissions with no role will not be recovered since Microsoft does not allow adding such permissions via Graph APIs. For example, no role will be assigned when a Restricted View permission is added to a user from Advanced Setting.
- [Microsoft 365 Backup Storage](#) service is supported for SharePoint Online.

**Note:** This is a Private Preview feature. Private Preview was termed as Early Access in the earlier releases. Contact your Cohesity account team to enable the feature.

- SharePoint sites that are archived or locked will not be backed up and the source discovery may complete early due to these locked sites. Contact your Cohesity account team to configure the cluster to ignore the locked sites during discovery.

#### SharePoint Lists

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- Recovery of comments does not include the commenter name and the actual time the comment was added.
- Item-level granular recovery is not supported.
- [External lists](#) are not supported.



- Hidden lists backup is supported, while system hidden lists (catalogs) recovery is not supported.
- Hidden lists (apart from catalogs) are recovered as not hidden.
- Recovery of sites (to the original or alternate location) creates new lists with the current DateTime suffix.
- Attachments with more than 4 MB size are not backed up.
- Columns of the type *User* in the recovered lists may display incorrect user for alternate restore.
- Recovered lists for the template type *Playlist* do not display the embedded video.
- For the comments that include mentions, if any of the mentioned users are deleted, the names of the users are displayed instead of the mentions.
- For embedded images, the linkage and thumbnail may be broken in the restored list.
- Lists items backup is not supported for Team Sites under Teams and Group sites under Groups.
- List views are not supported.
- Recovery of lists fails for the following:
  - if the list includes a lookup column.
  - if the list includes a managed metadata column.

## Protect Microsoft 365 SharePoint Online Sites

Once you have [registered your Microsoft 365 domain](#) as a source, you're ready to protect the SharePoint Online sites in your domain.

To protect your Microsoft 365 SharePoint Online sites:

1. In **DataProtect as a Service**, under **Sources**, find the Microsoft 365 source and click into it.
2. Click the **Site** tab.
3. Select the individual SharePoint Online site you wish to protect or:
  - Click **Users > Select All Child Objects** to protect all the SharePoint Online sites in this source.
  - Click **Users > Auto Protect This** to protect all the SharePoint Online sites in this source.
4. Click the **Protect** icon above the list.
5. Choose a policy to specify backup frequency and retention. If you don't have a policy, you can easily [create one](#).
6. Under **Settings**, edit the **Start Time** if necessary.

- Under **Additional Settings**, you can enable **Indexing**, configure a specific **End Date, Alerts**, and other [additional settings](#).

**Note:** If you plan to recover individual [document library items](#), in addition to [whole sites](#), you need to enable **Indexing** in this step. When you do, you can include or exclude specific sites from indexing.

- Click **Protect**.

**Note:** The backups start immediately after you protect the objects, regardless of the time you set for the protection run.

**Next >** When the first protection run completes, you will be ready to [recover your protected SharePoint Online sites](#) when and if you need to.

### Additional Settings

Advance Settings	Description
<b>Start Time</b>	Available only if the selected policy is set to <b>Backup Daily</b> . Indicates what time the protection run should start. Enter the <b>Start Time</b> and select <b>AM</b> or <b>PM</b> . The default time zone is the browser's time zone. You can change the time zone of the protection run by selecting a different time zone <a href="#">here</a> .
<b>SLA</b>	The service-level agreement (SLA) defines how long the administrator expects a protection run to take. Enter: <ul style="list-style-type: none"> <li>• <b>Full</b>. The number of minutes you expect a full protection run, which captures all the blocks in an object, to take.</li> <li>• <b>Incremental</b>. The number of minutes you expect an incremental protection run, which captures only the changed blocks in an object, to take.</li> </ul>
<b>Cancel Runs at Quiet Time Start</b>	<i>(Available only if the selected policy has at least one <a href="#">Quiet Time</a>)</i> When enabled, all the protection runs that are currently executing will cancel when the Quiet Time period starts. By default, this setting is disabled, meaning that after a protection run starts, it continues to execute even when a Quiet Time period starts. However, new protection runs will not start during a Quiet Time.
<b>Indexing</b>	By default, indexing is enabled.  <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> Indexing is mandatory for granular restore of SharePoint sites.</p> </div>

## Manage Existing Protection


Edit protection settings, change the policy, and start, stop, & pause protection.

Once you have [applied protection](#) to the objects in your sources, DataProtect as a Service for Government (FedRAMP) makes it easy to make changes to that protection quickly. You can:

- Edit additional settings like **End Date**, **Exclusions**, **Alerts**, and more.
- Apply a different policy.
- Start an on-demand protection run, pause and resume it, or even remove protection.

### Edit Protection Settings

To edit protection settings:

1. In **DataProtect as a Service**, navigate to **Sources**.
2. Click into the **Source** name.
3. Select **Show All > Protected** and use the other filters, search box, and views at the top to narrow your search.
4. Click the **Actions** menu (  ) next to the object and select **Edit Protection** to open the protection settings for that object.

### Apply a New Protection Policy

To change the **Policy**, click the drop-down and select a different policy. To help you choose, each policy in the list shows the **Backup** frequency and the **Retain** period for each backup.

If you don't have a policy that meets your needs, scroll to the bottom of the list and click **Create Policy** to [create your own policy](#).

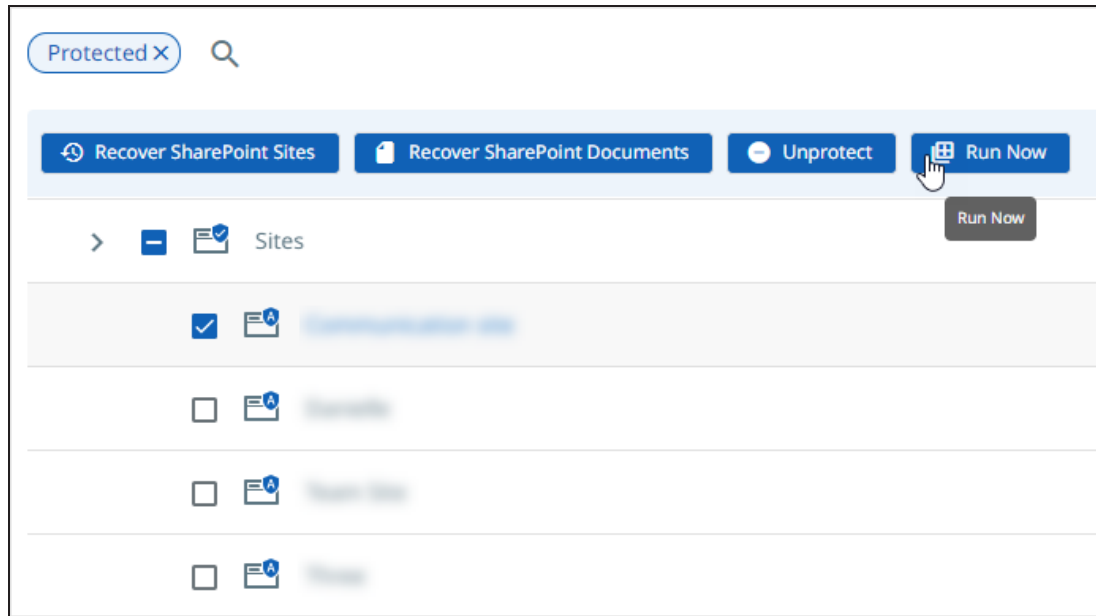
### Edit Additional Protection Settings

Under **Settings**, you can change the protection **Start Time** (and select the **Time Zone**).

Click the drop-down next to **Additional Settings** to change more options. See [Additional Protection Settings](#) for details.

### Start, Stop, or Remove Protection

When you select protected objects in one of your sources, DataProtect as a Service for Government (FedRAMP) presents buttons for the actions that are possible for those objects.



With the protected objects selected, you can click:

- **Recover SharePoint Sites** to recover the SharePoint sites.
- **Recover SharePoint Documents** to recover the SharePoint documents.
- **Run Now** to start an on-demand protection run immediately.
- **Unprotect** to remove protection from the object.

**Tip:** If a protected object is deleted from the source, you can search the object using Global Search and unprotect it.

### Additional Settings

Advance Settings	Description
<b>Start Time</b>	Available only if the selected policy is set to <b>Backup Daily</b> . Indicates what time the protection run should start. Enter the <b>Start Time</b> and select <b>AM</b> or <b>PM</b> . The default time zone is the browser's time zone. You can change the time zone of the protection run by selecting a different time zone here.

Advance Settings	Description
<p><b>SLA</b></p>	<p>The service-level agreement (SLA) defines how long the administrator expects a protection run to take. Enter:</p> <ul style="list-style-type: none"> <li>• <b>Full.</b> The number of minutes you expect a full protection run, which captures all the blocks in an object, to take.</li> <li>• <b>Incremental.</b> The number of minutes you expect an incremental protection run, which captures only the changed blocks in an object, to take.</li> </ul>
<p><b>Cancel Runs at Quiet Time Start</b></p>	<p><i>(Available only if the selected policy has at least one Quiet Time)</i></p> <p>When enabled, all the protection runs that are currently executing will cancel when the Quiet Time period starts. By default, this setting is disabled, meaning that after a protection run starts, it continues to execute even when a Quiet Time period starts. However, new protection runs will not start during a Quiet Time.</p>
<p><b>Indexing</b></p>	<p>By default, indexing is enabled.</p> <div style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p><b>Note:</b> Indexing is mandatory for granular restore of SharePoint sites.</p> </div>

## Recover Microsoft 365 SharePoint Online Sites & Items

After you [protect your users' Microsoft 365 SharePoint Online sites](#), you can recover them — as [whole sites](#) or just [specific document library items](#) — from DataProtect as a Service for Government (FedRAMP), to the same location, alternate location, or across Microsoft 365 domains.

**Note:** To recover site system files such as HTML, Javascript, and so on, ensure that you enable Custom Scripts permissions on the tenant. For more information, see [Tenant Permissions](#) in Microsoft 365 Requirements.

You can recover:

- [SharePoint Sites](#)
- [SharePoint Document Library Items](#)

### Recover SharePoint Sites

To recover protected Microsoft 365 SharePoint Online sites:

1. In **DataProtect as a Service**, go to **Sources** to set up your recovery task.
2. Click on the **Source** name.

3. Above the tree, select **Show All > Protected**.
4. Find the sites you need and click the **Recover** button on that row to open the **New Recovery** form with the **Latest** snapshot (protection run).
5. In the **New Recovery** form, if you need to add more SharePoint Online sites and/or recover from an earlier backup, click the **Edit** icon in the top right of the form.
  - To add SharePoint Online sites, enter a **Search** term on the left, locate the other SharePoint Online sites, and select them.
  - To use a different Recovery Point for a site, click the **Edit** icon on the tile for that site. Find the recovery point you need and click **Select Recovery Point**.

**Note:** To recover a site collection and its sub-sites, search using the site collection relative URL such as `"/sites/myrootsite"` and add them to the recovery task.

Click **Next: Recover Options** to return to the form.

6. Under **Recover To**, select **Original Location** or **New Location**.

If you choose **New Location**, select a **Registered Source** and the **Target**.

**Note:** Sites created in satellite storage locations are recovered to the same location in the target tenant as the source tenant. If the same location is not available, the sites are recovered to the central location.

This is an Early Access feature. Contact your Cohesity account team to enable the feature.

7. Select your **Recovery Options**:
  - **Continue on Error.** Enable to recover even if errors occur when recovering SharePoint Online sites. For example, if one of the sites cannot be recovered, Cohesity will still attempt to recover the other selected sites.
  - **Include Preservation Hold Library.** Enable to recover the Preservation Hold Library that is part of the Cohesity snapshot. Recovering the Preservation Hold Library data may increase the recovery time substantially as it can include a large amount of data. The recovery will fail if the Target Location does not have sufficient space.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

- **Task Name.** Change the default name of the recovery task.
8. Click **Start Recovery**.

**Next** > Protect your Microsoft 365 [Mailboxes](#), [OneDrives](#), and [Teams](#) so you can recover them easily when you need to, as well!

### Recover SharePoint Document Library Items

**Important:** Before you can recover SharePoint document library items, you need to set up [SharePoint protection](#) with **Indexing** enabled.

To recover specific document library items from a protected Microsoft 365 SharePoint Online Site:

1. In **DataProtect as a Service**, go to **Sources** to set up your recovery task.
2. Click on the **Source** name and select the **Site** tab.
3. Use the search or filter options, find and select the site you need, click the **Actions** menu (:) on that row, and select **Recover SharePoint Documents** to open the **New Recovery** form.
4. In the **New Recovery Microsoft 365 - SharePoint Online** page, under the **Recovery Type** section, select any one of the following to search for the file or folder:
  - **Browse Site and Recover.** You can browse the individual site to navigate and select the files/document library to be restored.
  - **Search Files and Recover.** You can use the global search to find the files and document libraries that need to be restored.
5. To *browse* and recover:
  - a. In the **Recovery Type** section, select **Browse Site and Recover**.
  - b. Search for the site name and click the site name to browse the site.
  - c. Select the file or document library you plan to restore. Do any one of the following based on your requirements:
    - i. To recover the file(s) or document library(s), click **Next**.
    - ii. To download the file(s) or document library(s), click **Download Files**.

A new recovery task is created to download the file(s) or document library (s). When the task completes, from the **Activity** page, click the task name and then click **Download Files** to download the generated zip file.
  - d. Click **Next: Recover Options** to return to the form and skip to **step 8**.
6. To *search* and recover:

1. In the **Recovery Type** section, select **Search Files and Recover**.
2. Use the '\*' wildcard character and/or enter text (such as '\*.xlsx' or '\*.pdf') to search for the folders or files with a matching folder name or file name in the **Search** bar. Select the folders or files to recover from the search results.  
**Or**  
Click **Advanced Search** and select **Both**, **Files**, or **Folder** and search based on the available filters and click **Apply**.
3. To use a different **Recovery Point** for a folder or file, click the **Edit** icon on the tile for that folder or file. Find the recovery point you need and click **Select Recovery Point**.
4. Click **Next: Recover Options** to return to the form.
7. Under **Recover To**, select **Original Location** or **New Location**.
  - If you choose **Original Location**, the existing document library is overwritten.
  - If you choose **New Location**, select a **Registered Source** and the **Target Site**, and specify the **Document Library** name to which you plan to recover the document library items. Optionally, you can also enter a new **prefix for the Document Library**.

**Note:** If a document library with the specified name does not exist on the site, Cohesity creates the document library and recovers the folders or files to that document library.

8. Select your **Recovery Options**:
  - **Continue on Error**. Enable to recover even if errors occur when recovering the document library items. For example, if a document cannot be recovered, Cohesity will still attempt to recover the other selected documents from that document library.
  - **Task Name**. Change the default name of the recovery task.
9. Click **Start Recovery**.

#### Recover SharePoint Lists

Cohesity now supports the recovery of the Lists in Microsoft 365 SharePoint Online. Lists are a collection of data like links, announcements, contacts, issue trackers, surveys, and so on.

For more details, see [SharePoint Online](#).

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.



**Next** > Protect your Microsoft 365 [Mailboxes](#), [OneDrives](#), and [Teams](#) so you can recover them easily when you need to, as well!

## Microsoft Teams

Microsoft Teams is a collaboration solution provided by Microsoft that is bundled with the Microsoft 365 service. For more information, see [Microsoft documentation](#). Using the policy-based data protection solution from DataProtect as a Service for Government (FedRAMP), you can backup and recover Teams data in Microsoft 365.

## Considerations

Review and understand the following considerations before you protect your Microsoft 365 Teams data:

- Granular recovery of files and folders is supported.
- Backup and recovery of channel tabs are not supported.
- Backup and recovery of subsites of Teams site is not supported.
- If folders such as Feeds, Sync Issues, Legacy Archive Journals, Outbound, Managed Folders, Files, Yammer Root, Clutter, MeContact, and Archive, are not already present, the folders are skipped during recovery.
- Recovering the following Teams data from the Teams backup is not supported:
  - Channel names and descriptions
  - System Document Libraries
- Backup and download of the following is not supported:
  - Self-message (messages sent to self)
  - Saved or pinned Posts property in the conversation
  - Meeting recordings metadata
  - Shared Channels
- Granular recovery of Team sites is not supported when Site Tagging is enabled.
- Backup of Teams with no owners is supported when at least one Exchange Online licensed member is available in the Teams.

If no owners/members are available in the Teams, you can contact your Cohesity account team to configure a service account (with an Exchange Online license). This service account will be added as a member of the Teams before backup/recovery and removed after the backup/recovery is completed.

**Note:** This is a Private Preview feature. Private Preview was termed as Early Access in the earlier releases. Contact your Cohesity account team to enable the feature.

- File/folder permissions with no role will not be recovered since Microsoft does not allow adding such permissions via Graph APIs. For example, no role will be assigned when a Restricted View permission is added to a user from Advanced Setting.

## Protect Microsoft 365 Teams

Once you have [registered your Microsoft 365 domain](#) as a source, you're ready to use DataProtect as a Service for Government (FedRAMP) to protect the Teams data in your domain.

To protect your Microsoft 365 Teams:

**Note:** If the Teams Posts option is enabled under the Teams during app registration, the Teams Posts will be backed up along with the corresponding Teams.

Teams backup may fail if the Azure subscription configuration is not set appropriately.

This is an Early Access feature. Contact your Cohesity account team to enable the feature.

1. In **DataProtect as a Service**, under **Sources**, find the Microsoft 365 source and click into it.
2. Click the **Teams** tab.
3. Select the individual Team you wish to protect or:
  - Click **Users > Select All Child Objects** to protect all the Teams in this source.
  - Click **Users > Auto Protect This** to protect all the Teams in this source.
4. Click the **Protect** icon above the list.
5. Choose a policy to specify backup frequency and retention. If you don't have a policy, you can easily [create one](#).
6. Under **Settings**, edit the **Start Time** if necessary.
7. Under **Additional Settings**, you can enable **Indexing**, configure a specific **End Date, Alerts**, and other [additional settings](#).

**Note:** If you plan to recover individual document library items (coming soon!), in addition to whole sites, you need to enable **Indexing** in this step. When you do, you can include or exclude specific sites from indexing.

8. Click **Protect**.

**Note:** The backups start immediately after you protect the objects, regardless of the time you set for the protection run.

**Next >** When the first protection run completes, you will be ready to [recover your protected Teams](#) when and if you need to.

### Additional Settings

Advance Settings	Description
Start Time	Available only if the selected policy is set to <b>Backup Daily</b> . Indicates what time the protection run should start. Enter the <b>Start Time</b> and select <b>AM</b> or <b>PM</b> . The default time zone is the browser's time zone. You can change the time zone of the protection run by selecting a different time zone here.
SLA	The service-level agreement (SLA) defines how long the administrator expects a protection run to take. Enter: <ul style="list-style-type: none"> <li>• <b>Full</b>. The number of minutes you expect a full protection run, which captures all the blocks in an object, to take.</li> <li>• <b>Incremental</b>. The number of minutes you expect an incremental protection run, which captures only the changed blocks in an object, to take.</li> </ul>
Cancel Runs at Quiet Time Start	<i>(Available only if the selected policy has at least one Quiet Time)</i> When enabled, all the protection runs that are currently executing will cancel when the Quiet Time period starts. By default, this setting is disabled, meaning that after a protection run starts, it continues to execute even when a Quiet Time period starts. However, new protection runs will not start during a Quiet Time.
Indexing	By default, indexing is enabled.  <b>Note:</b> Indexing is mandatory for granular restore of Teams contents.

### Manage Existing Protection


Edit protection settings, change the policy, and start, stop, & pause protection.

Once you have [applied protection](#) to the objects in your sources, DataProtect as a Service for Government (FedRAMP) makes it easy to make changes to that protection quickly. You can:

- Edit additional settings like **End Date**, **Exc2lusions**, **Alerts**, and more.
- Apply a different policy.
- Start an on-demand protection run, pause and resume it, or even remove protection.

#### Edit Protection Settings

To edit protection settings:

1. In **DataProtect as a Service**, navigate to **Sources**.
2. Click into the **Source** name.
3. Select **Show All > Protected** and use the other filters, search box, and views at the top to narrow your search.
4. Click the **Actions** menu (  ) next to the object and select **Edit Protection** to open the protection settings for that object.

#### Apply a New Protection Policy

To change the **Policy**, click the drop-down and select a different policy. To help you choose, each policy in the list shows the **Backup** frequency and the **Retain** period for each backup.

If you don't have a policy that meets your needs, scroll to the bottom of the list and click **Create Policy** to [create your own policy](#).

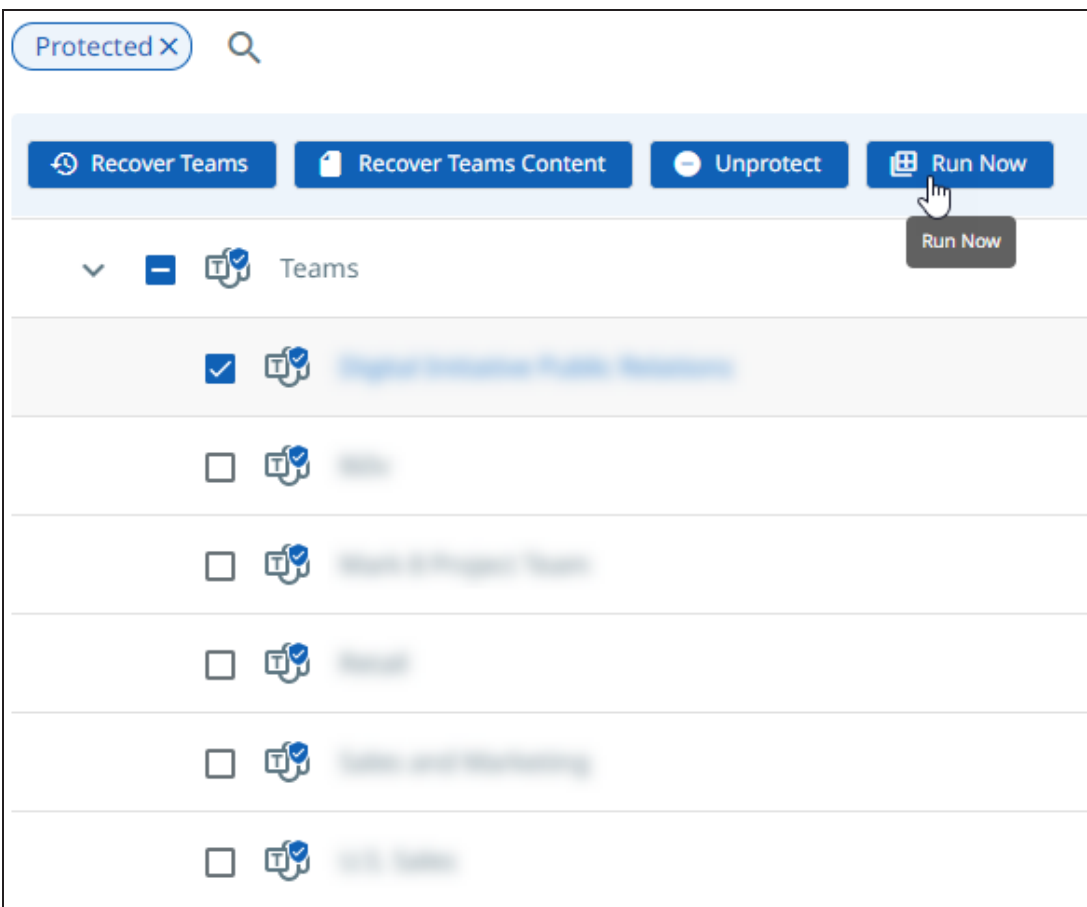
#### Edit Additional Protection Settings

Under **Settings**, you can change the protection **Start Time** (and select the **Time Zone**).

Click the drop-down next to **Additional Settings** to change more options. See [Additional Protection Settings](#) for details.

#### Start, Stop, or Remove Protection

When you select protected objects in one of your sources, DataProtect as a Service for Government (FedRAMP) presents buttons for the actions that are possible for those objects.



With the protected objects selected, you can click:

- **Recover Teams** to recover the Teams.
- **Recover Teams Content** to recover the Teams content.
- **Run Now** to start an on-demand protection run immediately.
- **Unprotect** to remove protection from the object.

**Tip:** If a protected object is deleted from the source, you can search the object using Global Search and unprotect it.

Additional Settings

Advance Settings	Description
<b>Start Time</b>	Available only if the selected policy is set to <b>Backup Daily</b> . Indicates what time the protection run should start. Enter the <b>Start Time</b> and select <b>AM</b> or <b>PM</b> . The default time zone is the browser's time zone. You can change the time zone of the protection run by selecting a different time zone here.
<b>SLA</b>	The service-level agreement (SLA) defines how long the administrator expects a protection run to take. Enter: <ul style="list-style-type: none"> <li>• <b>Full</b>. The number of minutes you expect a full protection run, which captures all the blocks in an object, to take.</li> <li>• <b>Incremental</b>. The number of minutes you expect an incremental protection run, which captures only the changed blocks in an object, to take.</li> </ul>
<b>Cancel Runs at Quiet Time Start</b>	<i>(Available only if the selected policy has at least one Quiet Time)</i> When enabled, all the protection runs that are currently executing will cancel when the Quiet Time period starts. By default, this setting is disabled, meaning that after a protection run starts, it continues to execute even when a Quiet Time period starts. However, new protection runs will not start during a Quiet Time.
<b>Indexing</b>	By default, indexing is enabled.  <div style="border-left: 2px solid #0070C0; padding-left: 10px; background-color: #F0F0F0;"> <p><b>Note:</b> Indexing is mandatory for granular restore of Teams contents.</p> </div>

## Recover Microsoft 365 Teams and Teams Content

After you protect your users' Teams, you can recover them — as [whole Teams](#) or just [specific Teams content](#) — from DataProtect as a Service for Government (FedRAMP) to the original Team in the same Microsoft 365 domain.

You can recover:

- [Microsoft 365 Teams](#)
- [Microsoft 365 Teams Content](#)

### Recover Microsoft 365 Teams

To recover protected Microsoft 365 Teams:

1. In **DataProtect as a Service**, go to **Sources** to set up your recovery task.
2. Click on the **Source** name and select the **Teams** tab.

3. Above the tree, select **Show All > Protected**.
4. Find the Team you need and click the **Recover** button on that row to open the **New Recovery** form with the **Latest** snapshot (protection run).
5. In the **New Recovery** form, if you need to add more Teams and/or recover from an earlier backup, click the **Edit** icon in the top right of the form.
  - To add Teams, enter a **Search** term on the left, locate the other Teams, and select them.
  - To use a different **Recovery Point** for a Team, click the **Edit** icon on the tile for that Team. Find the recovery point you need and click **Select Recovery Point**.

Click **Next: Recover Options** to return to the form.

6. Under **Recover To**, select **Original Location** or **New Location**.
  - If you choose **Original Location**, the existing Teams content is overwritten.
  - If you choose **New Location**, select a **Registered Source** and the **Target Team** or click **Create New Team** to **create a new Team**.

For sample recovery use cases, see [Sample Teams Recovery Use Cases](#).

7. Select your **Recovery Options**:
  - **Restore Original Owner Members**. Disable the option if you do not want to restore the original owners and channel members to the newly created Team.
  - **Team Owner**. Select the target team owner that needs to be added to the original team owners.
  - **Continue on Error**. Enable to recover even if errors occur when recovering Teams. For example, if one of the Teams cannot be recovered, Cohesity will still attempt to recover the other selected Teams.
  - **Task Name**. Change the default name of the recovery task.
8. Click **Start Recovery**.

[Sample Teams Recovery Use Cases](#)

Use Case	Instructions
Restore the Team’s data to the original Microsoft 365 domain.	Under <b>Recover To</b> , select <b>Original Location</b> .
Restore a Team’s data to the original Microsoft 365 domain and add a new owner.	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>Original Location</b>.</li> <li>2. In <b>Recovery Options</b>, disable <b>Restore Original Owner Members</b> and select an <b>Additional Team Owner</b> from the <b>Team Owner</b> drop-down list.</li> </ol>

Use Case	Instructions
<p>Restore the Team's data to a different Team that exists on the original Microsoft 365 domain.</p>	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the original Microsoft 365 domain as the <b>Registered Source</b> and select the <b>Target Team</b> to which you plan to restore the data.</li> </ol>
<p>Restore the Team's data to a different Team that exists on the original Microsoft 365 domain and add a new owner.</p>	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the original Microsoft 365 domain as the <b>Registered Source</b> and select the <b>Target Team</b> to which you plan to restore the data.</li> <li>3. Under <b>Recovery Options</b>, select an <b>Additional Team Owner</b> from the <b>Team Owner</b> drop-down list.</li> </ol>
<p>Restore the Team's data to a new Team on the original Microsoft 365 domain.</p>	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the original Microsoft 365 domain as the <b>Registered Source</b>, click <b>Create New Team</b> and specify the <b>Team Name</b>.</li> </ol>
<p>Restore the Team's data to a new Team on the original Microsoft 365 domain and add a new owner.</p>	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the original Microsoft 365 domain as the <b>Registered Source</b>, click <b>Create New Team</b> and specify the <b>Team Name</b>.</li> <li>3. Under <b>Recovery Options</b>, select an <b>Additional Team Owner</b> from the <b>Team Owner</b> drop-down list.</li> </ol>
<p>Restore the Team's data to a different Team that exists on a different Microsoft 365 domain.</p>	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the target Microsoft 365 domain from the <b>Registered Source</b> drop-down.</li> <li>3. Select the <b>Target Team</b> to which you plan to restore the data.</li> </ol>
<p>Restore the Team's data to a new Team on a different Microsoft 365 domain. Also, add a new owner.</p>	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the target Microsoft 365 domain from the <b>Registered Source</b> drop-down.</li> <li>3. Click <b>Create New Team</b> and specify the <b>Team Name</b>.</li> <li>4. Under <b>Recovery Options</b>, select an <b>Additional Team Owner</b> from the <b>Team Owner</b> drop-down list.</li> </ol>



**Next** > Protect your Microsoft 365 [Mailboxes](#), [OneDrives](#), and [SharePoint Online Sites](#) so you can recover them easily when you need to, as well!

### Recover Microsoft 365 Teams Content

To recover specific content from a protected Microsoft 365 Team:

1. In **DataProtect as a Service**, go to **Sources** to set up your recovery task.
2. Click into the **Source** name and select the **Teams** tab.
3. Use the search or filter options, find and select the Team you need, and click **Recover Teams Content** on that row to open the **New Recovery** form.
4. Use the '\*' wildcard character and/or enter the text (such as '\*.xlsx' or '\*.jpg') to search for the folders or files with a matching folder name or file name in the **Search** bar. Select the folders or files to recover from the search results.

#### Or

Click **Advanced Search** and select **Both**, **Files**, or **Folder** and search based on the available filters and click **Apply**.

5. To use a different **Recovery Point** for a folder or file, click the **Edit** icon on the tile for that folder or file. Find the recovery point you need and click **Select Recovery Point**.
6. Click **Next: Recover Options** to return to the form.
7. Under **Recover To**, select **Original Location** or **New Location**.
  - If you choose **Original Location**, the existing Teams content is overwritten.
  - If you choose **New Location**, select a **Registered Source** and the **Target Team** or click **Create New Team** to create a new Team. Then, select the **Target Channel** or click **Create New Channel** and select **Public** or **Private** to create a new channel in the selected Team. If you choose to create a **Private** channel then select the channel owner from the drop-down.
  - Choose **Download** to download the Teams content.  
A new recovery task is created to download the content. When the task is completed, from the **Activity** page, click the task name and then click **Download Files** to download the generated zip file.

**Note:** When you download multiple files from different snapshots, multiple recovery jobs are run and the files are downloaded separately.

For sample recovery use cases, see [Sample Teams Content Recovery Use Cases](#).

8. Select your **Recovery Options**:

- **Restore Original Owner Members.** Disable the option if you do not want to restore the original owners and channel members to the newly created Team.
- **Team Owner.** Select the target team owner that needs to be added to the original team owners.
- **Continue on Error.** Enable to recover even if errors occur when recovering Teams content. For example, if one of the Teams cannot be recovered, Cohesity will still attempt to recover the other selected Teams.
- **Task Name.** Change the default name of the recovery task.

9. Click **Start Recovery**.

Sample Teams Content Recovery Use Cases

Use Case	Instructions
Restore the Team’s data to the original Microsoft 365 domain.	Under <b>Recover To</b> , select <b>Original Location</b> .
Restore a Team’s data to the original Microsoft 365 domain and add a new owner.	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>Original Location</b>.</li> <li>2. In <b>Recovery Options</b>, disable <b>Restore Original Owner Members</b> and select an <b>Additional Team Owner</b> from the <b>Team Owner</b> drop-down list.</li> </ol>
Restore the Team’s data to a different Team that exists on the original Microsoft 365 domain.	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the original Microsoft 365 domain as the <b>Registered Source</b> and select the <b>Target Team</b> to which you plan to restore the data.</li> <li>3. Select the <b>Target Channel</b> or click <b>Create New Channel</b> to create a new target channel to which you plan to restore the channel data.</li> </ol>
Restore the Team’s data to a different Team that exists on the original Microsoft 365 domain. Also, restore the channel data to an existing channel.	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the original Microsoft 365 domain as the <b>Registered Source</b> and select the <b>Target Team</b> to which you plan to restore the data.</li> <li>3. Select the <b>Target Channel</b> to which you plan to restore the channel data.</li> </ol>

Use Case	Instructions
<p>Restore the Team's data to a different Team that exists on the original Microsoft 365 domain. Also, restore the channel data to a new channel.</p>	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the original Microsoft 365 domain as the <b>Registered Source</b> and select the <b>Target Team</b> to which you plan to restore the data.</li> <li>3. From the <b>Target Channel</b> drop-down, click <b>Create New Channel</b> to create a new channel in the selected Team.</li> </ol>
<p>Restore the Team's data to a different Team that exists on the original Microsoft 365 domain and add a new owner.</p>	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the original Microsoft 365 domain as the <b>Registered Source</b> and select the <b>Target Team</b> to which you plan to restore the data.</li> <li>3. Select the <b>Target Channel</b> or click <b>Create New Channel</b> to create a new target channel to which you plan to restore the channel data.</li> <li>4. Under <b>Recovery Options</b>, select an <b>Additional Team Owner</b> from the <b>Team Owner</b> drop-down list.</li> </ol>
<p>Restore the Team's data to a new Team on the original Microsoft 365 domain.</p>	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the original Microsoft 365 domain as the <b>Registered Source</b>, click <b>Create New Team</b> and specify the <b>Team Name</b>.</li> <li>3. Select the <b>Target Channel</b> or click <b>Create New Channel</b> to create a new target channel to which you plan to restore the channel data.</li> </ol>

Use Case	Instructions
<p>Restore the Team's data to a new Team on the original Microsoft 365 domain and add a new owner.</p>	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the original Microsoft 365 domain as the <b>Registered Source</b>, click <b>Create New Team</b> and specify the Team Name.</li> <li>3. Select the <b>Target Channel</b> or click <b>Create New Channel</b> to create a new target channel to which you plan to restore the channel data.</li> <li>4. Under <b>Recovery Options</b>, select an <b>Additional Team Owner</b> from the <b>Team Owner</b> drop-down list.</li> </ol>
<p>Restore the Team's data to a different Team that exists on a different Microsoft 365 domain.</p>	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the target Microsoft 365 domain from the <b>Registered Source</b> drop-down.</li> <li>3. Select the <b>Target Team</b> to which you plan to restore the data.</li> <li>4. Select the <b>Target Channel</b> or click <b>Create New Channel</b> to create a new target channel to which you plan to restore the channel data.</li> </ol>
<p>Restore the Team's data to a new Team on a different Microsoft 365 domain. Also, add a new owner.</p>	<ol style="list-style-type: none"> <li>1. Under <b>Recover To</b>, select <b>New Location</b>.</li> <li>2. Select the target Microsoft 365 domain from the <b>Registered Source</b> drop-down.</li> <li>3. Click <b>Create New Team</b> and specify the <b>Team Name</b>.</li> <li>4. From the <b>Target Channel</b> drop-down, click <b>Create New Channel</b> to create a new channel in the selected Team.</li> <li>5. Under <b>Recovery Options</b>, select an <b>Additional Team Owner</b> from the <b>Team Owner</b> drop-down list.</li> </ol>

[Download Teams Posts](#)


To download Teams Posts from all Channels:

1. Navigate to **Sources**.
2. Click on the required source and click the **Teams** tab.

3. Select **Show All > Protected** and use the other filters, search box, and views at the top to narrow your search.
4. Click the **Actions** menu next to the object and click **Download Teams Posts**.
5. In the **Download Teams Posts** page, select the required snapshot, provide the task name, and click **Recover**.
6. Click the **View Progress** button in the pop-up message or click the **Activity** menu.
7. Once the recovery is successful, click **Download**. The Teams Posts will be downloaded by default in the **.htm** format.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

To download Teams Posts from a single Channel:

1. Navigate to **Sources**.
2. Click on the required source and click the **Teams** tab.
3. Select **Show All > Protected** and use the other filters, search box, and views at the top to narrow your search.
4. Click the **Recover Teams Content** icon (  ) next to the object.
5. In the **Recover Teams Content** page, select the **Item Type** as **Channels**.
6. Hover over the required Channel and click the **Download Posts** button.
7. In the **Download Teams Items** page, select the required snapshot, provide the task name, and click **Download**.
8. Click the **View Progress** button in the pop-up message or click the **Activity** menu.
9. Once the recovery is successful, click **Download**. The Teams Posts will be downloaded.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature.

**Next >** Protect your Microsoft 365 [Mailboxes](#), [OneDrives](#), and [SharePoint Online Sites](#) so you can recover them easily when you need to, as well!

## Microsoft Groups

Microsoft 365 groups are used for collaboration between users, both inside and outside your company. With each Microsoft 365 group, members get a group email and shared workspace for conversations, files, calendar events, and a planner.

**Note:** This is an Early Access feature. Contact your Cohesity account team to enable the feature for your tenant.

Using the policy-based data protection solution from DataProtect as a Service for Government (FedRAMP), you can back up and recover Unified Groups data in Microsoft 365.

## Considerations

Review and understand the following considerations before you protect your Microsoft 365 Groups data:

- Granular recovery of Group messages and other contents is not supported.
- Restoring system document libraries is not supported. You can restore only the non-system document libraries on a Group site.
- The entities protected for Groups include the SharePoint sites associated with the Group.
- Mail-enabled security groups, security groups, and distribution lists are not supported.
- Granular recovery of Group sites is not supported when Site Tagging is enabled.
- Backup of Groups (Public and Private) with no owners is supported when at least one Exchange Online licensed member is available in the Group.

If no owners/members are available in the Group, you can contact your Cohesity account team to configure a service account (with an Exchange Online license). This service account will be added as a member of the Group before backup/recovery and removed after the backup/recovery is completed.

**Note:** This is a Private Preview feature. Private Preview was termed as Early Access in the earlier releases. Contact your Cohesity account team to enable the feature.

- File/folder permissions with no role will not be recovered since Microsoft does not allow adding such permissions via Graph APIs. For example, no role will be assigned when a Restricted View permission is added to a user from Advanced Setting.

## Protect Microsoft 365 Groups

Once you have [registered your Microsoft 365 domain](#) as a source, you're ready to protect the Groups in your domain.

To protect your Microsoft 365 Groups:

1. In **DataProtect as a Service**, under **Sources**, find the Microsoft 365 source and click into it.
2. Click the **Group** tab.
3. Select the individual Team you wish to protect or:
  - Click **Groups** > **Select All Child Objects** to protect all the Teams in this source.
  - Click **Groups** > **Auto Protect This** to protect all the Teams in this source.
4. Click the **Protect** icon above the list.
5. Choose a policy to specify backup frequency and retention. If you don't have a policy, you can easily [create one](#).
6. Under **Settings**, edit the **Start Time** if necessary.
7. Under **Additional Settings**, you can enable **Indexing**, configure a specific **End Date**, **Alerts**, and other [additional settings](#).

**Note:** If you plan to recover individual document library items (coming soon!), in addition to whole sites, you need to enable **Indexing** in this step. When you do, you can include or exclude specific sites from indexing.

8. Click **Protect**.

**Note:** The backups start immediately after you protect the objects, regardless of the time you set for the protection run.

### Additional Settings

Advance Settings	Description
<b>Start Time</b>	Available only if the selected policy is set to <b>Backup Daily</b> . Indicates what time the protection run should start. Enter the <b>Start Time</b> and select <b>AM</b> or <b>PM</b> . The default time zone is the browser's time zone. You can change the time zone of the protection run by selecting a different time zone here.

Advance Settings	Description
<b>SLA</b>	<p>The service-level agreement (SLA) defines how long the administrator expects a protection run to take. Enter:</p> <ul style="list-style-type: none"> <li>• <b>Full.</b> The number of minutes you expect a full protection run, which captures all the blocks in an object, to take.</li> <li>• <b>Incremental.</b> The number of minutes you expect an incremental protection run, which captures only the changed blocks in an object, to take.</li> </ul>
<b>Cancel Runs at Quiet Time Start</b>	<p><i>(Available only if the selected policy has at least one Quiet Time)</i></p> <p>When enabled, all the protection runs that are currently executing will cancel when the Quiet Time period starts. By default, this setting is disabled, meaning that after a protection run starts, it continues to execute even when a Quiet Time period starts. However, new protection runs will not start during a Quiet Time.</p>

## Manage Existing Protection


Edit protection settings, change the policy, and start, stop, & pause protection.

Once you have [applied protection](#) to the objects in your sources, DataProtect as a Service for Government (FedRAMP) makes it easy to make changes to that protection quickly. You can:

- Edit additional settings like **End Date, Exclusions, Alerts**, and more.
- Apply a different policy.
- Start an on-demand protection run, pause and resume it, or even remove protection.

### Edit Protection Settings

To edit protection settings:

1. In **DataProtect as a Service**, navigate to **Sources**.
2. Click on the **Source** name.
3. Select **Show All > Protected** and use the other filters, search box, and views at the top to narrow your search.
4. Click the **Actions** menu (  ) next to the object and select **Edit Protection** to open the protection settings for that object.

### Apply a New Protection Policy

To change the **Policy**, click the drop-down and select a different policy. To help you choose, each policy in the list shows the **Backup** frequency and the **Retain** period for each backup.

If you don't have a policy that meets your needs, scroll to the bottom of the list and click **Create Policy** to [create your own policy](#).



Edit Additional Protection Settings

Under **Settings**, you can change the protection **Start Time** (and select the **Time Zone**). Click the drop-down next to **Additional Settings** to change more options. See [Additional Protection Settings](#) for details.

Start, Stop, or Remove Protection

When you select protected objects in one of your sources, DataProtect as a Service for Government (FedRAMP) presents buttons for the actions that are possible for those objects. With the protected objects selected, you can click:

- **Recover** to recover the Groups.
- **Run Now** to start an on-demand protection run immediately.
- **Unprotect** to remove protection from the object.

**Tip:** If a protected object is deleted from the source, you can search the object using Global Search and unprotect it.

Additional Settings

Advance Settings	Description
<b>Start Time</b>	Available only if the selected policy is set to <b>Backup Daily</b> . Indicates what time the protection run should start. Enter the <b>Start Time</b> and select <b>AM</b> or <b>PM</b> . The default time zone is the browser's time zone. You can change the time zone of the protection run by selecting a different time zone here.
<b>SLA</b>	The service-level agreement (SLA) defines how long the administrator expects a protection run to take. Enter: <ul style="list-style-type: none"> <li>• <b>Full</b>. The number of minutes you expect a full protection run, which captures all the blocks in an object, to take.</li> <li>• <b>Incremental</b>. The number of minutes you expect an incremental protection run, which captures only the changed blocks in an object, to take.</li> </ul>
<b>Cancel Runs at Quiet Time Start</b>	<i>(Available only if the selected policy has at least one Quiet Time)</i> When enabled, all the protection runs that are currently executing will cancel when the Quiet Time period starts. By default, this setting is disabled, meaning that after a protection run starts, it continues to execute even when a Quiet Time period starts. However, new protection runs will not start during a Quiet Time.

## Recover Groups

After you protect the Groups in your domain, you can recover them as whole Groups from DataProtect as a Service for Government (FedRAMP), to the same Microsoft 365 Group, to an alternate Microsoft 365 Group, or to a new Microsoft 365 Group in the same Microsoft 365 domain.

### Points to note:

- Granular recovery of Group contents is not supported.
- If you're restoring a Group that does not exist in the Microsoft 365 domain, Cohesity creates a new Group with the metadata and data from the backup snapshot.
- If you restore to an existing Group, the group resources in the existing Microsoft 365 Group are overwritten or appended with the restored data. The following table details the group resources that are overwritten or appended:

Restore Behavior	Group Resource Type
Appended	members
	owners
	mails (data)
Overwritten	hideFromAddressLists
	hideFromOutlookClients
	displayName visibility
	securityEnabled
	description
	theme

You can restore the Microsoft 365 Group data to:

- The same Microsoft 365 Group.
- A different Microsoft 365 Group in the same Microsoft 365 domain.
- A new Microsoft 365 Group in the same Microsoft 365 domain.

To recover protected Microsoft 365 Group:

1. In **DataProtect as a Service**, go to **Sources** to set up your recovery task.
2. Click on the **Source** name and select the **Group** tab.
3. Above the tree, select **Show All > Protected**.
4. Find the Group you need and click the **Recover** button on that row to open the **New Recovery** form with the **Latest** snapshot (protection run).
5. In the **New Recovery** form, if you need to add more Groups and/or recover from an earlier backup, click the **Edit** icon in the top right of the form.
  1. To add Teams, enter a **Search** term on the left, locate the other Teams, and select them.
  2. To use a different **Recovery Point** for a Team, click the **Edit** icon on the tile for that Team. Find the recovery point you need and click **Select Recovery Point**.
6. Click **Next: Recover Options** to return to the form.
7. Under **Recover To**, select **Original Location** or **New Location**.  
If you choose **New Location**, specify the **Group Name** and the **Group SMTP**.
8. Select your **Recovery Options**:
  1. **Continue on Error**. Enable to recover even if errors occur when recovering Groups. For example, if one of the Groups cannot be recovered, Cohesity will still attempt to recover the other selected Groups.
  2. **Task Name**. Change the default name of the recovery task.
9. Click **Start Recovery**.

**Next** > Protect your Microsoft 365 [Mailboxes](#), [OneDrives](#), [SharePoint Online Sites](#), and [Teams](#) so you can recover them easily when you need to, as well!

# Monitoring

## Reports

Cohesity provides one-stop-shop reporting on DataProtect as a Service for Government (FedRAMP). You have an aggregated view of your Cohesity deployment regardless of the use case, workload, or deployment type (on-premises, consumed as a Cohesity-hosted service, or a combination).

The built-in reports are designed to address your top use cases out-of-the-box. You can view an overall summary of your data protection jobs and storage systems, or analyze data at the granular level using powerful filtering options. You can filter, schedule, email, and download reports.

**Note:** A user logging in to DataProtect as a Service for Government (FedRAMP) through SSO cannot schedule reports if its user account is not available on the **Access Management** page.

The report that you schedule or download inherits the filters that you have applied.

## View Reports

To view a report:

1. [Log in to DataProtect as a Service for Government \(FedRAMP\)](#).
2. In **DataProtect as a Service**, navigate to **Reports**.  
By default, the **Library** tab is displayed.
3. Click a report card. For more information, see [Choose a Report Type](#).

Each report helps you view, visualize, and analyze data. The following table describes the key features of reports:

Filters	Each report provides various filters that help you pare down the report until it only shows the data that you want in the report. The filter options change depending on the type of report. For more information, see <a href="#">Filter Report Data</a> .
Glance bar	The glance bar provides a summary of the report for the time period you set in the filter.
Charts	Each report includes chart(s) that provide a graphical representation of data.

Data table	The <b>Data</b> table in the report provides deeper insights to help you analyze the data. You can customize the columns in the table. For more information, see <a href="#">Customize Table Columns</a> .
Common tasks	You can perform the following tasks: <ul style="list-style-type: none"> <li>• <a href="#">Download Reports</a></li> <li>• <a href="#">Schedule Reports</a></li> <li>• <a href="#">Manage Scheduled Reports</a></li> <li>• <a href="#">Reset to Default View</a></li> </ul>

## Choose a Report Type

Each different report type can help you identify the information you need. Currently, 16 built-in reports are available:

- [Failures](#)
- [Protected / Unprotected Objects](#)
- [Protection Runs](#)
- [Recovery](#)

## Filter Report Data

Reporting in DataProtect as a Service for Government (FedRAMP) provides a comprehensive view of the data under management. You have full control over what data you want to include and view in your reports. Use the filters to pare down your report until it only shows the data that you want in the report. The filter options change depending on the type of report.

For more information about the filtering options available in each report, refer to the help page for the respective report.

## Customize Table Columns

Each report in DataProtect as a Service for Government (FedRAMP) provides comprehensive data. In each report, data is displayed in a tabular format. You can add and remove columns from the **Data** table. The changes you make to columns in a table persist until you change them again or restore the report to the default view.

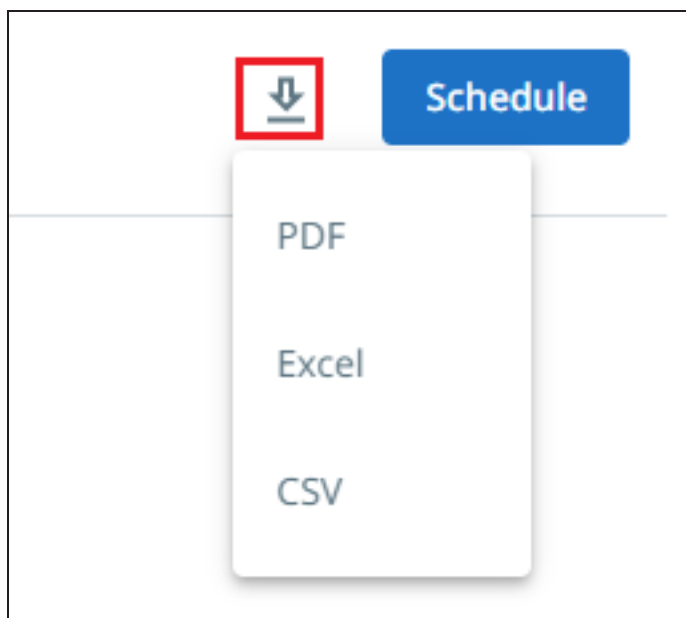
To customize table columns:

1. [Log in to DataProtect as a Service for Government \(FedRAMP\)](#).
2. In **DataProtect as a Service**, navigate to **Reports**.

3. Click a report card.
4. In the upper-right corner of the table, click the **Settings** (⚙️) icon:
  - Enable the toggle to add a column
  - Disable the toggle to remove a column

## Download Reports

You can download reports in different file formats from the reports page. On any report, click the **Download** icon and select one of the file formats:



The report in the selected file format gets downloaded to your system.

**Note:** The time taken to generate a report depends on multiple factors such as the number of clusters selected, other filters applied on the report, amount of data, and so on. If the report is very large, it may take a few moments to download the report.

## Schedule Reports

You can schedule reports to run at periodic intervals. Once you select a report and filter the scope, you can schedule the report to run and send an email to recipients at specified times.

### Important Points to Note

- SSO users can view and download reports. To schedule reports, SSO users must be explicitly added in DataProtect as a Service for Government (FedRAMP). For more information about explicitly adding users, see [Add SSO Users & Groups](#).
- If the report is too large, the email will contain a download link instead of an attachment.
- Columns included in the scheduled report are the columns available in the default view. If you have customized the table, those changes are not reflected in the scheduled report.

To schedule reports:


1. [Log in to DataProtect as a Service for Government \(FedRAMP\)](#).
2. In **DataProtect as a Service**, navigate to **Reports**.
3. Click a report card. For more information, see [Choose a Report Type](#).
4. Click **Schedule**.

**Note:** If the SSO user is not explicitly added in DataProtect as a Service for Government (FedRAMP), the **Schedule** button is not displayed.


The **Schedule Report** pop-up window is displayed:


## Schedule Report

**Schedule Name**




**Schedule**

Every  

At   Time Zone

**Recipients**

 Recipients' Emails

**Format**

PDF  CSV  Excel

5. Configure the following details:

- **Schedule Name**—Enter a name for your report.
- **Schedule**—Choose the frequency and the time at which to run the report.
- **Recipients**—Enter the email address of the recipient. You can enter multiple email addresses.
- **Email Subject**—Enter a subject line for the email.
- **Format**—Select the format(s). The recipients receive the report in the format that you select.

6. Click **Schedule**.

The recipients receive a new email with the updated report on the schedule you selected. See your scheduled reports under the **Scheduled** tab on the **Reporting** page.

## Manage Scheduled Reports


You can perform the following tasks from the **Scheduled** tab:



- Instantly run a report
- Pause a report
- Modify the settings of a report
- Delete a report

**Note:** Users with the **Super Admin** role can view and manage all scheduled reports in the same DataProtect as a Service for Government (FedRAMP) account.

To manage scheduled reports:

1. [Log in to DataProtect as a Service for Government \(FedRAMP\)](#).
2. In **DataProtect as a Service**, navigate to **Reports**.
3. Click the **Scheduled** tab.
4. Hover over a report and click the **Actions** menu (  ):
  - Select **Run Now** to instantly run and email the report.
  - Select **Pause** to pause the schedule.
  - Select **Edit** to modify the settings of a scheduled report. Update the settings as necessary and click **Schedule**.
  - Select **Delete** to delete a scheduled report. You must click **Delete** to confirm the deletion.

## Reset to Default View

Once you filter a report or customize table columns, you can reset the report page's view to the default view. To switch to the default reports page view, click the **Restore to default display** button:



The page refreshes and reverts to the default view.

## Failures

The **Failures** report provides a summary and list of objects that had one or more backup run failures. It also helps you identify consecutive failures in the last three backups, and breaks down the failed objects by object type.

**Example use case:** Which object do I have no successful backup of in the last week?

### Filter Report Data

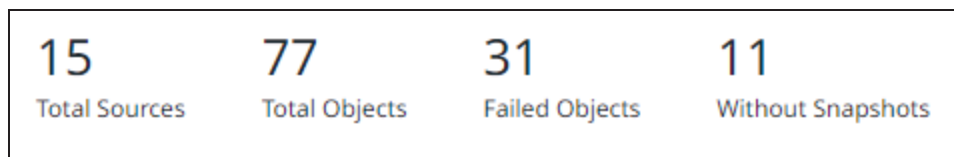
The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all cluster(s) to include.
- **Source**—Select all the sources to include.
- **Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.
- **Time Range**—Set the time period for your report.
- **Object**—Enter an object name to filter by the name of the object.
- **Organization**—Choose one or more organizations to see the report data specific to the selected organizations.

### Glance Bar

The glance bar provides a summary of the report for the specified period:

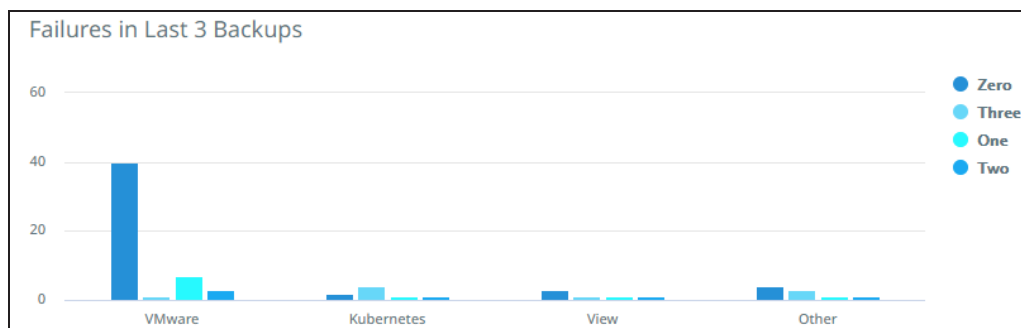
- **Total Sources**—The total number of sources.
- **Total Objects**—The total number of objects.
- **Failed Objects**—The total number of objects that experienced one or more backup run failures during the specified date range.
- **Without Snapshots**—The total number of objects without any snapshots.



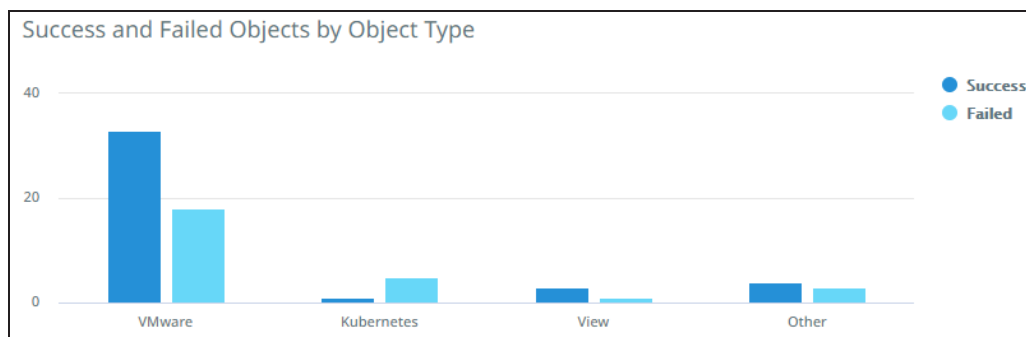
### Charts

The report includes the following two charts:

- **Failures in Last 3 Backups**



- **Success and Failed Objects by Object Type**



### Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by object name, source, system name, or policy.

**Note:** You can add or remove columns. For more information, see [Customize Table Columns](#).

The data displayed in the **Policy** and **System** columns are from the last backup run of the object in the specified time period.

Column Name	Description
Object Name	The name of the object.
Source	The hostname or IP address of the registered source.
System	The name of the cluster on which the protection job was run.
Policy	The protection policy associated with the Protection Group.
Last Failed Run	The date and time at which the last backup run failed.
Failed Backups	The total number of backup runs that failed.
Failures in Last 3 Backups	The total number of failures in the last three backups.
Last Fail Reason	The reason for the failure of the last backup.

### Related Topics

- [View Reports](#)
- [Filter Report Data](#)

- [Download Reports](#)
- [Schedule Reports](#)
- [Manage Scheduled Reports](#)
- [Reset to Default View](#)

## Protected Objects

The **Protected Objects** report provides a summary and list of all protected objects that had a backup run. You can view the backup status and the objects with an active snapshot.

**Example use case:** Do I have a good backup of my VM in the last month?

### Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all cluster(s) to include.
- **Source**—Select all the sources to include.
- **Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.
- **Backup Status**—Filter by objects with successful backups or unsuccessful backups.
- **Last Run Status**—Filter by the status of the most recent protection run — Canceled, Failed, Running, Success, and/or Warning.
- **Time Range**—Set the time period for your report.

**Note:** If you set a time period, the report displays all objects that had a backup run during the selected time period. If an object is no longer protected, the report would still display data if the object had a backup run during the selected time period. If an object is protected and if it did not have a backup run during the selected time period, the report does not display the data specific to this object.

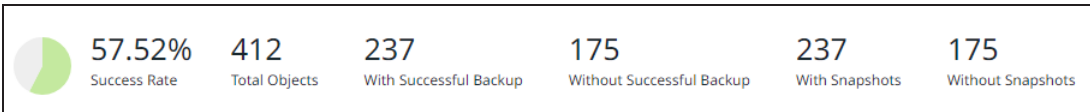
- **Object**—Enter an object name to filter by the name of the object.
- **Organization**—Choose one or more organizations to see the report data specific to the selected organizations.

### Glance Bar

The glance bar provides a summary of the report for the specified period:

- **Success Rate**—**Without Successful Backup / Total Objects.**
- **Total Objects**—The total number of objects.

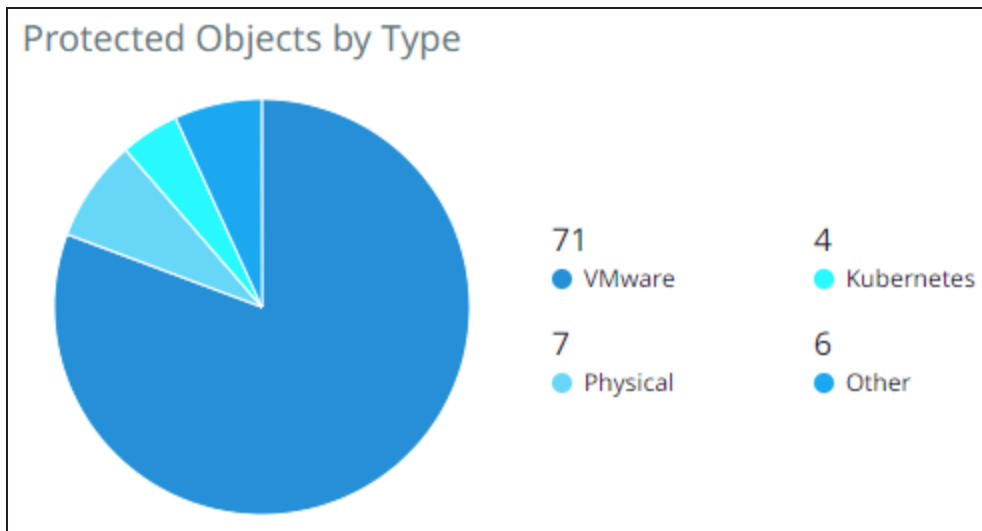
- **With Successful Backup**—The total number of objects that have one or more successful backups.
- **Without Successful Backup**—The total number of objects that did not have any successful protection runs.
- **With Snapshots**—The total number of objects with snapshots retained. This number can differ from the earlier “With Successful Backups”, for example, all backups fail for an object during the selected date range but the object still has actively retained snapshots from earlier backups (that occurred before the selected date range).
- **Without Snapshots**—The total number of objects without snapshots.



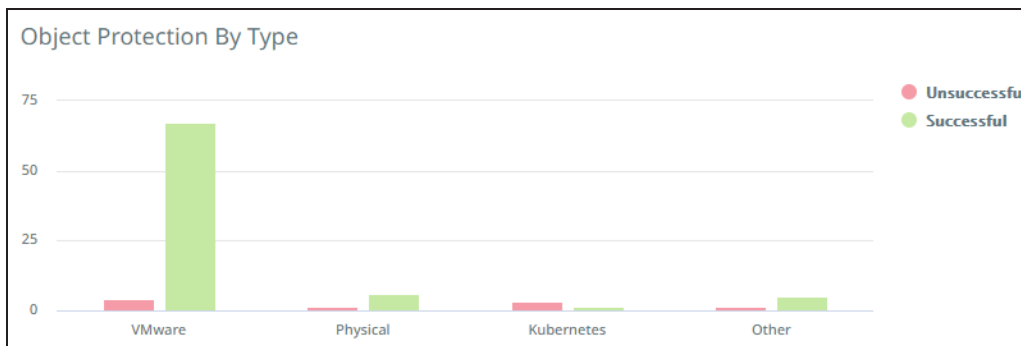
### Charts

The report includes the following two charts:

- **Protected Objects by Type**



- **Object Protection by Type**



## Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by object name, system name, source, or policy.

**Note:** You can add or remove columns. For more information, see [Customize Table Columns](#).

Column Name	Description
Object Name	The name of the protected object.
Source	The hostname or IP address of the registered source.
Policy	The protection policy associated with the latest run of the object.
Last Run	The date and time at which the last backup for the object ran.
Last Successful Backup	The date and time at which the last successful backup for the object ran.
Active Snapshots	The total number of active snapshots for the object.
Successful Backups	The total number of successful backups for the object.
Unsuccessful Backups	The total number of unsuccessful backups for the object.
System	The name of the cluster on which the object had the latest run.

## Related Topics

- [View Reports](#)
- [Filter Report Data](#)
- [Download Reports](#)
- [Schedule Reports](#)
- [Manage Scheduled Reports](#)
- [Reset to Default View](#)

## Protected / Unprotected Objects

The **Protected / Unprotected Objects** report provides a summary and list of objects along with their protection status. You can identify objects that are not associated with a Protection Group. The report does not contain data about Cohesity views.

**Example use case:** Are all the objects in my vCenter protected?

**Filter Report Data**

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all cluster(s) to include.
- **Source**—Select all the sources to include.
- **Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.
- **Protection Status**—Filter by object protection status — Protected or Unprotected.
- **Object**—Enter an object name to filter by the name of the object.
- **Organization**—Choose one or more organizations to see the report data specific to the selected organizations.

**Glance Bar**

The glance bar provides a summary of the report for the specified period:

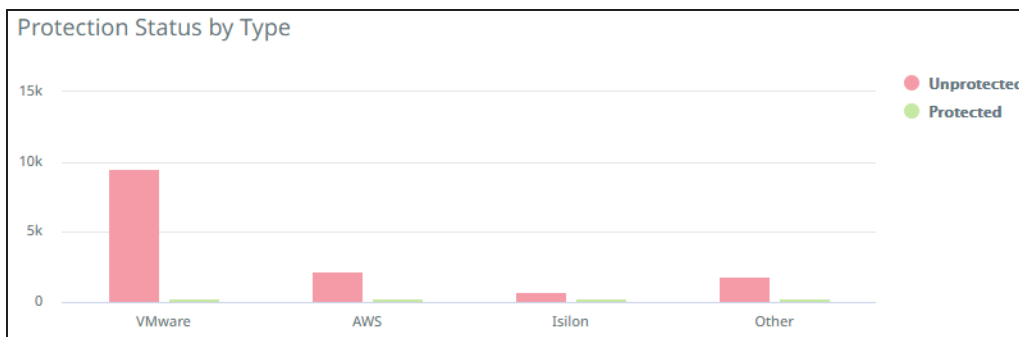
- **Protected Objects**—The percentage of **Protected Objects** to **Total Objects**.
- **Total Sources**—The total number of sources.
- **Total Objects**—The total number of objects.
- **Protected Objects**—The total number of protected objects.
- **Unprotected Objects**—The total number of unprotected objects.



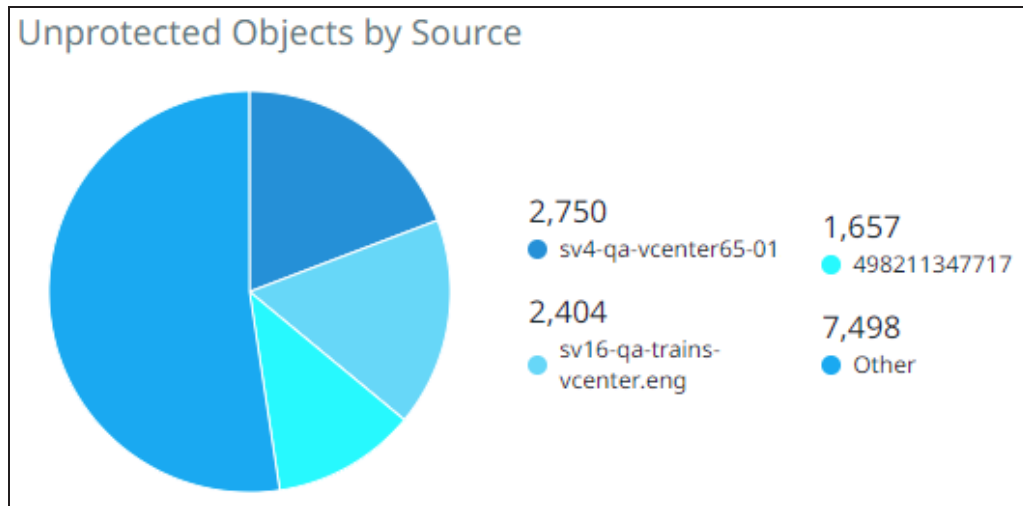
**Charts**

The report includes the following two charts:

- **Protection Status by Type**



• **Unprotected Objects by Source**



**Report Data**

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by object name, protection status, source, or system name.

**Note:** You can add or remove columns. For more information, see [Customize Table Columns](#).

Column Name	Description
Object Name	The name of the object.
Protection Status	The protection status of the object.
Source	The name of the registered source.
System	The name of the cluster on which the object is registered.



Column Name	Description
Logical Data	<p>The combined total of data in the objects that are protected by Cohesity. These metrics are different depending on workload type.</p> <ul style="list-style-type: none"> <li>• <b>VMs</b>—The data size reported by VMware is the provisioned amount, not the actual data residing in the VM. For example, if a VM is provisioned for 1 TB but contains only 100 GB of data, VMware reports it as 1 TB.</li> <li>• <b>All Other Workloads</b>—The data size reported is the actual front end data residing on the server. If a server with 1 TB capacity contains 100 GB of data, the server reports 100 GB.</li> </ul> <p><b>Note:</b> Cohesity does not include unprotected objects in these metrics.</p>
Organization	The name specified for the organization when added to the cluster.

## Related Topics

- [View Reports](#)
- [Filter Report Data](#)
- [Download Reports](#)
- [Schedule Reports](#)
- [Manage Scheduled Reports](#)
- [Reset to Default View](#)

## Protection Runs

The **Protection Runs** report provides a summary and list of all backup activities per object per run. You can view the summary and success rate of protection runs. You can also view the snapshot status of the protection run.

**Example use case:** How many failed protection runs did I have in the last week?

### Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all cluster(s) to include.
- **Source**—Select all the sources to include.
- **Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.

- **Run Status**—Filter by the status of the protection run — Canceled, Failed, Running, Success, and/or Warning.
- **Snapshot Status**—Filter by the status of the snapshot — Active or Expired.
- **Time Range**—Set the time period for your report.
- **Organization**—Choose one or more organizations to see the report data specific to the selected organizations.

**Glance Bar**

The glance bar provides a summary of the report for the specified period:

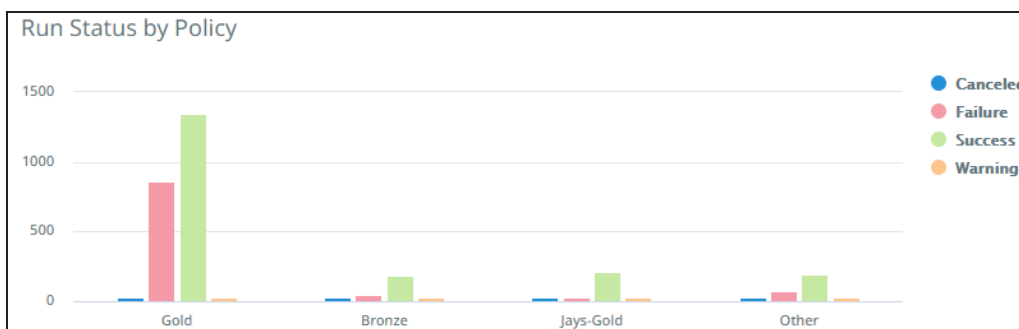
- **Success Rate**—Total Successful / Total Runs.
- **Total Runs**—The total number of protection runs.
- **Total Successful**—The total number of successful runs.
- **Success**—The total number of protection runs with status Success.
- **Warning**—The total number of protection runs with status Warning.
- **Failed**—The total number of protection runs with status Failed.
- **Canceled**—The total number of protection runs with status Canceled.
- **Running**—The total number of protection runs with status Running.
- **SLA Met**—The total number of protection runs that met SLA.
- **SLA Missed**—The total number of protection runs that missed SLA.



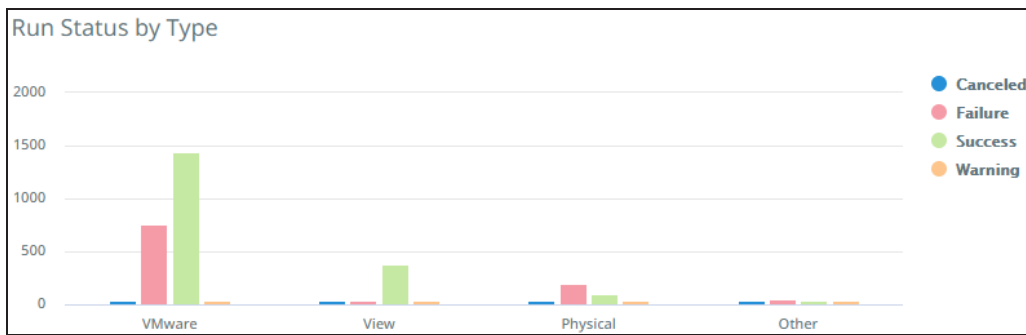
**Charts**

The report includes the following two charts:

- **Run Status by Policy**



• **Run Status by Type**



**Report Data**

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by object name, source, policy, system name, or snapshot status.

**Note:** You can add or remove columns. For more information, see [Customize Table Columns](#).

Column Name	Description
Start Time	The date and time at which the protection run started.
End Time	The date and time at which the protection run was completed.
Object Name	The name of the protected object.
Source	The hostname or IP address of the registered source.
Policy	The protection policy associated with the protection run for the corresponding object.
System	The name of the cluster on which the object had a protection run.
Snapshot Status	The status of the snapshot.
Duration	The time taken by the protection run.

Column Name	Description
Logical Data	<p>The combined total of data in the objects that are protected by Cohesity. These metrics are different depending on workload type.</p> <ul style="list-style-type: none"> <li>• <b>VMs</b>—The data size reported by VMware is the provisioned amount, not the actual data residing in the VM. For example, if a VM is provisioned for 1 TB but contains only 100 GB of data, VMware reports it as 1 TB.</li> <li>• <b>All Other Workloads</b>—The data size reported is the actual front end data residing on the server. If a server with 1 TB capacity contains 100GB of data, the server reports 100 GB.</li> </ul> <p><b>Note:</b> Cohesity does not include unprotected objects in these metrics. Currently, the logical data value shown on the DataProtect as a Service for Government (FedRAMP) Dashboard is a sum of the logical data values captured across all the protection runs. For instance, if the source has 100 GB of logical data, and assuming it remains at 100 GB for the first 10 protection runs, Cohesity would report, after 10 runs, the Logical Data to be 1000 GB (1 TB).</p>
Data Read	<p>Size of the set of protected objects as read by Cohesity for a single backup run. This number is a per protection run statistic and is not additive across backup runs.</p>
Data Written	<p>Data written on the Cohesity platform after the unique logical data has been reduced by data deduplication and data compression.</p> <p><b>Note:</b> This number reflects unique data written, before resiliency operations.</p>
Organization	<p>The name specified for the organization when added to the cluster.</p>

## Related Topics

- [View Reports](#)
- [Filter Report Data](#)
- [Download Reports](#)
- [Schedule Reports](#)
- [Manage Scheduled Reports](#)
- [Reset to Default View](#)

## Recovery

The **Recovery** report provides a summary and list of all the clone and recovery tasks that were executed. It also provides other details such as the time taken for the operation and status of the operation.

**Note:** If a Cohesity view is unprotected, the report does not display data about clone view operations.

**Example use case:** How many recovery tasks failed in the last week?

### Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all cluster(s) to include.
- **Source**—Select all the sources to include.
- **Organization** – Choose one or more organizations to see the report data specific to the selected organizations.
- **Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.
- **Status**—Filter by the status of the recovery task — Canceled, Failed, Running, Success, and/or Warning.
- **Time Range**—Set the time period for your report.
- **Object**—Enter an object name to filter by the name of the object.

### Glance Bar

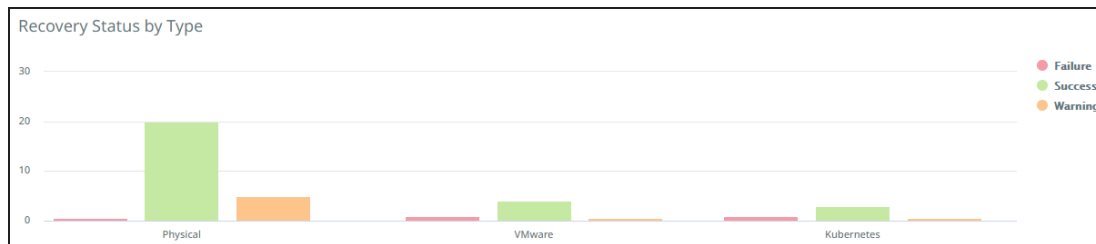
The glance bar provides a summary of the report for the specified period:

- **Success Rate—Successful / Total Recoveries.**
- **Total Recoveries**—The total number of recovery runs.
- **Successful**—The total number of recoveries with status Success.
- **Failed**—The total number of recoveries with status Failed.
- **Warning**—The total number of recoveries with status Warning.
- **Canceled**—The total number of recoveries with status Canceled.
- **Running**—The total number of recoveries with status Running.



### Chart

The report includes the **Recovery Status by Type** chart:



### Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by object name, source, system name, task name, or username.

Column Name	Description
Start Time	The date and time at which the recovery task started.
Object Name	The name of the object.
Source	The hostname or IP address of the registered source.
System	The name of the cluster on which the recovery task was run.
Recovery Point	The date and time of the backup run from which the object was recovered.
Duration	The time taken by the recovery task.
Task Name	The name of the recovery task.
Username	The name of the user who initiated the recovery.

### Service Consumption

The **Service Consumption** report provides statistics — like average usage, peak usage, and change rates — about the DataProtect as a Service for Government (FedRAMP) consumed by your protected objects. It also helps break down current usage and monthly peak usage by type.

### Detect Ransomware Attacks

Ransomware can take over enterprise data and threaten to publish it or block access to it until a ransom is paid. DataProtect as a Service for Government (FedRAMP) detects

potential ransomware attacks in your environment.

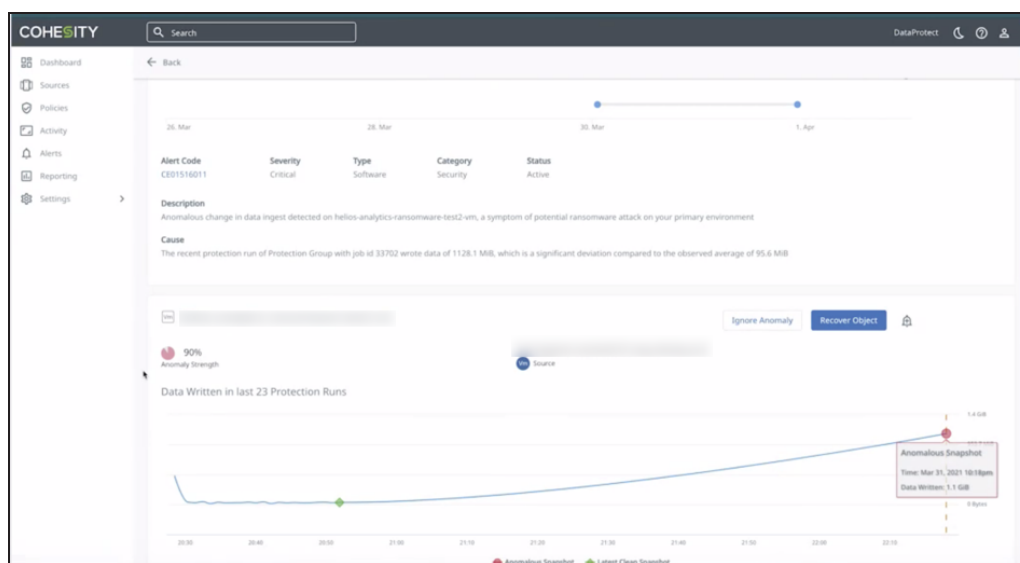
We use machine learning algorithms to continuously monitor change rates in the backup data. If the rate is out of the normal range — based on daily and historical rates — DataProtect as a Service for Government (FedRAMP) flags it as a potential ransomware attack.

If DataProtect as a Service for Government (FedRAMP) detects an anomaly during a protection run of your data, it triggers the critical alert, **DataIngestAnomalyAlert**. Using the alert information, you can investigate the anomaly and decide on the next course of action.

After reviewing the anomaly, you can either ignore the anomaly or recover the object from the last clean snapshot.

To locate and inspect potential anomalies:

1. In **DataProtect as a Service**, navigate to **Health > Alerts** and then click the **Severity** filter.
2. Select **Critical** and click **Apply**.
3. If you see a **DataIngestAnomalyAlert** alert, click into it.
4. On the **DataIngestAnomalyAlert** page, review the alert details.
5. Once you have thoroughly reviewed the alert, click:
  - **Ignore Anomaly** to dismiss the anomaly.
  - **Recover Object** to recover the object from the last clean snapshot.



## Alerts

The DataProtect as a Service for Government (FedRAMP) creates an alert for various reasons:

- It finds a potential problem
- Certain criteria exceed the defined threshold
- Informational events which occur in the system
- To indicate the success or failure of the protection run.

Each alert has a severity rating that indicates the seriousness of the problem:

- **Critical**—Immediate action is required because it detects a severe problem that might be imminent or major functionality is not working, such as a missing VM backup.
- **Warning**—Action is required, but the affected functionality is still working, such as the restore task failed due to some external target connectivity and/or credentials issues.
- **Informational**—Immediate action is not required, and the alert provides an informational message.

For a listing of the Alerts created by the DataProtect as a Service for Government (FedRAMP), see [Alerts References](#).

## Analyze the Alert

You can click on an alert from the **Alerts** tab and view the alert details on the **Details for <Alert\_Name>** page.

The **Details for <Alert\_Name>** page includes a timeline view showing the date and time the alert was triggered. The page also provides the following details of the alert:

Details	Description
<b>Alert Code</b>	The alert code. You can click on the alert code for detailed information about the alert.
<b>Severity</b>	The severity rating of the alert.
<b>Type</b>	The alert type. It defines the Cohesity component that triggered the alert.
<b>Category</b>	The alert category.
<b>Status</b>	The status of the alert. It can be Active, Resolved, or Note.
<b>Description</b>	A brief description of the problem that triggered the alert.
<b>Cause</b>	A brief description of the cause of the problem.



## Alert Notification

You can configure general alert email notifications or enable Webhooks for alerts notification in the **Health > Notification** tab. For more information, see [Configure Alert Notification Settings](#).

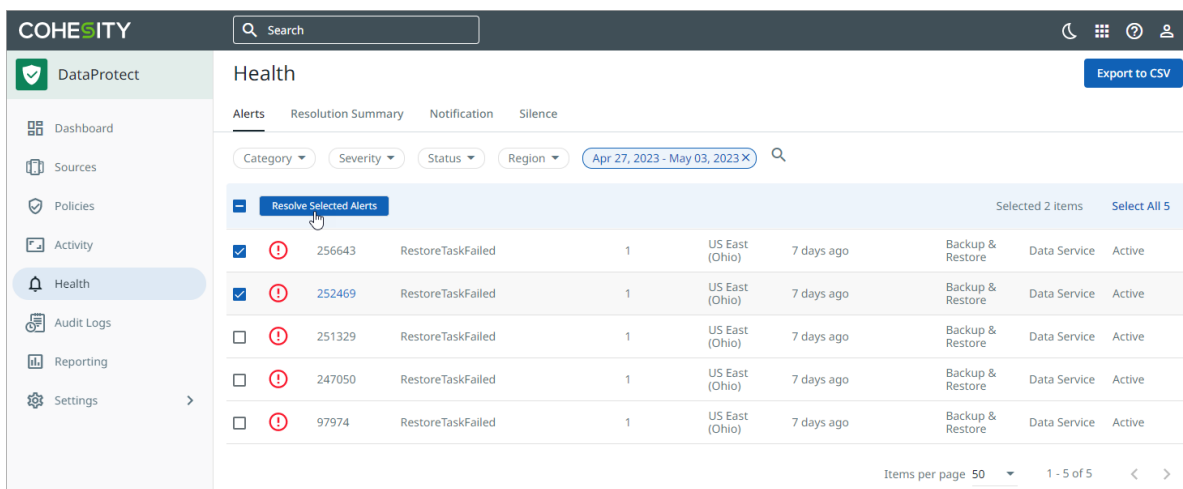
## Resolve Alerts

In case if you are aware of the problem and confirm that the issue has been resolved or if the issue does not require further attention, from the Alerts tab, you can manually resolve those alert(s). You can either create a new resolution of the alert(s) or attach an existing resolution to the alert(s).

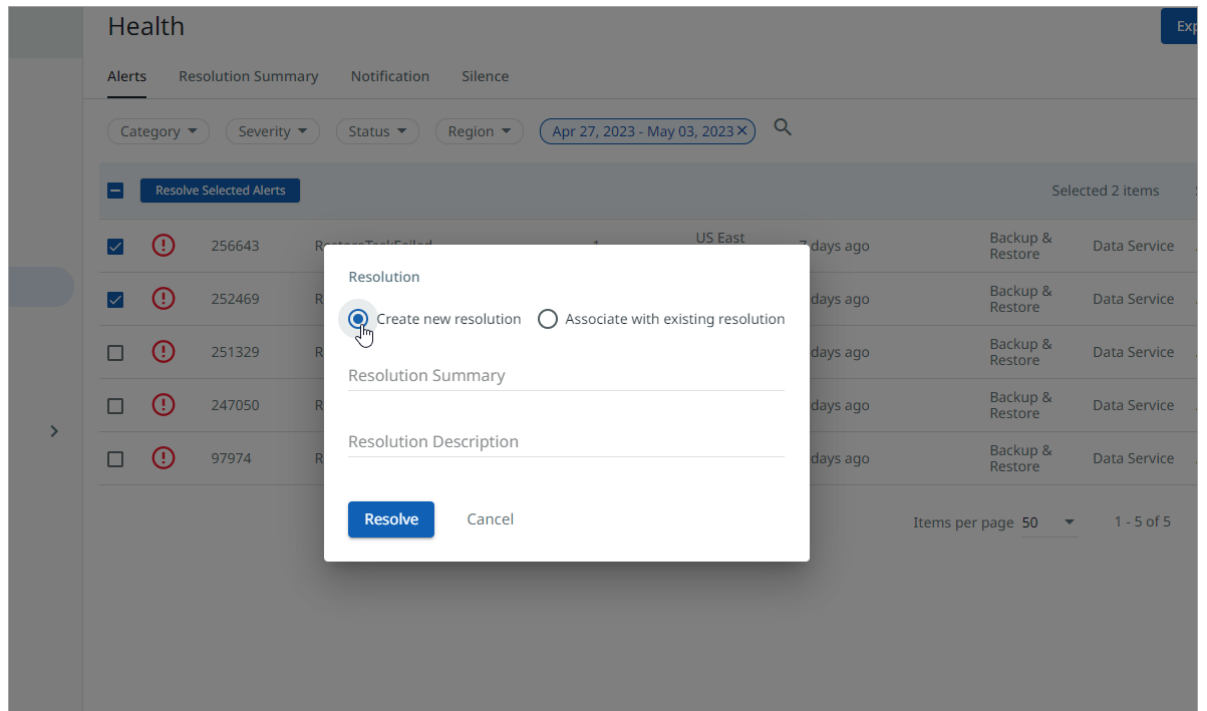
### Create a New Resolution

To create a new resolution:

1. In the **Alerts** tab, select an alert or multiple alerts that you plan to resolve and click **Resolve Selected Alerts**.



2. In the **Resolution** dialog, do the following:
  1. Select **Create new resolution**.



2. In the **Resolution Summary** field, add a resolution summary for the alert.
3. In the **Resolution Description** field, add a brief description of the resolution.
4. Click **Resolve**.

The resolution is added to the selected alerts, and the alert(s) status is marked as **Resolved**.

### Attach an Existing Resolution

To attach an existing resolution to the alert(s):

1. In the **Alerts** tab, select an alert or multiple alerts that you plan to resolve and click **Resolve Selected Alerts**.

The screenshot shows the COHE SITY Health Alerts interface. The left sidebar contains navigation options: Dashboard, Sources, Policies, Activity, Health (selected), Audit Logs, Reporting, and Settings. The main content area is titled 'Health' and includes tabs for Alerts, Resolution Summary, Notification, and Silence. A search bar and filters for Category, Severity, Status, and Region are present. A date range filter is set to 'Apr 27, 2023 - May 03, 2023'. A table of alerts is displayed with columns for ID, Category, Severity, Status, Region, Time, and Action. Two alerts are selected, and the 'Resolve Selected Alerts' button is highlighted. The table data is as follows:

ID	Category	Severity	Status	Region	Time	Action
256643	RestoreTaskFailed	High	Active	US East (Ohio)	7 days ago	Backup & Restore
252469	RestoreTaskFailed	High	Active	US East (Ohio)	7 days ago	Backup & Restore
251329	RestoreTaskFailed	High	Active	US East (Ohio)	7 days ago	Backup & Restore
247050	RestoreTaskFailed	High	Active	US East (Ohio)	7 days ago	Backup & Restore
97974	RestoreTaskFailed	High	Active	US East (Ohio)	7 days ago	Backup & Restore

2. In the **Resolution** dialog, do the following:

1. Select **Associate with existing resolution.**

The screenshot shows the 'Resolution' dialog box overlaid on the Health Alerts page. The dialog box has the following elements:

- Resolution** (Section Header)
- Create new resolution
- Associate with existing resolution
- Resolution Summary \* (Dropdown menu)
- Resolution Description (Text input field)
- Resolve (Blue button)
- Cancel (Text button)

2. From the **Resolution Summary** drop-down, you can search and select the resolution that you plan to attach to the alert.

3. Click **Resolve**.

The existing resolution is attached to the selected alerts, and the status of the alert(s) are marked as **Resolved**.

### Resolve an alert in the Details for <Alert\_Name> page

Once you have reviewed the alert, you can resolve the alert using the page's **Resolution** section. You can create a new alert resolution or attach an existing one in the **Resolution** section.

The screenshot shows the COHESITY interface for an alert titled "Details for RestoreTaskFailed". The interface includes a sidebar with navigation options like Dashboard, Sources, Policies, Activity, Health, Audit Logs, Reporting, and Settings. The main content area shows the alert details, including a date range selector, a timeline graph, and a table with columns for Alert Code, Severity, Type, Category, and Status. Below the table, there are sections for Description and Cause. The "Resolution" section is highlighted with a red box and contains two radio buttons: "Create new resolution" (selected) and "Associate with existing resolution". Below these are text input fields for "Resolution Summary" and "Resolution Description", and a "Resolve" button.

To create a new resolution:

1. In the **Resolution** section, select **Create new resolution**.
2. In the **Resolution Summary** field, add a resolution summary for the alert.
3. In the **Resolution Description** field, add a brief description of the resolution.
4. Click **Resolve**.

To attach an existing resolution:

1. In the **Resolution** section, select **Associate with existing resolution**.
2. From the **Resolution Summary** drop-down, you can search and select the resolution that you plan to attach to the alert.
3. Click **Resolve**.

## Configure Alert Notification Settings

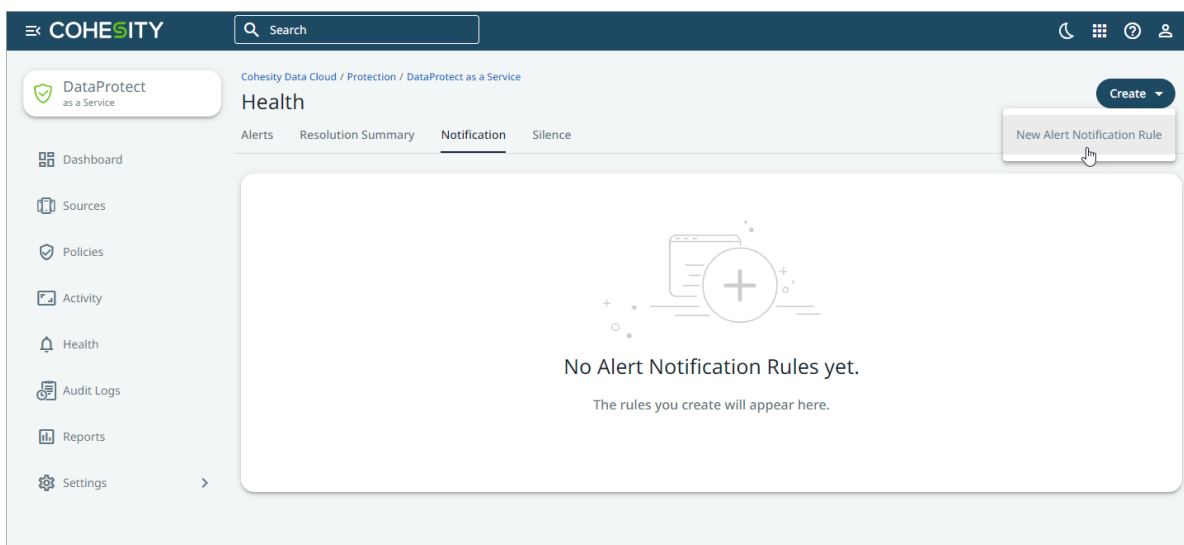
You can configure general alert notification rules from the **Health** page in the **Notification** tab. You can configure email and webhook as the notification output for the alert notification.

### Create Alert Notification Rule for Email Notifications

You can add different alert notification rules that send emails based on the alert categories, severities, and names.

To create an alert notification rule for email notifications:

1. In **DataProtect as a Service**, navigate to the **Health > Notification** tab.
2. Click **Create > New Alert Notification Rule**.



3. In the **Create Alert Notification Rule** dialog, perform the following:
  1. Enter a unique **Notification Name** for the alert notification rule.
  2. In the **Notification Filters** section, select the filter based on your requirements:

**Note:** The alert notification is sent when an alert matches the combination of the filter settings you have configured.

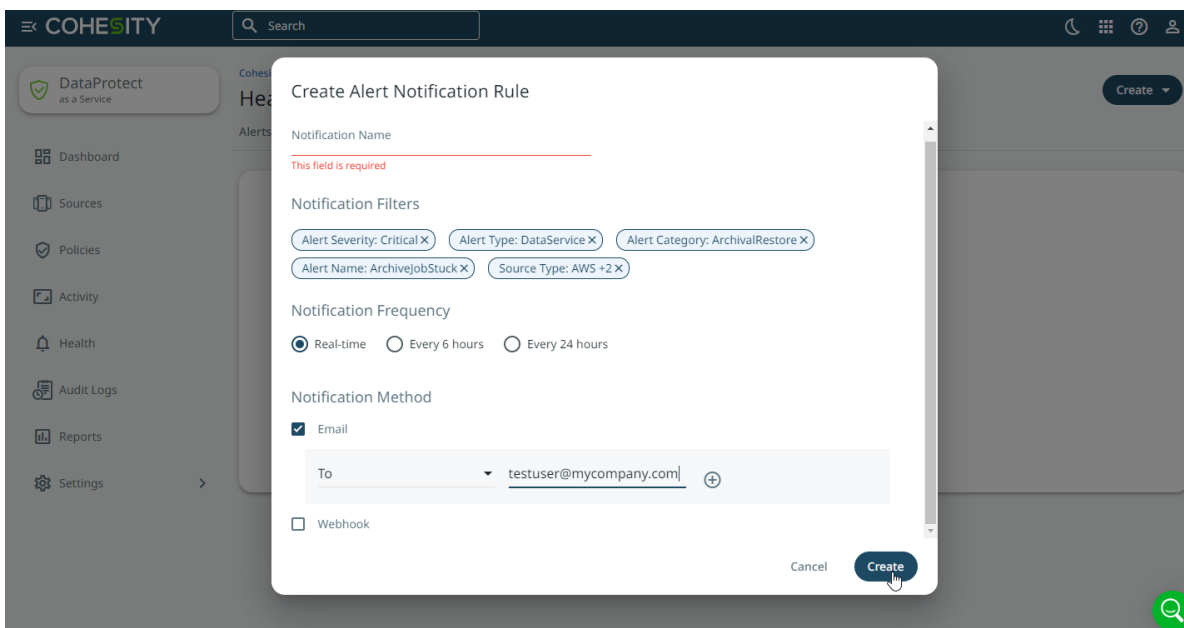
Details	Description
<b>Alert Severity</b>	Select one or more severities from the drop-down. Otherwise, all alerts with any severity will trigger the rule.

Details	Description
<b>Alert Category</b>	Select one or more categories from the drop-down. Otherwise, all alerts in any category will trigger the rule.
<b>Alert Name</b>	Select one or more names from the drop-down. Otherwise, any Alert name will trigger the rule. If you selected any categories, the list includes only alerts in those categories.
<b>Source Type</b>	Select one or more sources from the drop-down. Otherwise, any source will trigger the rule.

3. In the **Notification Method** section, select **Email**. Choose one of the options from the drop-down based on your requirement:

Details	Description
<b>To</b>	Type an email address or distribution list of the recipients to whom you plan to send the email notification.
<b>Cc</b>	Type an email address or distribution list of the recipients to whom you plan to send a copy of the email notification.

Click **+** to add multiple email addresses based on your requirement.



4. Click **Create**.

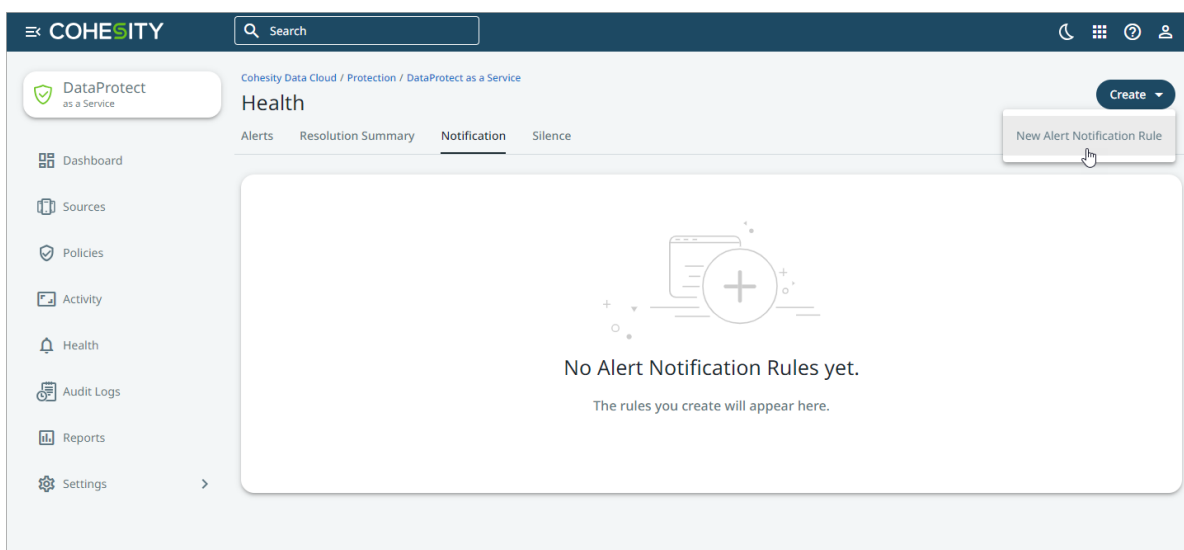
## Create Alert Notification Rule for Webhooks Notification

Webhooks are HTTP callbacks that are usually triggered by some event. Webhooks are configured on one website, and when an event occurs on this website, an HTTP request is made to the configured URL, which invokes an action on the other website.

You can enable webhooks for DataProtect as a Service for Government (FedRAMP) alerts by creating an alert notification rule. When the alert is triggered and meets the criteria in the rule, DataProtect as a Service for Government (FedRAMP) sends an HTTP request to the specified website. Your application can interpret the request. For example, the webhook might notify the website about a critical protection run alert, and your application might open a trouble ticket to track the problem.

To create an alert notification rule for Webhook notifications:

1. In **DataProtect as a Service**, navigate to the **Health > Notification** tab.
2. Click **Create > New Alert Notification Rule**.

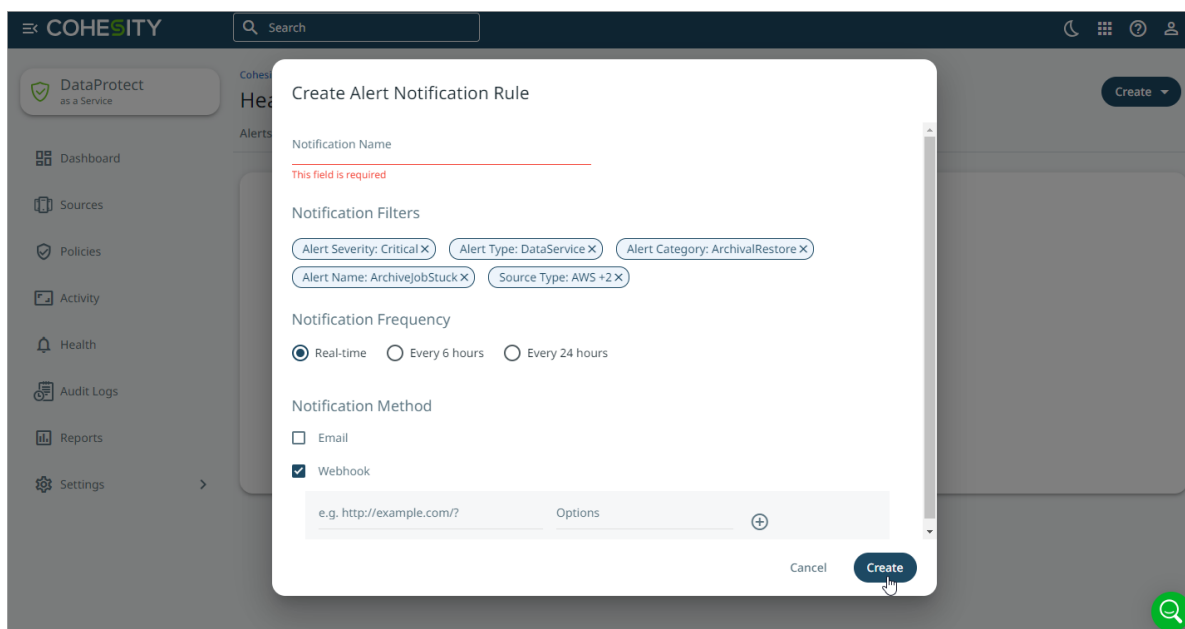


3. In the **Create Alert Notification Rule** dialog, perform the following:
  1. Enter a unique **Notification Name** for the alert notification rule.
  2. In the **Notification Filters** section, select the filter based on your requirements:

**Note:** The alert notification is sent when an alert matches the combination of the filter settings you have configured.

Details	Description
<b>Alert Severity</b>	Select one or more severities from the drop-down. Otherwise, all alerts with any severity will trigger the rule.
<b>Alert Category</b>	Select one or more categories from the drop-down. Otherwise, all alerts in any category will trigger the rule.
<b>Alert Name</b>	Select one or more names from the drop-down. Otherwise, any Alert name will trigger the rule. If you selected any categories, the list includes only alerts in those categories.
<b>Source Type</b>	Select one or more sources from the drop-down. Otherwise, any source will trigger the rule.

- In the **Notification Method** section, select **Webhook**, and provide the URL and cURL options.



- Click **Create**.

#### Alert Request

When an alert is triggered, a sample payload, as shown below, will be available at the configured URL:

#### Request:

```
'https://test-service-now.com/api/x_hesin_cohesity_c/cohesitywebhook'
```

The Payload sent to the above URL:



```

{
  "receiver": "00101000005nBps_test1",
  "status": "firing",
  "alerts": [
    {
      "status": "firing",
      "labels": {
        "account_id": "00101000005nBps",
        "alert_category": "BackupRestore",
        "alert_code": "CE00610005",
        "alert_id": "10534",
        "alert_state": "Open",
        "alert_type_bucket": "DataService",
        "alert_type_id": "10005",
        "alertname": "ProtectedObjectFailed",
        "cluster_id": "1609127048663690",
        "cluster_id_str": "4327092961767844",
        "cluster_name": "DPCluster",
        "failure_reason": "Testing DP alerts raise.",
        "first_occurrence_usecs": "1682699539084721",
        "hidden_from_user": "false",
        "job_id": "18211",
        "job_name": "Test12",
        "job_type": "kOracle",
        "matchedTags": "WorkloadSource_kOracle",
        "object_id": "181",
        "object_name": "obj181",
        "run_id": "182",
        "run_start_time": "2023.02.07 11:21:00 Pacific Time",
        "run_url": "https://test.com",
        "severity": "Critical",
        "tenant_id": "d520840916/",
        "type": "kOracle"
      },
      "annotations": {
        "cause": "Testing DP alerts raise..",
        "description": "Backup of obj181 that is part of protection group Test12
of type kOracle failed with error Testing DP alerts raise",
        "help": "Please refer to KB for details/resolution.",
        "occurrence": "Start at 2023-04-28 16:32:19.084721 +0000 UTC, total 1
time."
      },
      "startsAt": "2023-04-28T16:32:19.084721Z",
      "endsAt": "0001-01-01T00:00:00Z",
    }
  ]
}

```

```

    "generatorURL": "",
    "fingerprint": "bfef9abae71570f0"
  }
],
"groupLabels": {
  "account_id": "00101000005nBps",
  "alertname": "ProtectedObjectFailed",
  "severity": "Critical"
},
"commonLabels": {
  "account_id": "00101000005nBps",
  "alert_category": "BackupRestore",
  "alert_code": "CE00610005",
  "alert_state": "Open",
  "alert_type_bucket": "DataService",
  "alert_type_id": "10005",
  "alertname": "ProtectedObjectFailed",
  "cluster_id": "1609127048663690",
  "cluster_id_str": "4327092961767844",
  "cluster_name": "DPCluster",
  "failed_objects": "obj181",
  "failure_reason": "Testing DP alerts raise.",
  "hidden_from_user": "false",
  "job_id": "18211",
  "job_type": "kOracle",
  "matchedTags": "WorkloadSource_kOracle",
  "run_start_time": "2023.02.07 11:21:00 Pacific Time",
  "run_url": "https://test.com",
  "severity": "Critical",
  "tenant_id": "d520840916/",
  "type": "kOracle"
},
"commonAnnotations": {
  "help": "Please refer to KB for details/resolution."
},
"externalURL": "https://helios-dev3-internal.cohesitycloud.co/alertmanager-d1",
"version": "4",
"groupKey": "{}/{account_id=\"00101000005nBps\",alertname=~\"^(?:ProtectedObjectFailed)$\",hidden_from_user=\"false\",matchedTags=~\"^(?:.*WorkloadSource_kOracle.*)$\",tenant_id=\"d520840916/\"}:{account_id=\"00101000005nBps\", alertname=\"ProtectedObjectFailed\", severity=\"Critical\"}",
"truncatedAlerts": 0

```

}

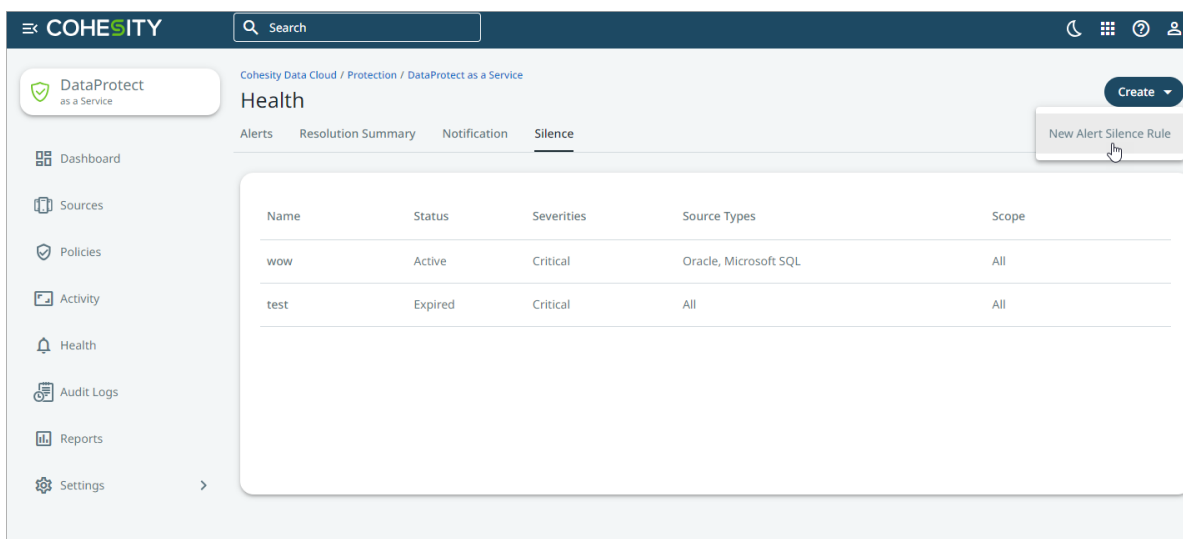
### Silence Alert Notifications

Sometimes, it makes sense to silence alert notifications, such as during maintenance or testing windows.

You can silence alerts that match the rules you define in the Silence tab. Optionally, you can silence alerts for specific periods that you define. Once silenced, alerts are triggered and displayed on the Alerts page, but email or Webhook notifications are not sent.

To create an alert silence rule:

1. In **DataProtect as a Service**, navigate to the **Health > Silence tab**.
2. Click **Create > New Silence Rule**.

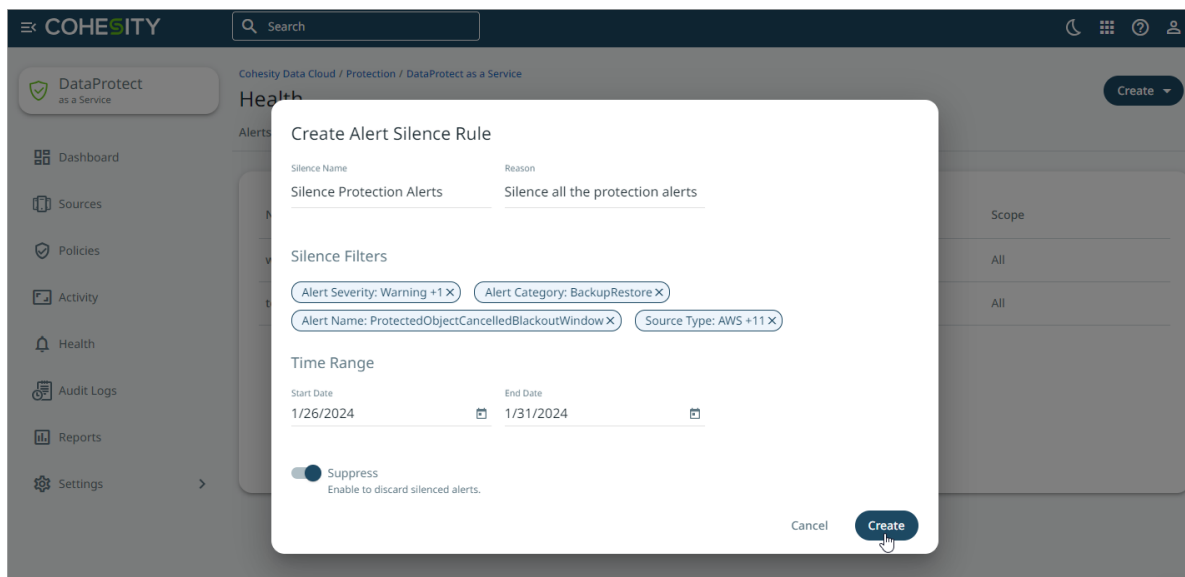


3. In the **Create Alert Silence Rule** dialog, perform the following:
  1. Enter a **Silence Name** for this alert silence rule and provide the **Reason** why you are creating the alert silence rule.
  2. In the **Silence Filters** section, select the filters based on your requirements:

Details	Description
<b>Alert Severity</b>	Select one or more severities from the drop-down you want to silence.
<b>Alert Category</b>	Select one or more categories from the drop-down you want to silence.
<b>Alert Name</b>	Select one or more names from the drop-down you want to silence.

Details	Description
Source Type	Select one or more sources from the drop-down for which you want the alerts silenced.

- In the **Time Range** section, select a date in the **Start Date** and **End Date** fields to set the period within which the alert notifications must be silenced.
- Enable **Suppress** if you do not want the alert to persist and appear on the **Alerts** page.



- Click **Create**.

## Alerts References

This topic provides details on all the alerts triggered by DataProtect as a Service for Government (FedRAMP):

- [Archival and Restore Alerts](#)
- [Backup and Restore Alerts](#)
- [Security Alerts](#)

### Archival and Restore Alerts

This topic covers provides details on all the alerts triggered by DataProtect as a Service for Government (FedRAMP):

CE00820004 ArchiveJobFailed

**Alert Description:** The archive task for a job failed.

**Reason:** This alert is triggered when the archive task of a job fails. This alert is triggered only once per archive task. This alert can be caused by one of the following conditions:

- When an archive task fails due to external target connectivity and/or credentials issues.
- When an archive task fails due to an internal Cohesity issue.

**Action:** Check and fix external target connectivity or credential issues. If the archive task fails after fixing these issues, contact [Cohesity Support](#).

**Severity:** Warning

**Dedup Interval:** 604800 seconds

#### CE00820005 ArchiveJobStuck

**Alert Description:** The archive task for a job is stuck.

**Reason:** This alert is triggered when the archive task of a job is stuck and does not make any progress for more than 3 hours. If the archive task continues to be stuck/queued, this alert is triggered once a week per archive task. This alert can be caused by one of the following conditions:

- When an archive task doesn't make progress due to some external target connectivity and/or credential issues.
- When an archive task doesn't progress due to an internal Cohesity issue.

**Action:** Check and fix the external target connectivity or credential issues.

**Severity:** Warning

**Dedup Interval:** 604800 seconds

#### CE00820008 IceboxDedupCacheFull

**Alert Description:** The Icebox dedup cache is full.

**Reason:** The alert is triggered when the number of archived chunks maintained in the Distributed Key Value Store exceeds the default threshold value. When this happens, the effectiveness of deduplication for the archived data is impacted and could result in transferring more data to the external target.

**Action:** Contact [Cohesity Support](#).

**Severity:** Warning

**Dedup Interval:** 604800 seconds

#### CE00820001 MediaErrorDuringArchival

**Alert Description:** The archival job is waiting to correct an error.

**Reason:** This alert is triggered when no more tapes are available for archiving data.

**Action:** Add new tapes.

**Severity:** Critical

**Dedup Interval:** 604800 seconds

CE00820002 [MediaErrorDuringRestore](#)

**Alert Description:** The restore task is waiting to correct the error.

**Reason:** One or more tapes required to restore data are unavailable. This alert is triggered when the tape required to restore data is unavailable in the tape drive.

**Action:** Insert the required tapes to continue with the restore. The required tapes are listed in the alert.

**Severity:** Critical

**Dedup Interval:** 604800 seconds

CE00820007 [RestoreJobFailed](#)

**Alert Description:** The restore task failed.

**Reason:** This alert is triggered when the restore task of a job fails. This alert is triggered only once per archive task. This alert can be caused by one of the following conditions:

- When a restore task fails due to some external target connectivity and/or credentials issues.
- When a restore task fails due to an internal Cohesity issue.

**Action:** Check and fix external target connectivity or credential issues. If the restore task fails after fixing these issues, contact [Cohesity Support](#).

**Severity:** Warning

**Severity:** 604800 seconds

CE00820006 [RestoreJobStuck](#)

**Alert Description:** The restore task is stuck.

**Reason:** This alert is triggered when the restore task of a job is stuck and does not make any progress for more than one day. If the restore task continues to be stuck/queued, this alert is triggered once a week per Restore task. The alert can be caused by one of the following conditions:

- When a restore task doesn't make progress due to some external target connectivity and/or credentials issues.
- When a restore task doesn't progress due to an internal Cohesity issue.

**Action:** Check and fix external target connectivity or credential issues. If the restore task doesn't progress after fixing these issues, contact [Cohesity Support](#).

**Severity:** Warning

**Dedup Interval:** 604800 seconds

## Backup and Restore Alerts

### CE00608002 MissingVMBBackup

**Alert Description:** Missing VM backup.

**Reason:** This alert is triggered when a descriptor VMDK file has been backed up, but the corresponding flat VMDK file is missing from the backup.

**Action:** No action is required.

**Severity:** Critical

**Dedup Interval:** 3600 seconds

### CE00610016 ObjectBackupSlaViolated

**Alert Description:** The SLA for the backup of an object is violated.

**Reason:** The alert can be triggered when the load on the DataProtect as a Service for Government (FedRAMP) is higher than anticipated, or the primary source is loaded, and the DataProtect as a Service for Government (FedRAMP) cannot back it up fast enough.

**Action:** Verify if a new workload is recently added to the Cohesity cluster or if the primary source is throttling Cohesity APIs/calls.

**Severity:** Warning

### CE00610006 PolicyFieldsDeprecated

**Alert Description:** The policy settings in a policy have been deprecated

**Reason:** The alert is raised after the Cohesity cluster is upgraded from a 4.x release to a 5.x release and the cluster detects that some policy settings used in the current policies on the cluster have been deprecated.

**Action:** Open the listed policy in the Cohesity Dashboard, verify the current settings, and make any necessary adjustments. See the [ALERT: CE00610006 POLICYFIELDSDEPRECATED](#) KB article.

**Severity:** Warning

**Dedup Interval:** 86400 seconds

### CE00610005 ProtectedObjectFailed

**Alert Description:** The backup of an object that is part of a protection run failed with an error.

**Reason:** The alert is raised when the Cohesity cluster detects that an object (such as a VM) failed to be backed up during a Protection Run. One alert is raised for each object (such as a VM) that failed to be backed up. For instructions on how to enable this alert, contact [Cohesity Support](#). A protection run can fail to back up an object for the following reasons:

- There is an issue with the primary environment, such as a removed VM or a Snapshot failure.
- The primary storage is full. (The primary storage contains the objects backed up by the Cohesity cluster.)
- The Cohesity Agent is unreachable while attempting to back up physical servers.

**Action:** See the [CE00610005 | BackupRestore - BackupObjectFailed](#) KB article for a resolution.

**Severity:** Critical

**Dedup Interval:** 86400 seconds

#### CE00610009 ProtectedObjectSLaViolated

**Alert Description:** The service level agreement violation (SLA) of an object in the protection run was violated.

**Reason:** The alert is triggered when the service level agreement violation (SLA) occurs for an individual object in a Protection run. A Protection run may take longer than the specified SLA for the following reasons:

- If the primary storage is slow.
- The network is slow.
- You specified SLA that is too short.

**Action:** Investigate why the Protection run took longer than the specified SLA. If appropriate, adjust the time period specified in the SLA.

**Severity:** Warning

**Dedup Interval:** 86400 seconds

#### CE00608003 VMCrackingSkipped

**Alert Description:** The VM contents are not indexed.

**Reason:** The alert is triggered when the DataProtect as a Service for Government (FedRAMP) detects 5 consecutive unsuccessful attempts to index a VM. The alert can be caused by the following conditions:

- The DataProtect as a Service for Government (FedRAMP) is not able to mount the VMDK.
- The VM Snapshot has an issue.

**Action:** No action is required.

**Severity:** Warning

**Dedup Interval:** 3600 seconds



**CE00610014 VMMigrationIdentified**

**Alert Description:** The VM(s) present in the vCenter have been identified to be migrated from other VCenter(s).

**Reason:** The alert is triggered when the DataProtect as a Service for Government (FedRAMP) identifies a VM in a vCenter that was earlier part of another vCenter registered on DataProtect as a Service for Government (FedRAMP).

**Action:** No action is required if the migrated VMs are mentioned in the alert. If not, contact [Cohesity Support](#).

**Severity:** Critical

**Dedup Interval:** 86400 seconds

**CE00610021 ProtectionPolicyModified**

**Alert Description:** The Protection Policy was modified by a user.

**Reason:** This alert is triggered when a Protection Policy is modified. The modification might include any changes apart from DataLock-related changes in the policy.

**Action:** No action is required.

**Severity:** Informational

**Dedup Interval:** 86400 seconds

**CE00610019 PolicyDataLockChanged**

**Alert Description:** Datalock settings were changed in the Protection Policy.

**Reason:** This alert is triggered if you enable or disable DataLock for a Protection Policy.

**Action:** No action is required. Using this alert, you can validate if the DataLock was enabled or disabled by a valid user.

**Severity:** Informational

**Dedup Interval:** 86400 seconds

**CE00610020 PolicyDataLockDurationChanged**

**Alert Description:** Datalock retention for the Protection Policy was changed.

**Reason:** This alert is triggered when you change the DataLock duration for a Protection Policy.

**Action:** No action is required. Using this alert, you can validate if a valid user modified the DataLock configuration.

**Severity:** Informational

**Dedup Interval:** 86400 seconds

**CE00610017 ProtectionPolicyDeleted**

**Alert Description:** A Protection Policy was deleted.

**Reason:** This alert is triggered when you delete a Protection Policy.

**Action:** No action is required. Using this alert, you can validate if a valid user deleted the Protection Policy.

**Severity:** Warning

**Dedup Interval:** 86400 seconds

#### CE00610023 ProtectionRunModified

**Alert Description:** A protection run was modified.

**Reason:** This alert is triggered when a Protection run is modified. The modification might include deleting a Protection run, enabling a legal hold, etc.

**Action:** No action is required.

**Severity:** Informational

**Dedup Interval:** 86400 seconds

#### CE00610027 ObjectDeletionRejected

**Alert Description:** A protection run was modified.

**Reason:** This alert is triggered when the user deletes a specific snapshot for an object instead of deleting the entire view. The deletion is rejected because the view is marked immutable, and therefore individual object deletion can not be performed.

**Action:** Evaluate if the user can delete the entire view instead of individual snapshots.

**Severity:** Warning

**Dedup Interval:** 3600 seconds

## Security Alerts

#### CE01516011 DataIngestAnomalyAlert

**Alert Description:** Anomalous change in data ingests detected on your Source, which might be a symptom of a potential ransomware attack on your primary environment.

**Reason:** This alert is triggered when an anomalous change in the data ingest rate for a protected Source is detected and is only generated if the cluster is registered with DataProtect as a Service for Government (FedRAMP). The change might be a symptom of a ransomware attack on your primary environment.

**Action:** Consider restoring the Source from a Snapshot. This alert provides a link to begin an Instant Recovery using the latest clean Snapshot. For more information on detecting anomalies and ransomware attacks, see [Detect Anomalies](#) and [Detect Ransomware Attacks](#).

**Severity:** Warning

**Dedup Interval:** 3600 seconds

## Audit Logs

The **Audit Logs** page records the events that occur in DataProtect as a Service for Government (FedRAMP). The events are:

- Read or write actions performed by the users on DataProtect as a Service for Government (FedRAMP).
- Login and logout actions performed by the Helios users.

## View Audit Logs

On the **Audit Logs** page in DataProtect as a Service for Government (FedRAMP), you can find the following details for the events that are logged by the registered regions:

- Date
- Time
- User & action
- System (DataProtect as a Service for Government (FedRAMP) region)

**Note:** By default, only the write actions performed by the users on Cohesity clusters are displayed on the **Audit Logs** page. To see read actions, select **Read Actions** from the **Actions** filter and click **Apply**. See [Use Filters to Locate Specific Logs](#) next.

## Use Filters to Locate Specific Logs

Use the following filters to narrow the listed audit logs and locate the specific logs.

Filter	Purpose
Date Range	Filter the audit logs based on the selected time window.
System	Filter the audit logs based on the DataProtect as a Service for Government (FedRAMP) regions.
Users	View the audit trails of specific users.
Category	Filter the audit logs based on predefined categories. See <a href="#">Review Audit Log Categories</a> next.
Action	Filter the audit logs based on the read or write actions performed by the users in the registered regions. See <a href="#">Logged Actions</a> below

## Review Audit Log Categories

Audit logs are logged under predefined categories for you to find the relevant audit logs and analyze the correct logs quickly.

- API Key
- Access Token
- Alert
- Alert Notification Rule
- Group
- Helios Event
- IDP Configuration
- Protection Group
- Protection Policy
- Recovery Task
- Region
- Resolution
- Snapshot
- SNMP Config
- Source
- Tenant
- User

## Logged Actions

Along with the read actions, the following write actions are logged:

Write Actions	Descriptions
Accept	A user accepted the license agreement.
Activate	A user activated an entity such as Protection Run.
Add	A user added a Region.
Apply	A user applied a setting or configuration.
Assign	A user assigns a source to a tenant.

Write Actions	Descriptions
Cancel	A user canceled an entity such as a running Protection run or a Recovery task.
Clone	A user cloned an entity such as a Snapshot, VM, or SQL Database.
Close	A user closed an SMB file.
Cloud Spin	A user deployed a VM on the cloud.
Cluster Expand	A user expanded the cluster.
Create	A user created an entity such as a Protection run.
Deactivate	A user deactivated a Protection run.
Delete	A user deleted an entity such as a Protection run, or Protection Policy.
Disjoin	A user disjoined the Cluster from an AD domain.
Download	A user downloaded a VMX file or a file from a VM Snapshot.
Import	A user performed a generic action for any import operations. For example, the user has imported patch binary.
Install	A user performed a generic action for any installation. For example, the user has installed an app.
Join	A user joined the Cluster to an AD domain.
Login	A user logged in to the DataProtect as a Service for Government (FedRAMP).
Logout	A user logged out of the DataProtect as a Service for Government (FedRAMP).
Mark	A user marked an entity for removal such as a disk.
Modify	A user modified an entity such as a User, Protection run, or Remote Cluster.
Notification Rule	A user modified the notification rule.
Overwrite	A user performed an overwrite operation.

Write Actions	Descriptions
Pause	A user paused an entity such as a running Protection run.
Recover	A user recovered an entity such as a VM, file, or SQL Database.
Refresh	A user performed a refresh of the entities in the DataProtect as a Service for Government (FedRAMP). For example, the user refreshed the source configuration.
Register	A user registered an entity such as an External Target (Vault).
Mark Removal	A user marked an entity for removal. For example, the user marked a disk for removal.
Rename	A user renamed an entity.
Restart	A user restarted a service.
Resume	A user performed a resume action on a Protection run.
Revert	A user reverted a setting or action.
Run Diagnostics	A user ran a diagnostics. For example, the user ran diagnostics on the agent to collect logs and other metrics.
Run Now	A user performed a Run Now action on a Protection run.
Schedule	A user scheduled an event.
Schedule Report	A user scheduled an email report.
Search	A user searched for a term.
Start	A user started a service.
Stop	A user stopped a service.
Unassign	A user removes a source from a tenant.
Uninstall	A user uninstalled an app.
Unregister	A user unregistered an entity such as a Source.


Write Actions	Descriptions
Update	A user updated an entity in a Cohesity cluster.
Upgrade	A user upgraded the Cohesity cluster.
Upload	A user uploaded an entity.
Validate	A user validated an entity.

## Set Log Retention Period for Cluster Audit Logs

You can set the retention period for cluster audit logs. When you set a retention period, the logs are retained on the cluster until the retention period ends.

**Note:** The default retention period is 180 days.

To set a retention period for cluster audit logs, follow the steps below:

1. In **DataProtect as a Service**, navigate to **Security > Audit Logs > Settings**.
2. In the **Settings** tab, click the edit icon for **Log Retention Period**.
3. Enter the desired number and choose a type of retention period (Days, Weeks, Months, or Years).
4. Select the  icon to save.

A push notification with the message **Settings Updated** is displayed.


Cohesity converts weeks, months, or years into days and displays it as the **Log Retention Period**.

## Download Audit Logs

You can download the Audit Logs in CSV format from DataProtect as a Service for Government (FedRAMP) for analysis and sharing.

**Note:** The downloaded .CSV file contains more details than what the Helios Dashboard displays. For example, the file contains details about the IP addresses of the systems from which the cluster is accessed, tenants, impersonation, and so on.

To download audit logs:

1. In **DataProtect as a Service**, navigate to **Audit Logs**.
2. In the top right, click the **Download**  icon.

The audit logs CSV file is downloaded.



# How-To Videos

Use these [videos](#) to learn some of the key tasks you'll be performing in Cohesity DataProtect as a Service in detail.

# Cohesity Support

## Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to [Cohesity Support](#), to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the [Cohesity Support Portal](#) to create a new case.
- Click the (?) icon on the Cohesity UI and select Support Portal.

## Creating a customer support case for Cohesity Cloud Services (CCS)

When creating a customer support case for Cohesity Cloud Services (CCS), follow the steps listed below:

1. Mention CCS in the subject and select **CCS** as the **Issue Type**.
2. Provide the case information.
3. Edit the **Case Subject** as per you cloud region. For example, for AWS region, **CCS (AWS\_Region): <Input Issue Subject Information>**.
4. Update the **Issue Type** field to **CCS**.

Additionally, provide the **Cluster ID** and the **Support Token** information if a SaaS connector is involved.

## Support/Service Assistance

First contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing or technical support related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit [Cohesity Knowledge Base](#).
- Log in to the [Cohesity Support Portal](#) to create a new case.
- To monitor your open cases, log in to the portal, click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

## Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

**Note:** Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

