

Version 1.1

Jan 2022

# Protect OneDrive for Business with Cohesity

*Reduce Complexity with Seamless Data Protection  
for OneDrive for Business*

## **ABSTRACT**

*As organizations transition to Microsoft OneDrive for Business for business-critical collaboration, they realize the need for a data protection solution for their Microsoft 365 domain. Cohesity delivers features and capabilities that organizations can leverage to protect their OneDrive for business data, ensuring business continuity while meeting compliance and regulatory requirements.*

# Table of Contents

Introduction to Data Protection for OneDrive for Business .....	4
Features and Benefits of Cohesity Data Protection for OneDrive for Business .....	4
Cohesity's Backup Solution for OneDrive for Business.....	5
How Cohesity Protects OneDrive for Business .....	7
Full Backup Workflow .....	7
Incremental Backup Workflow .....	7
Set Up Data Protection for OneDrive for Business .....	9
Prerequisites .....	9
<i>Select a Microsoft 365 User Account .....</i>	<i>9</i>
<i>Register an App on Azure Active Directory .....</i>	<i>9</i>
Register Microsoft 365 as Source in Cohesity .....	16
Create a Protection Policy .....	18
Create a Protection Group .....	18
OneDrive For Business Data Recovery .....	19
OneDrive for Business Restore Workflows on Cohesity .....	19
<i>OneDrive for Business Drive Recovery Workflow .....</i>	<i>19</i>
<i>OneDrive for Business Files and Folders Recovery Workflow.....</i>	<i>20</i>
Recover OneDrive for Business.....	20
<i>Select the Recovery Source .....</i>	<i>21</i>
<i>Select the Restore Granularity .....</i>	<i>21</i>
<i>Select the Restore Destination .....</i>	<i>23</i>
Best Practices .....	26
Maintain Business Continuity with Disaster Recovery .....	27
Replicate Backups to Other Cohesity Clusters .....	27
Conclusion.....	28
Your Feedback .....	29
About the Author .....	29
Document Version History.....	29

## Figures

Figure 1: Protect Your OneDrive for Business with Cohesity .....	6
Figure 2: Cohesity Full Backup Workflow for OneDrive for Business .....	7
Figure 3: Cohesity Incremental Backup Workflow for OneDrive for Business .....	8
Figure 4: Cohesity Drive-level Restore Workflow for OneDrive for Business .....	19
Figure 5: Cohesity File- and Folder-level Restore Workflow for OneDrive for Business	20
Figure 6: Replicate Backups to Other Cohesity Clusters.....	27

## Tables

Table 1: Features and Benefits of Using Cohesity to Protect OneDrive for Business .....	5
---	---

## Introduction to Data Protection for OneDrive for Business

Growing adoption of Microsoft 365®, Microsoft's business productivity tools suite delivered in a SaaS (Software as a Service) model (including Exchange Online, OneDrive™ for Business, SharePoint Online, and more), has sparked fresh conversations on the division of responsibilities between Microsoft, now a *service provider*, and the organization that owns the data that is created and managed in Microsoft 365. Before SaaS models, data protection was the responsibility of the organization, as both the data and the infrastructure to manage it was owned by the organization, and typically resided on-premises with the organization.

However, with the introduction of SaaS like Microsoft 365, where the infrastructure is distributed, data protection is now a shared responsibility between customers, who create and use the data in cloud-based applications, and providers, who run the infrastructure for those applications.

As the SaaS provider, Microsoft protects your data in the event of:

- Application failures
- Infrastructure failures
- Disaster scenarios

However, you, the customer, are responsible for protecting the data from a series of other threats:

- Accidental data deletion
- Insider attack
- Security breaches
- Synchronization errors
- Administrative errors

Cohesity protects your data from all these threats.

## Features and Benefits of Cohesity Data Protection for OneDrive for Business

Starting with version 6.5, Cohesity adds data protection for OneDrive for Business to its support for the Microsoft 365 suite. This extends the benefits users can derive from Cohesity, many of which are the product of Cohesity's modern, web-scale architecture.

Although most organizations begin their journeys to overcoming mass data fragmentation by simplifying data protection, Cohesity's flexible architecture allows easy expansion to additional use cases, further increasing operational simplicity and improved total cost of ownership (TCO). Cohesity is a software-defined solution that works on-premises (on qualified Cisco, HPE, Dell, or Cohesity C Series platforms), in the public cloud, and at remote and branch offices on hypervisors like VMware and Hyper-V.

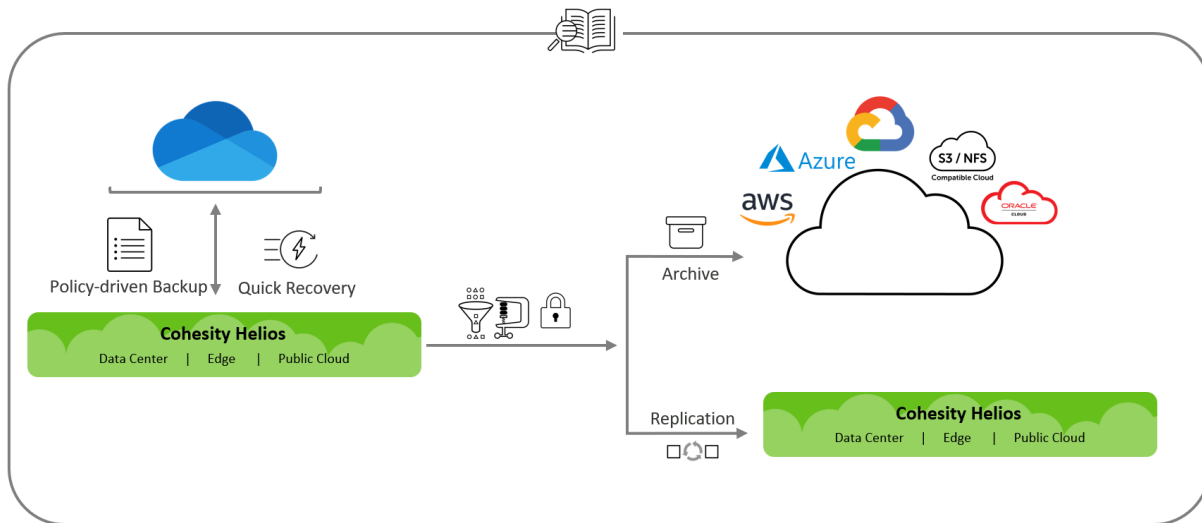
Table 1: Features and Benefits of Using Cohesity to Protect OneDrive for Business

FEATURES	BENEFITS
Scheduled Automated Backups	Automated scheduled backups
Browse and Restore	Ability to browse and restore OneDrive for Business data.
Search and Restore	Ability to search and restore OneDrive for Business data. * <i>Version 6.5 and higher</i>
Granular Recovery	While you can restore a full OneDrive for Business backup, you can also restore data at various levels granularity, down to individual folders and files.
Flexible Deployment Options	You can deploy Cohesity on-premises or in the cloud, giving you full flexibility in planning deployments.
Cross-Domain Data Recovery	If there are multiple M365 domains registered as a source to the same Cohesity cluster, you can restore data across those domains.
DataLock and Legal Hold	Cohesity Platform's DataLock and Legal Hold features help you meet regulatory compliance.
Forever Incremental	Cohesity's approach of taking a full backup once followed by forever incremental backups helps organizations meet the backup SLAs, as the daily data transfers are limited to just the changed data.
Global Deduplication	Global deduplication produces significant space savings across different workloads.
Auto Protect	When enabled, the Auto Protect feature automatically protects any new user who is added to the domain.
Data Migration across Microsoft 365 Domains	Use Cohesity <a href="#">to migrate data from one Microsoft 365 domain to another</a> .
Self-service Recovery	Using role-based access controls (RBAC), administrators can enable end users to recover their lost files and folders themselves.

## Cohesity's Backup Solution for OneDrive for Business

Microsoft 365 is a SaaS service. Cohesity interacts with M365 using [Graph APIs](#). Once you provide the M365 username, password app ID, and app secret, you can configure M365 as a source on the Cohesity cluster and back up your OneDrive for Business data.

Figure 1: Protect Your OneDrive for Business with Cohesity



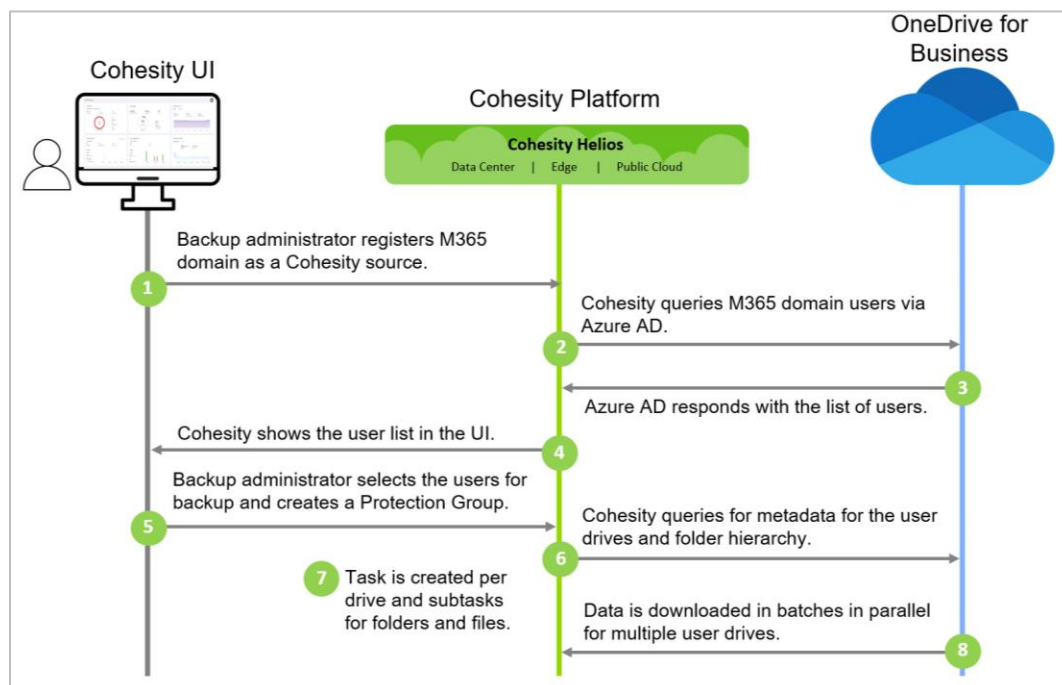
## How Cohesity Protects OneDrive for Business

Cohesity provides a straightforward sequence of tasks that constitute the procedure for backing up your OneDrive for Business data. Once the Microsoft 365 domain that includes your OneDrive for Business is registered as a source in Cohesity Platform, you can start configuring backups. Cohesity starts with a full backup, followed by a forever-incremental approach.

### Full Backup Workflow

The first step to OneDrive data protection is to take a full backup of the OneDrive for Business drives by adding them to a Cohesity Protection Group. When a Protection Run initiates, the metadata is downloaded first. Once the metadata is backed up, a task is created for each OneDrive for Business drive and subtasks are created to backup files and folders under the drive. The data is downloaded in parallel batches for multiple drives and indexed in parallel.

Figure 2: Cohesity Full Backup Workflow for OneDrive for Business



### Incremental Backup Workflow

After the first full backup is complete, the Protection Group continues to run at the interval you specify, performing an incremental backup to capture all data that has changed.

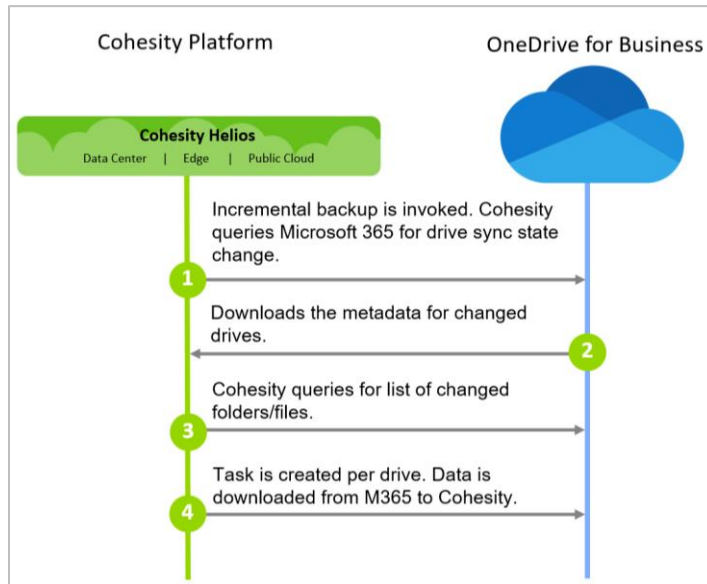
In the process of creating an incremental backup of your OneDrive for Business data, Cohesity performs several tasks in the following sequence:

1. The incremental backups are either scheduled in a [Cohesity Protection Policy](#) or triggered manually by an administrator.

2. Cohesity queries OneDrive for Business for the sync state. If the current sync state is different from the previous state, it means there are changes to the OneDrive.
3. Cohesity queries the M365 domain to retrieve the list of changed folders in each OneDrive.
4. A backup task is created for each OneDrive that has changed files and folders since the last backup. These files and folders are backed up and indexed in batches.

When the incremental backup run completes, it shows a Run Status of Success in the Protection Group's page.

Figure 3: Cohesity Incremental Backup Workflow for OneDrive for Business



## Set Up Data Protection for OneDrive for Business

Configuring and managing your OneDrive for Business backups from Microsoft 365 is a straightforward, two-step process in Cohesity Platform. First, you need to register Microsoft 365 as a Cohesity Platform source and then follow the wizard to create a Protection Policy and Protection Group for the backup. You can configure the backup schedule in the Protection Policy, or you can manually invoke a Protection Run.

To configure backups for the OneDrive for Business service in M365, confirm you have [met the prerequisites](#) and:

1. Register the M365 domain as a source in Cohesity Platform.
2. [Create a Protection Policy](#).
3. [Create a Protection Group](#).

### Prerequisites

Before you begin, ensure that you have:

- [Microsoft 365 user credentials](#). The user account used to authenticate with and backup data from Microsoft 365.
- [Registered an app in Azure AD](#) and captured:
  - **App ID**. The identifier for the app service that is registered in Azure Active Directory.
  - **Access Key**. The key corresponding to the app service.

### Select a Microsoft 365 User Account

In order to interact with and back up your OneDrive for Business data from Microsoft 365, Cohesity needs to be able to log in to your M365 domain with the primary SMTP address of a M365 user account that has global administrator privileges. The user must be a global administrator.

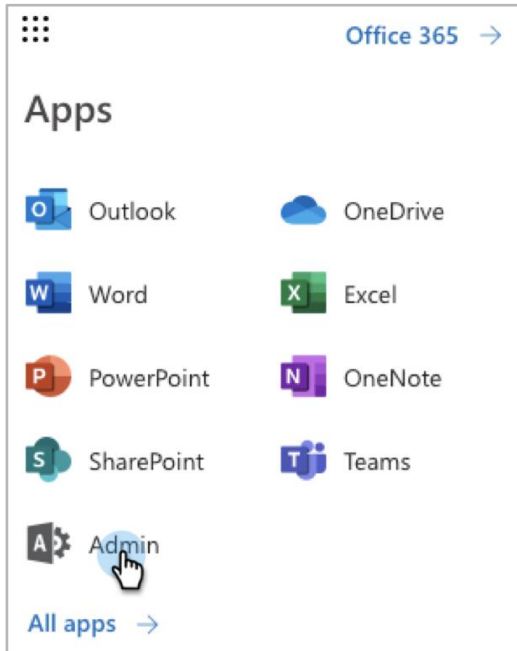
### Register an App on Azure Active Directory

For OneDrive for Business, Cohesity uses the [Microsoft Graph API](#) to connect with Microsoft 365. This requires that you register an app on Azure Active Directory and capture the App ID and Access Key to register Microsoft 365 with Cohesity. Also you need to add Graph API permissions to the designated app.

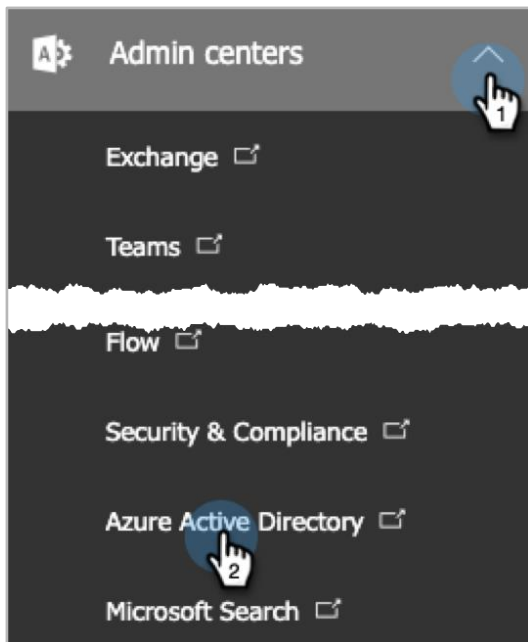
**NOTE:** If you already have an Azure AD App being used for Exchange Online, you only need to add permissions to the same app for OneDrive for Business backups. You can proceed directly to add [application permissions](#).

To register an app on Azure Active Directory:

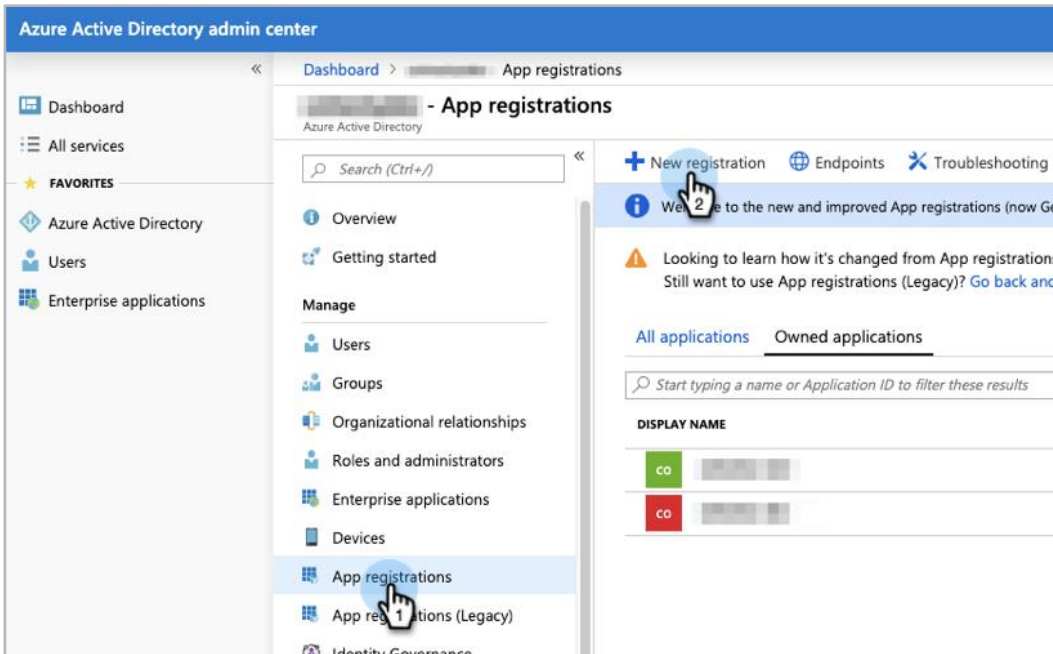
1. Log in to the Azure Portal (<https://portal.azure.com>) with your Microsoft 365 administrator user credentials. In the main menu on the left, click **Admin**.



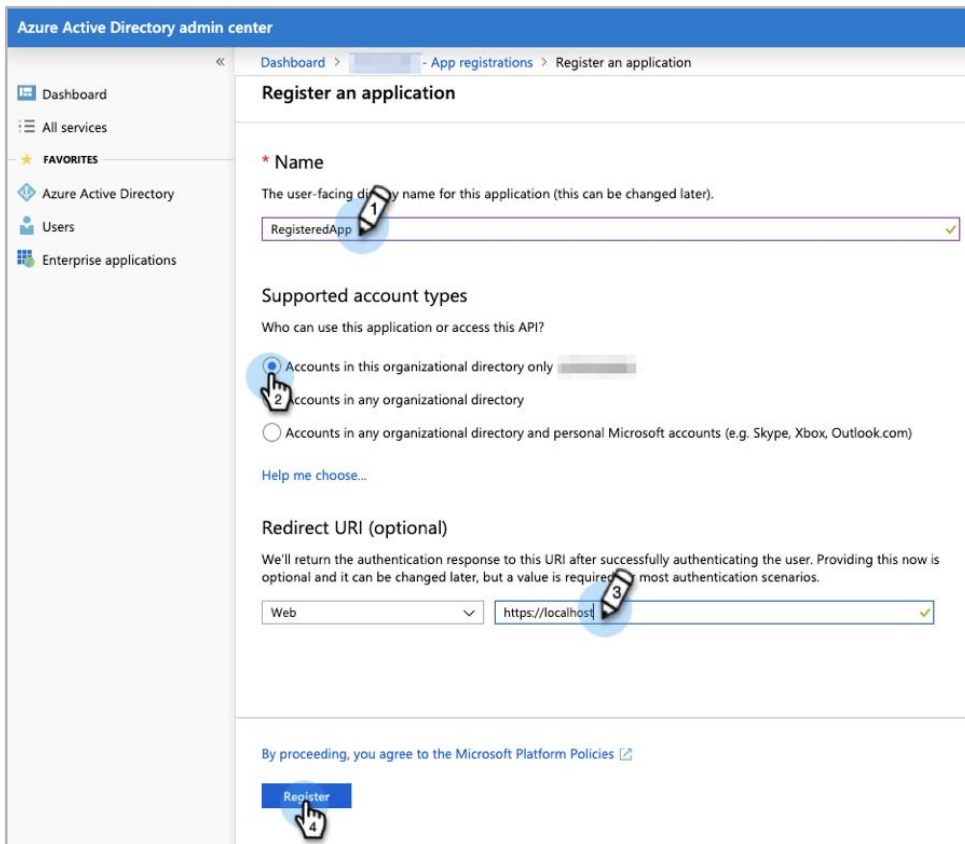
2. In the Microsoft Admin Center, select **Admin centers > Azure Active Directory**.



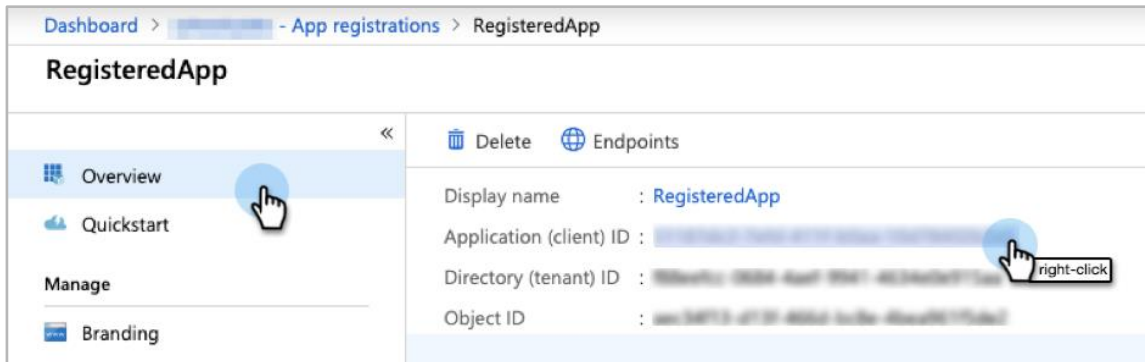
3. Select **App registrations > New registration**.



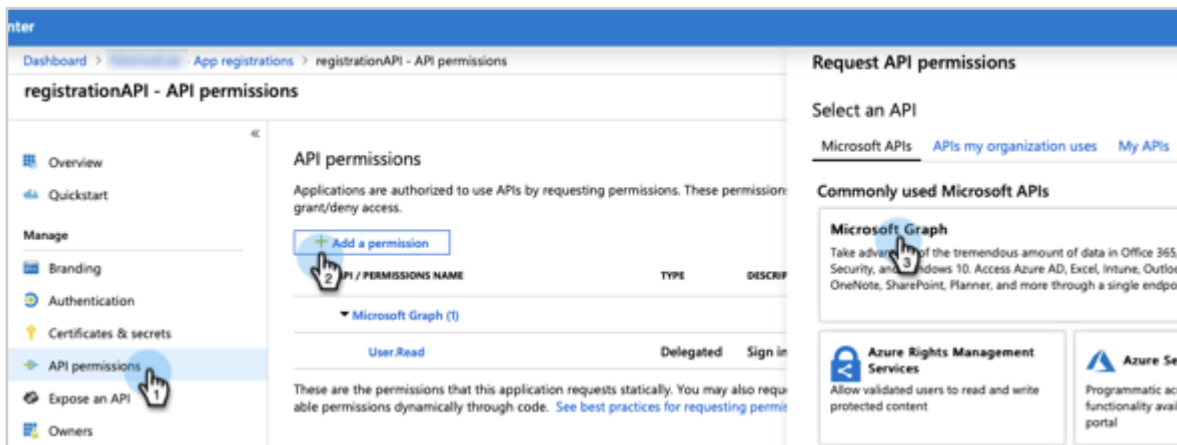
4. Enter a **Name** for your app, select the **Supported account types** that can access the app, and enter **https://localhost** as the **Redirect URI**. Then click **Register**.



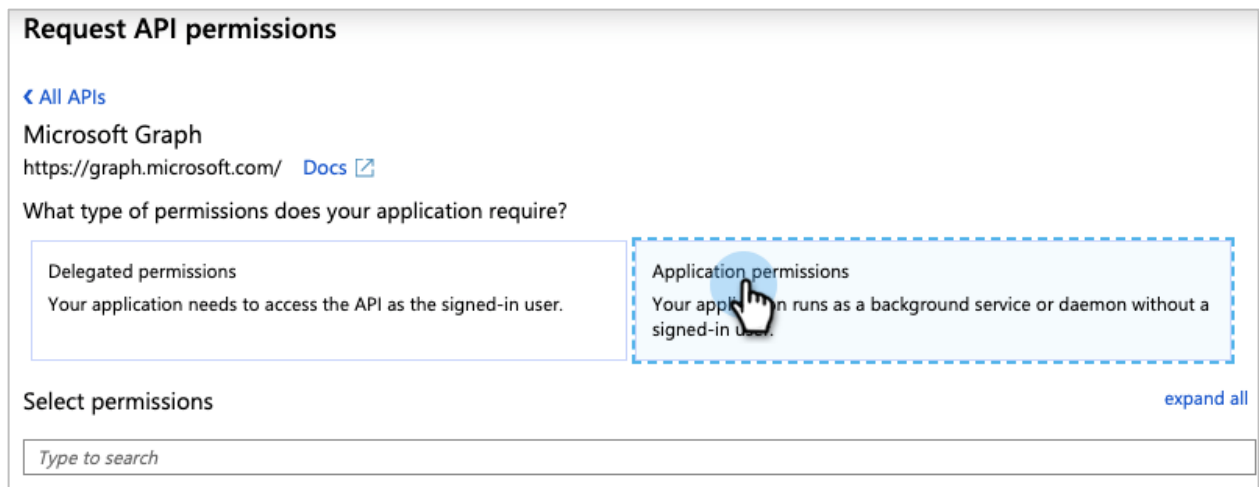
- On the RegisteredApp page, click **Overview** and copy the **Application (client) ID**. You will use this to register Microsoft 365 as a source on Cohesity Platform.



- On the same page, select **API permissions > Add a permission > Microsoft Graph API**.



- Click **Application permissions**.

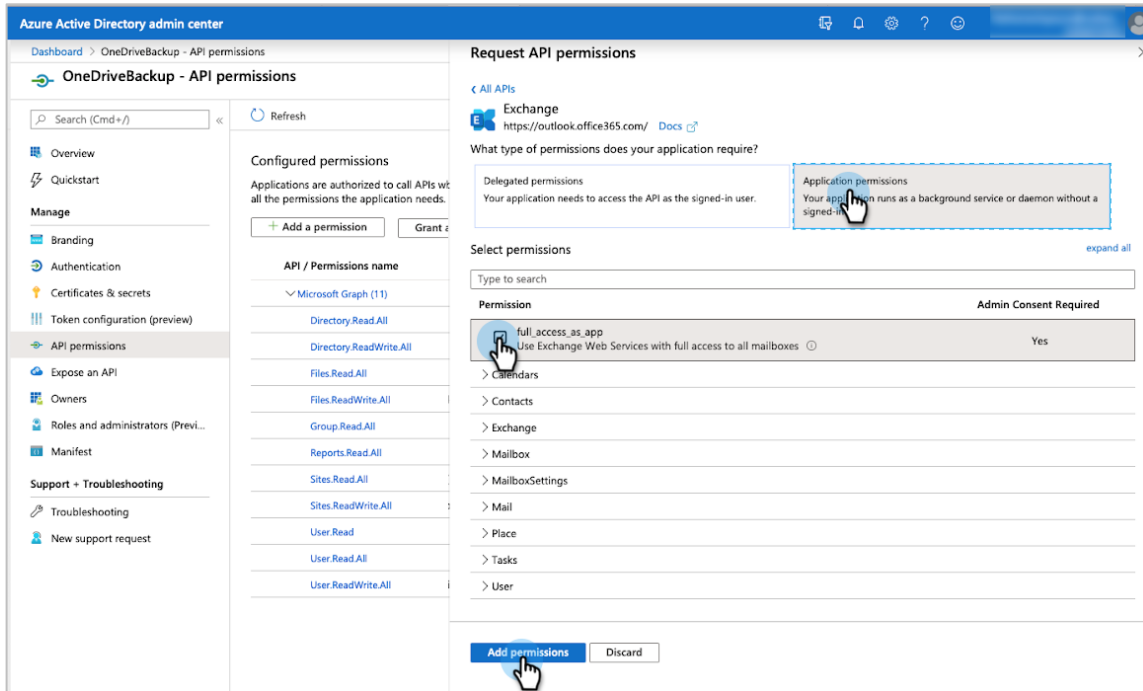


8. Click **Add permissions** and then:
  - Click **Directory** and select **Directory.Read.All** and **Directory.ReadWrite.All**.
  - Click **Files** and select **Files.Read.All** and **Files.ReadWrite.All**.
  - Click **Group** and select **Group.Read.All** and **Group.ReadWrite.All**.
  - Click **Reports** and select **Reports.Read.All**.
  - Click **Sites** and select **Sites.Read.All** and **Sites.ReadWrite.All**.
  - Click **User** and select **User.Read.All** and **User.ReadWrite.All**.
9. (Optional) Microsoft Graph is the de facto integration API for [OneDrive for Business](#), and leverages OAuth by default. However, if you plan to enable OAuth for Exchange Online Backups while [registering Microsoft 365 as a Cohesity source](#), you must add the following Exchange API permission to this app.

On the same page, select **API permissions > Add a permission > Exchange**. (If not, you can skip these two steps and proceed to [granting consent for your domain](#).)

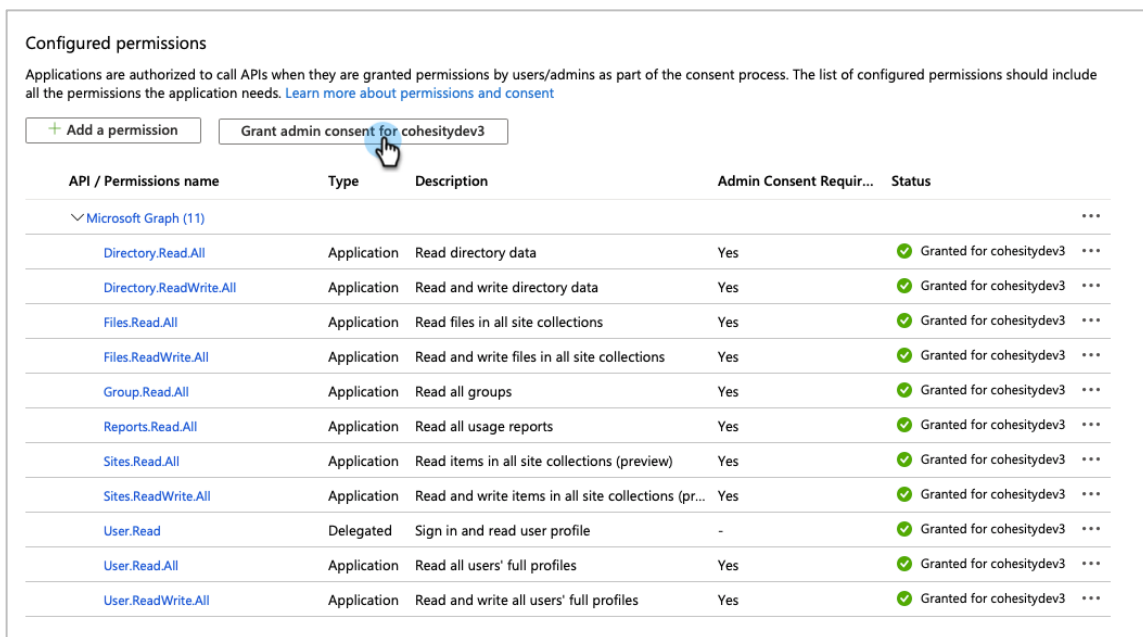
The screenshot shows the Azure Active Directory admin center interface. The main content area is titled 'Request API permissions' for the application 'OneDriveBackup - API permissions'. It features a search bar, a refresh button, and a list of 'Configured permissions' under the 'Microsoft Graph (11)' category. The permissions listed are: Directory.Read.All, Directory.ReadWrite.All, Files.Read.All, Files.ReadWrite.All, Group.Read.All, Reports.Read.All, Sites.Read.All, Sites.ReadWrite.All, User.Read, User.Read.All, and User.ReadWrite.All. A blue circle highlights the '+ Add a permission' button. To the right, there are sections for 'Request API permissions' (with a description of accessing resources in the Yammer web interface), 'More Microsoft APIs' (listing Azure Batch, Azure Data Catalog, Azure Data Explorer (with Multifactor Authentication), Azure Data Lake, and Speech), and 'Supported legacy APIs' (listing Azure Active Directory Graph and Exchange). The Exchange API is highlighted with a blue circle and a hand cursor.

10. Click **Application permissions**, select **full\_access\_as\_app**, and click **Add permissions**.



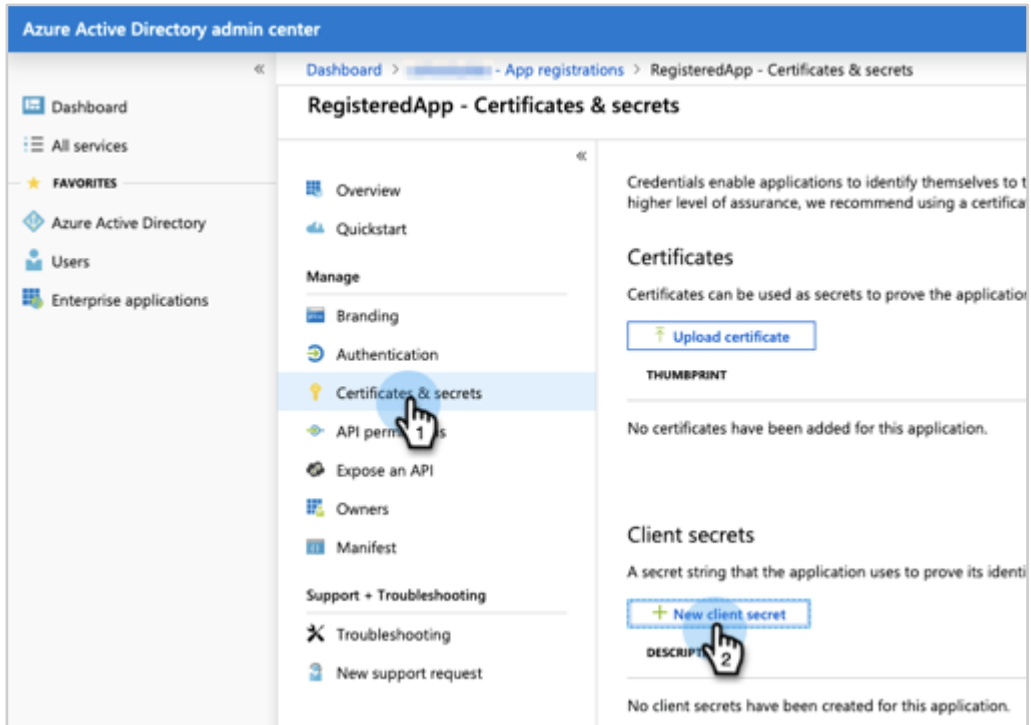
**NOTE:** You will also need to enable OAuth when you [register M365 as a Cohesity source](#) or by updating an existing M365 source in Cohesity. After this, you can use OAuth for your Microsoft 365 backup and restore operations.

11. Under **Grant Consent**, click **Grant admin consent for <domain\_name>**.

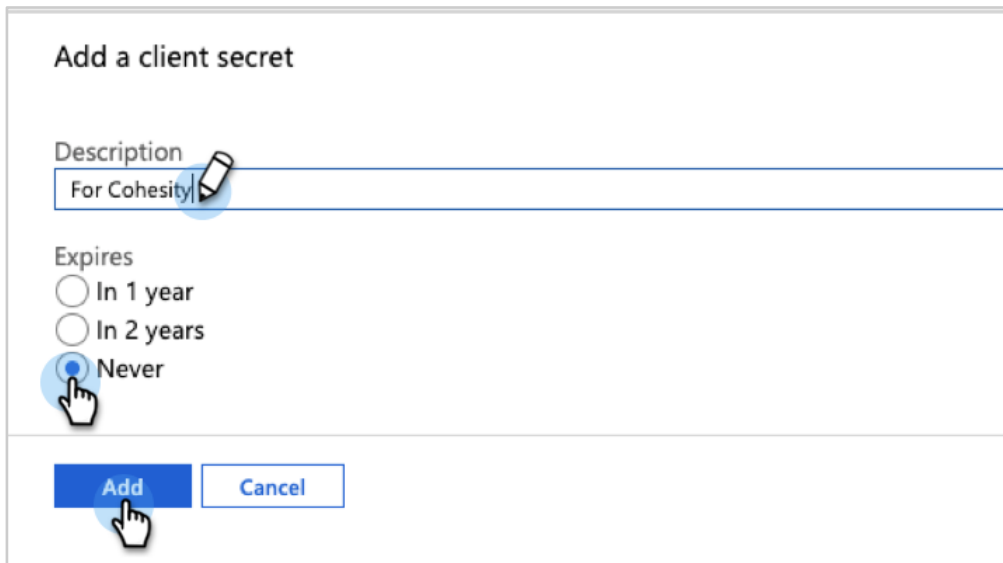


12. Under **App Registration**, click the application name that you entered previously.

13. Next, you need to add a new client secret (or “App Secret Key”) that the app can use to prove its identity when requesting a token. Click **Certificates & secrets > New client secret**.



14. Enter a **Description**, select **Never** under **Expires**, and click **Add**.



15. Under **Client secrets**, click the **Copy** button next to the string under **VALUE**.

**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
For Cohesity	31/12/2299	[REDACTED]

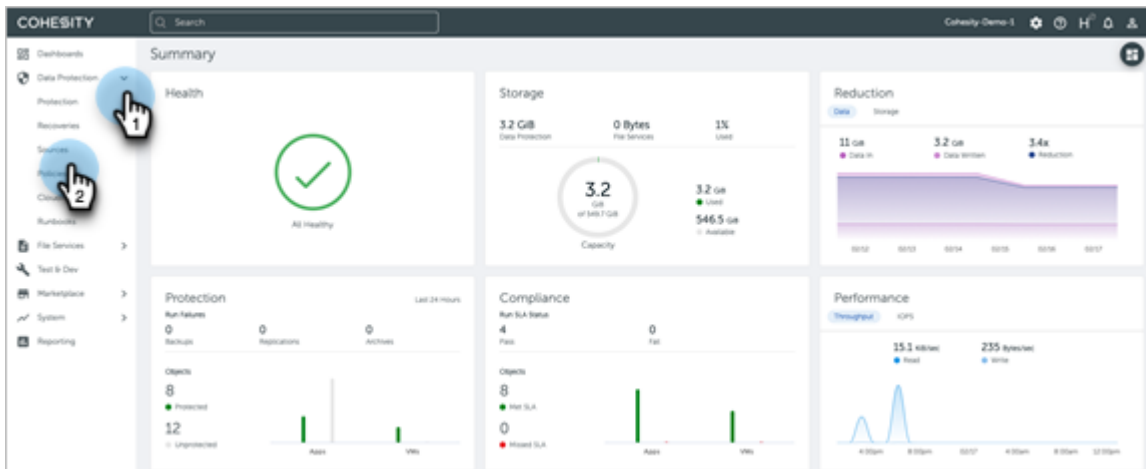
**NOTE:** Save this value in a safe location. You will use it to [register Microsoft 365 as a source in Cohesity](#).

## Register Microsoft 365 as Source in Cohesity

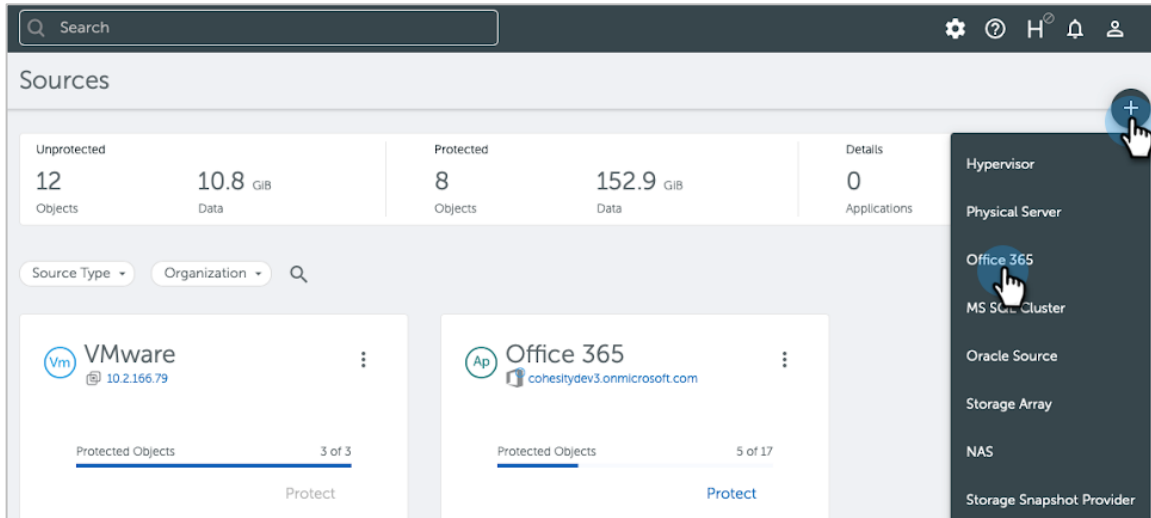
To configure any data source for data protection in Cohesity Platform, you need to register it as a source. The same applies to Microsoft 365.

To add your Microsoft 365 domain as a source:

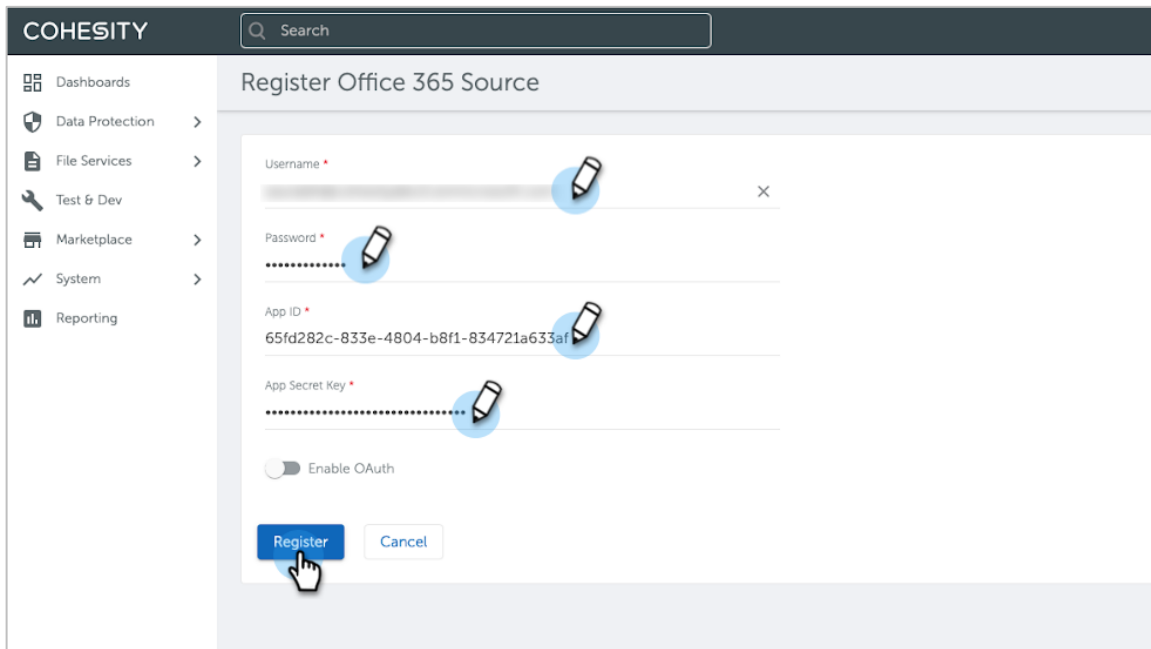
1. Log in to Cohesity Platform.
2. Select **Data Protection > Sources**.



3. Click **Add** button and select **Microsoft 365**.



4. Enter the Microsoft 365 **Username**, **Password**, **App ID**, and **App Secret Key** that you captured earlier, when [creating the Azure Active Directory app](#). Finally, click **Register**.



**NOTE:** To enable OAuth, first add [the Exchange API permission](#) to your [Azure Active Directory app](#) registered above, then click **Enable OAuth** here *before* you click **Register**.

## Create a Protection Policy

In Cohesity, Protection Groups use Protection Policies. Protection Policies reflect business needs, such as backup and archival frequency, retention requirements for each, as well as Recovery Point Objectives (RPOs), while a Protection Group defines operational requirements, such as which source objects to protect, the Protection Policy to use, and operational considerations like indexing, exclusions and inclusions, alerts, app consistency, and more. This process of combining business needs (Policy) with the objects to protect (source data) and the operational requirements (Group) provides rich flexibility to customers.

See [Create or Edit a Standard Policy](#) in the online Help.

See Cohesity's recommendations for protecting Microsoft 365 data in [5 Best Practices](#) below.

## Create a Protection Group

Protection Groups combine operational requirements—such as which objects to protect, indexing, etc. with the business requirements that are defined in a [Protection Policy](#). Multiple Protection Groups can use the same Protection Policy, but each Protection Group can have only one policy.

See [Add or Edit a Protection Group for Microsoft 365](#) in the online Help.

## OneDrive For Business Data Recovery

Restoring data for OneDrive for Business using Cohesity is simple and intuitive. You can restore your data at various levels of granularity: entire drives or specific files and folders. And you can restore both in-place (to original location), to an alternate location, and across Microsoft 365 domains.

### OneDrive for Business Restore Workflows on Cohesity

The workflow for restoring drives is a little different from the workflow for restoring files and folders.

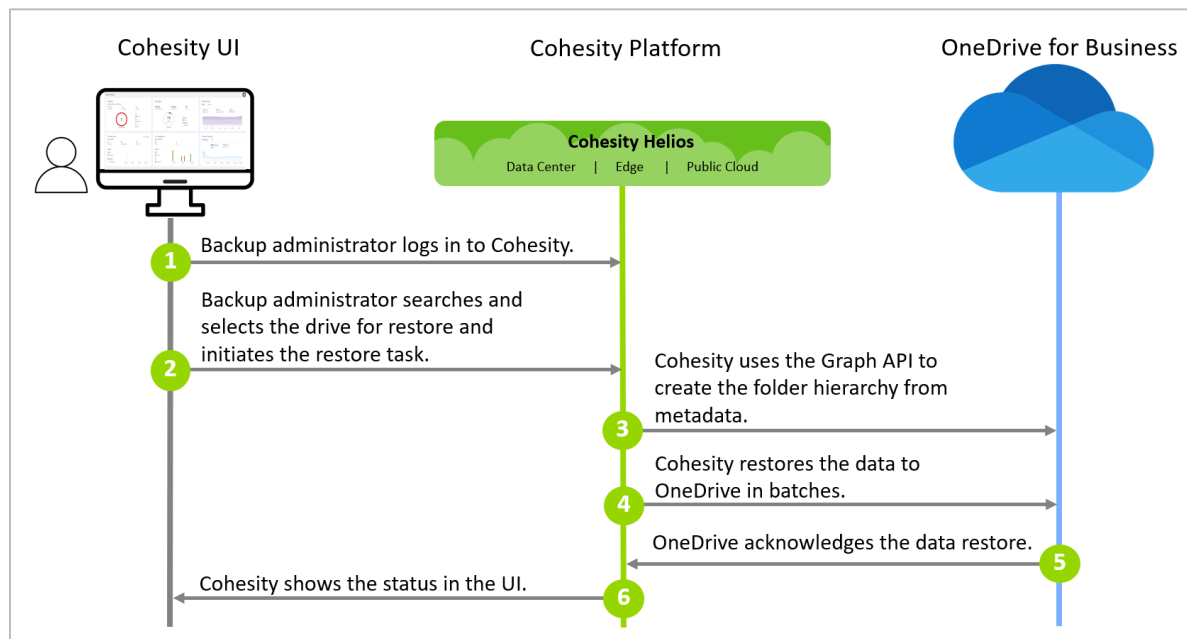
#### OneDrive for Business Drive Recovery Workflow

To start a OneDrive restore, the administrator searches through the backups by username or Protection Group name for the OneDrive that needs to be restored and then launches the restore operation.

At that point, Cohesity DataProtect:

1. Recreates the folder hierarchy from metadata in the backup.
2. Searches the internal metadata to locate the data blocks.
3. Collates the data and sends the data to OneDrive for Business using Microsoft Graph APIs.

Figure 4: Cohesity Drive-level Restore Workflow for OneDrive for Business



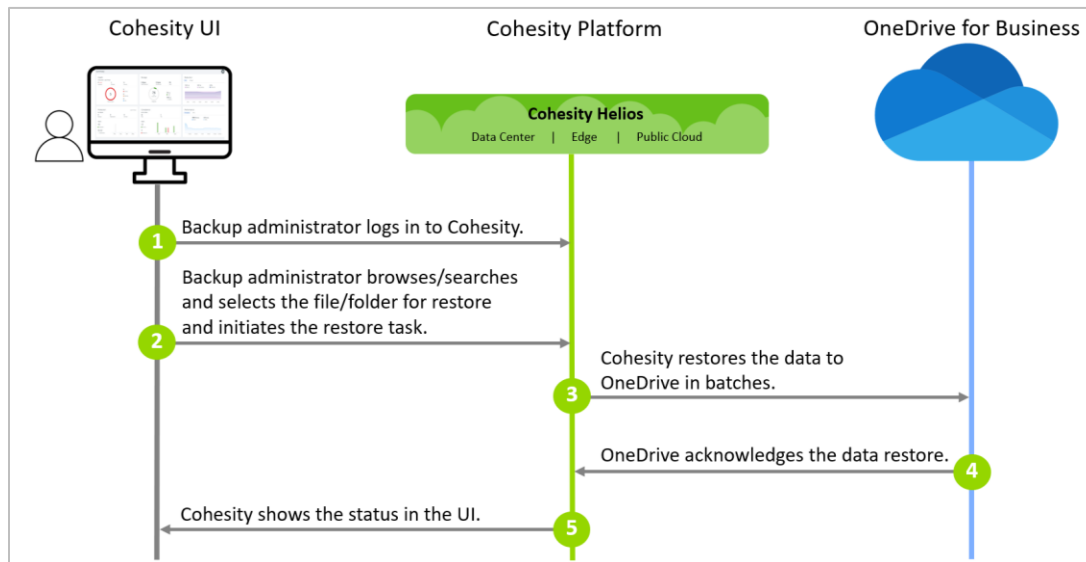
## OneDrive for Business Files and Folders Recovery Workflow

To start a files/folders restore, the administrator browses through the backups using the OneDrive username. The administrator then selects the files and folders that need to be restored and launches the restore operation.

At that point, Cohesity DataProtect:

1. Searches through the internal metadata to locate the data blocks containing the requested data.
2. Collates the data and uses Microsoft Graph APIs to restore it to OneDrive for Business.

Figure 5: Cohesity File- and Folder-level Restore Workflow for OneDrive for Business



## Recover OneDrive for Business

To restore your OneDrive for Business data:

1. Select the [recovery source](#).
2. Select the [restore granularity](#).
3. Select the [restore destination](#).

## Select the Recovery Source

In Cohesity Platform, navigate to **Data Protection > Recoveries**, then click the **Add** button and select **Microsoft 365** as the recovery source.

The screenshot shows the Cohesity Recoveries page. The left sidebar contains navigation options: Dashboards, Data Protection, Protection, Recoveries (highlighted), Sources, Policies, CloudRetrieve, Runbooks, File Services, Test & Dev, Marketplace, System, and Reporting. The main content area displays a summary of recovery jobs: 88 Succeeded, 0 Warning, 43 Failed, 0 Running, and 5 Canceled. Below this is a table of recovery jobs with columns for Name, Organization, Start Time, and Status. A dropdown menu is open on the right, showing various recovery sources: Files or Folders, VMs, Physical Server, MS SQL, Oracle, Migrate Database (MS SQL Only), Instant Volume Mount, Virtual Disks, Storage Volume, Office 365 (highlighted), and Active Directory.

Name	Organization	Start Time	Status
Recover-Office365_Apr_6_2020_11-02am	-	Apr 6, 2020 11:02am	Success
Recover-Office365_Apr_6_2020_10-59am	-	Apr 6, 2020 10:59am	Success
Recover-Office365_Apr_4_2020_2-01am	-	Apr 4, 2020 2:01am	Success
Recover-Office365_Apr_3_2020_8-12pm	-	Apr 3, 2020 8:12pm	Success

## Select the Restore Granularity

You can restore OneDrive for Business data at different granularities. You can restore an entire OneDrive for Business drive or specific files and folders.

### Recover a OneDrive

To recover an entire OneDrive for Business drive:

1. In the **Recover Microsoft 365** form, select **OneDrives > OneDrives**.
2. Use the username or Protection Group name to search the backups, select the user's OneDrive that you need to restore, and click **Continue**.
3. Select the [restore destination](#) (below).

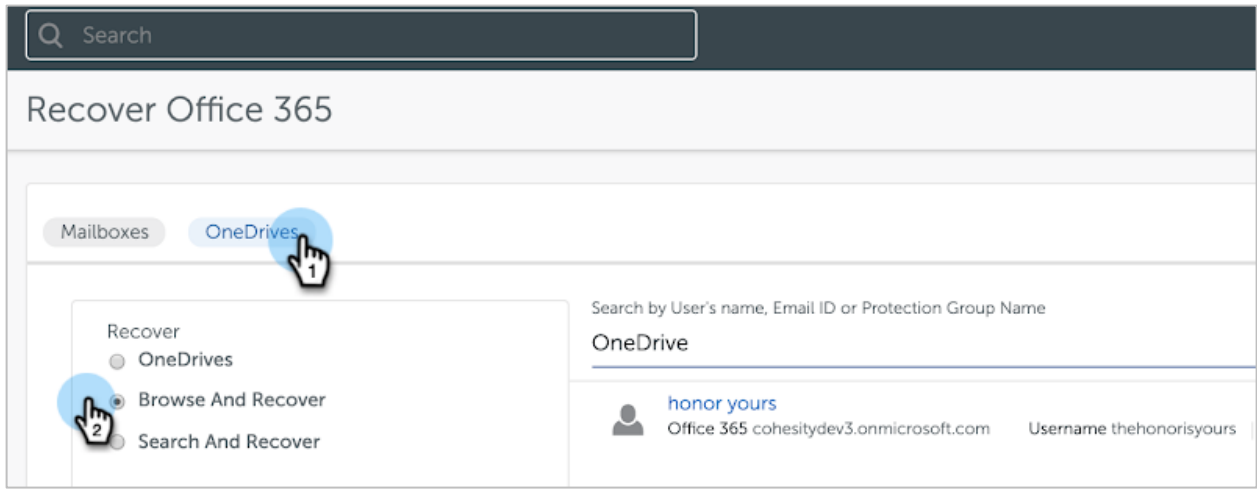
### Recover Files and Folders

You can recover specific files and folders using one of two approaches:

- **Browse and Restore.** You can browse the individual user's OneDrive to navigate and select the files and folders to be restored.
- **Search and Restore.** You can use global search to find the files and folders that need to be restored.

To browse and recover:

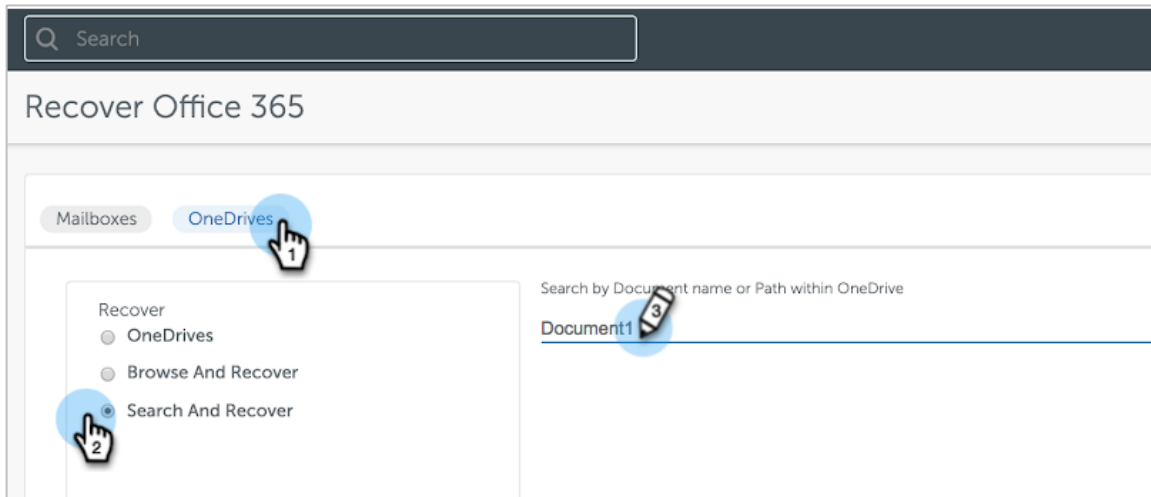
1. In the **Recover Microsoft 365** form, select **OneDrives > Browser And Recover**.



2. Search for the username and click it to browse the drive for the user.
3. Select the file or folder you want to restore. Click to **Add to Cart**.
4. Click **Save** to continue to restore. Alternatively, choose **Save and Continue** to select multiple files.
5. Click **Continue** to [select the restore destination](#).

To search and recover:

1. In the **Recover Microsoft 365** form, select **OneDrives > Search and Recover** and enter part or all of the file or folder name you need to recover.



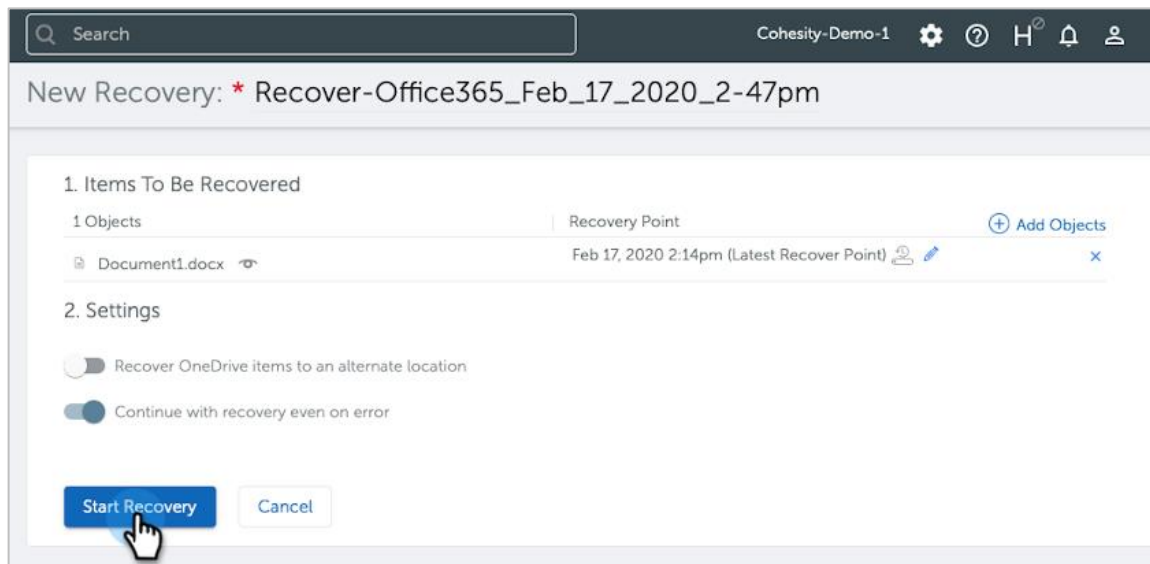
2. Select the file or folder and click **Continue** to [select the restore destination](#).

## Select the Restore Destination

There are two restore destinations that an administrator can select while performing a restore: to the same OneDrive or to a different OneDrive, in the same or a different M365 domain.

To choose a restore destination on the same OneDrive, select one of the following:

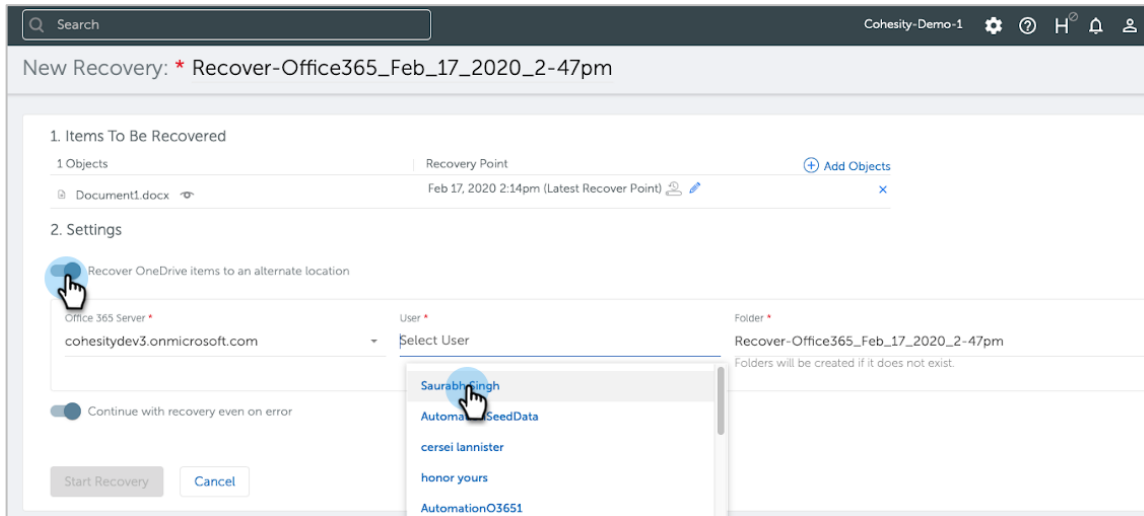
- **Recover to the same drive (default).** Data is restored to the same OneDrive from which it was backed up. Click **Start Recovery** to trigger the recovery.



**NOTE:** If the file or folder already exists, it is restored as a new version of the file. The older file can be accessed in the file's version history.

- **Recover to an alternate folder on the same OneDrive.** Data is restored to the same drive from which it was backed up but in an alternate folder.

To restore to an *alternate folder within the same OneDrive*, select **Restore OneDrive items to an alternate location** and choose the same user's OneDrive as the source user's OneDrive. You can keep the default folder name or provide a folder name to which the file should be restored.

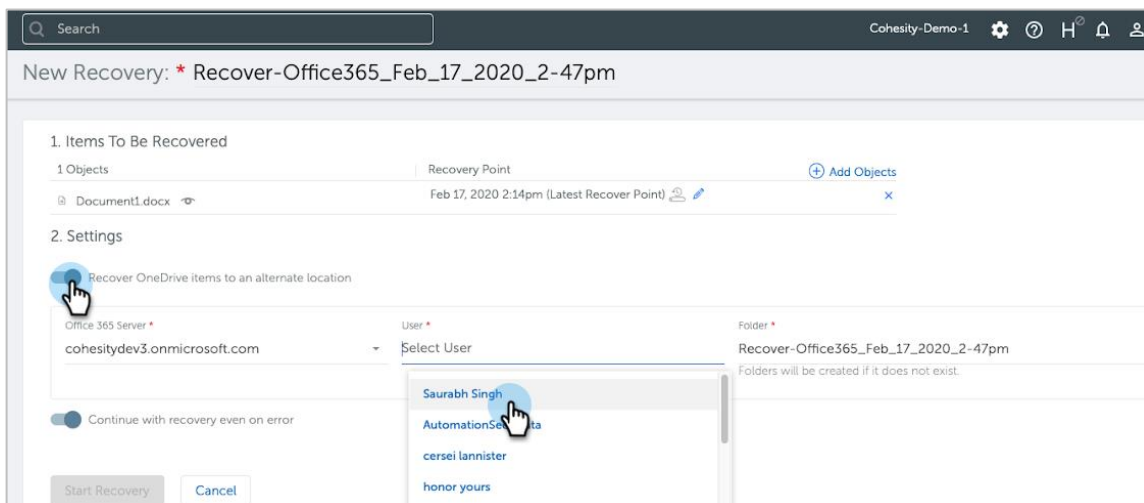


Click **Start Recovery** to launch the restore operation.

To choose a restore destination on a different OneDrive, select one of the following:

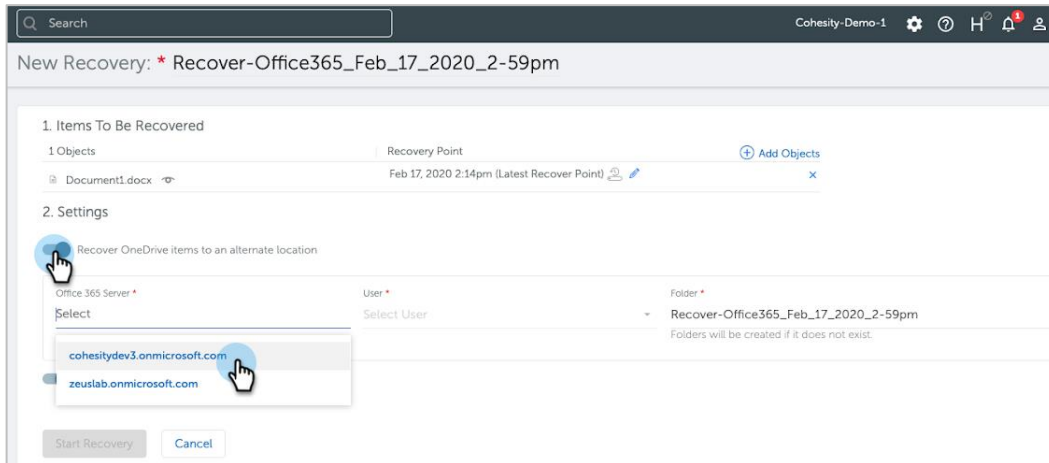
- **Recover to an alternate location in the same M365 domain.** Data is restored to a different user's OneDrive in the same Microsoft 365 domain.

To restore to an alternate location in the same M365 domain, select **Restore OneDrive items to an alternate location** and choose the OneDrive to which data needs to be restored.

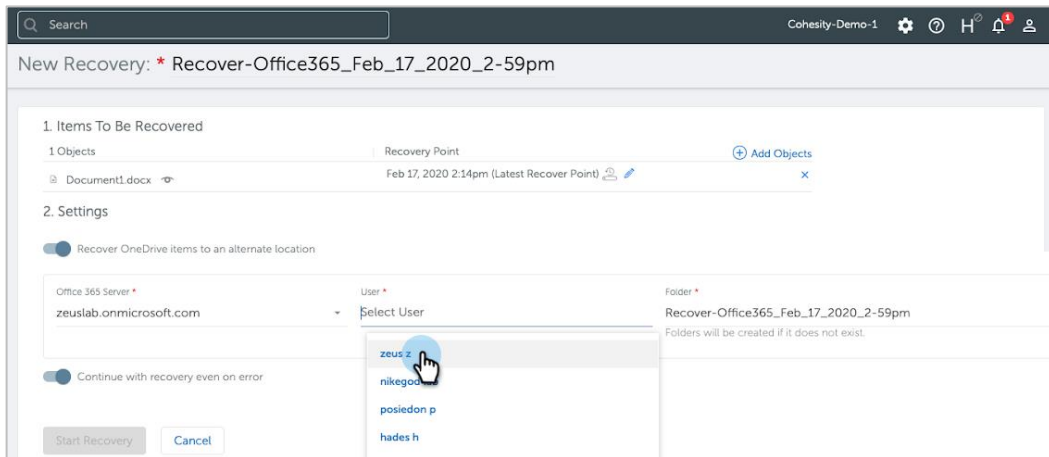


Click **Start Recovery** to launch the restore operation.

- **Recover to an alternate location in a *different* M365 domain.** Data is restored to an alternate location in a different Microsoft 365 domain. Note that to restore to an alternate location in a different M365 domain, both domains must be [registered as sources](#) in the same Cohesity cluster.
1. Select **Restore OneDrive items to an alternate location** and choose the **Microsoft 365 Server** to which data needs to be restored.



2. Select the OneDrive **User** to which the data needs to be restored.



3. Click **Start Recovery** to launch the restore operation.

**NOTE:** You can use this option to migrate data from one Microsoft 365 domain to another.

## Best Practices

For best results using Cohesity to protect your OneDrive for Business data, Cohesity recommends:

- Set **Retry Options** to **1** in your Cohesity Protection Policy, as the Microsoft 365 connector already includes the retry mechanism that handles failed requests. There is no need to increase this setting in the Protection Policy.
- Use **Auto-Protect** to avoid having to add new users to the Protection Group manually.
- Avoid adding the same users to multiple Protection Groups.
- As of Cohesity version 6.5, Exchange Online and OneDrive for Business backups for the same user cannot be performed in parallel. This will be addressed in future releases.

## Maintain Business Continuity with Disaster Recovery

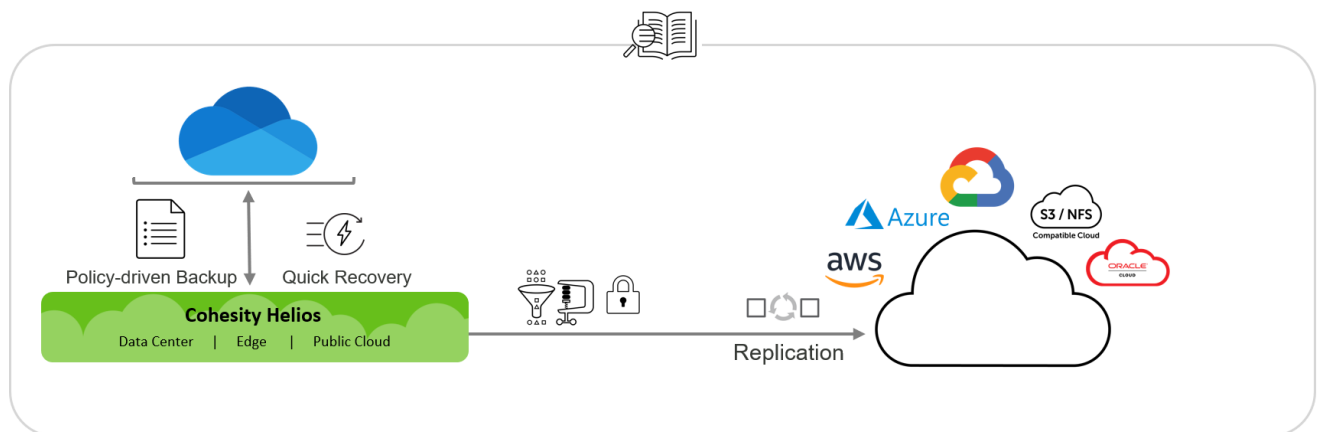
Cohesity provides replication for protecting your data from disruptions and disasters. Replication provides a simple way to store and then get your data back in the event of major business disruptions such as natural disasters and IT failures.

### Replicate Backups to Other Cohesity Clusters

Organizations can take advantage of Cohesity replication for cost-effective disaster recovery (DR). Cohesity provides a policy-based data replication solution from the core to the cloud to the edge, from one cluster to another cluster in your DR site.

As part of replication, Cohesity always performs deduplication and compression first, and sends only the changed data over the network. In the event of the primary site becoming unavailable, application and backup admins can failover to the DR site for backup and recovery of their data.

Figure 6: Replicate Backups to Other Cohesity Clusters



To replicate Microsoft 365 data to another Cohesity cluster:

1. Configure replication to another Cohesity cluster. See [Replication and Remote Access Setup](#) in the online Help.
2. Edit the [Protection Policy that you created for backup](#) and configure the **Replication** settings to meet your requirements. See Step 12 in [Create or Edit a Standard Policy](#) in the online Help.

The replication settings will take effect in the next scheduled Protection Run.

## Conclusion

Cohesity provides a simple and efficient solution for OneDrive for Business data protection. With Cohesity, you can take a “once full and forever incremental” backup, which not only helps you adhere to your backup SLAs, but also provides the ability to restore to multiple points in time. Efficient search and indexing provide the ability to restore protected data quickly. Cohesity’s backup solution for OneDrive for Business helps you take control of your data protection strategy.

## Your Feedback

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

## About the Author

Saurabh Singh is a Product Manager at Cohesity. In his role, Saurabh focuses on product management for Cohesity Data Management as a Service (DMaaS), Security, SaaS Backup, and Secure Multi-tenancy.

## Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.0	April 2020	First release
1.1	Jan 2022	Rebranding Updates

## ABOUT COHESITY

[Cohesity](#) radically simplifies data management. We make it easy to protect, manage, and derive value from data -- across the data center, edge, and cloud. We offer a full suite of services consolidated on one multicloud data platform: backup and recovery, disaster recovery, file and object services, dev/test, and data compliance, security, and analytics -- reducing complexity and eliminating [mass data fragmentation](#). Cohesity can be delivered as a service, self-managed, or provided by a Cohesity-powered partner.

Visit our [website](#) and [blog](#), follow us on [Twitter](#) and [LinkedIn](#) and like us on [Facebook](#).

© 2021. Cohesity, Inc. All Rights Reserved. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at [www.cohesity.com/agreements](http://www.cohesity.com/agreements).

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