COHESITY

Version 3.2

June 2023

Cohesity DataProtect Delivered as a Service Free Trial Guide

Sign Up. Connect. Protect.

Table of Contents

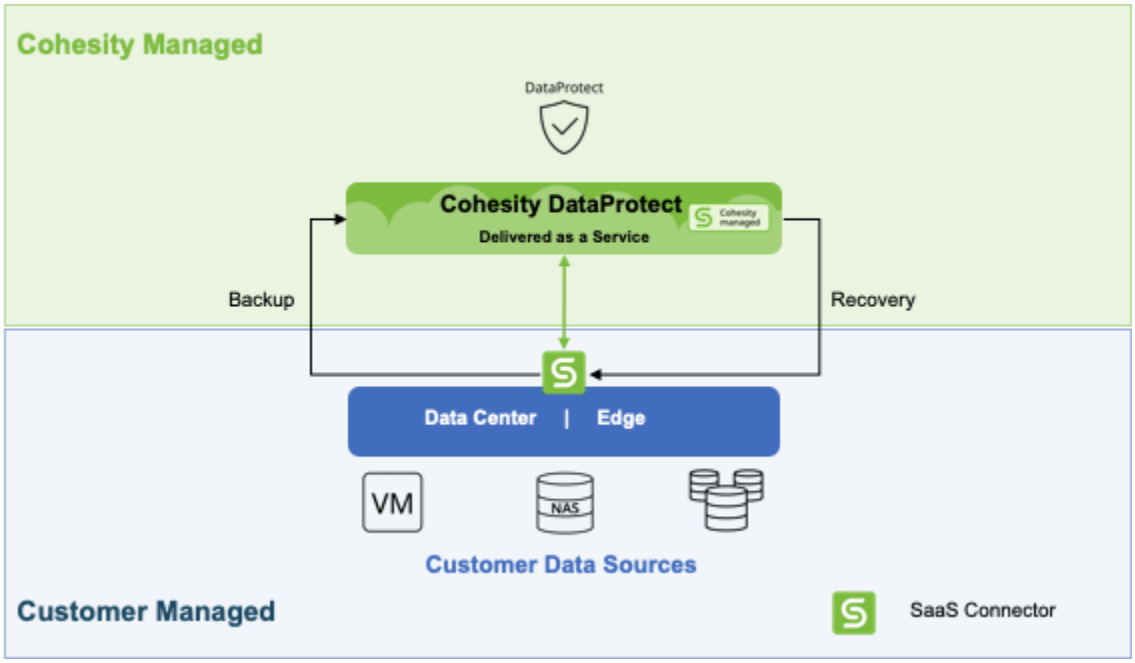
Figures

Introduction

Today's companies and organizations are overwhelmed with the exponential growth of the amount of data they collect, manage, and store. Like many facing this challenge, you need more options for managing your data infrastructure and data centers, such as having it managed for you in a Software as a Service (SaaS) model, without the infrastructure headaches.

We designed Cohesity Data Cloud to provide enterprise-grade Cloud Services by delivering a comprehensive set of data management SaaS offerings. The first offering is *Cohesity DataProtect delivered as a service*, which provides backup and protection for your virtual and physical workloads, databases, and applications. You can sign up and start backing up your data *today*.

Figure 1: Quickly Sign Up and Start Protecting Your Data, Databases, and Applications



With Cohesity DataProtect delivered as a service, you can:

- **Reduce complexity with Backup as a Service that is built for the hybrid cloud**, freeing up cycles to focus on other critical tasks.
- **Reduce backup setup to minutes** by automatically discovering workloads (once a secure connection is established) and applying policies to begin protection.
- **Support multiple diverse workloads**, including VMware VMs and NAS file data today, Microsoft 365 and enterprise databases in the coming months, and many more in the quarters ahead – all delivered in a single, converged experience.
- **Ensure efficient use of available bandwidth**, accelerating backups *to* the cloud, and data recovery *from* the cloud, by only transmitting the data that has changed.

This guide takes you through the on-boarding experience of Cohesity DataProtect delivered as a service. You'll get up to speed with the concepts, terminology, and procedures you need to sign up, connect, and start protecting your data quickly.

If you haven't already, be sure to sign up for your free trial!

Get Started

Now that you have signed up for the free trial, you can protect your data using Cohesity DataProtect delivered as a service in three simple steps:

1. **Set Up**. Select the region to store data and the encryption key management configuration.
2. **Connect**. Install the SaaS Connector and configure it to connect to the service.
3. **Protect**. Register your data source and start protecting it.
    a) Protect VMware
    b) Protect NAS
    c) Protect Microsoft SQL Server
    d) Protect Microsoft 365

Figure 2: Simplicity — Set Up, Connect, Protect

The free trial duration is 30 days and you can back up up to 5 TBs of data during the free trial.

Start with setting it up next!

Set Up Your Account

To begin using Cohesity DataProtect delivered as a service, you first need to log in to Cohesity Helios and:

- Choose the cloud region for your data.
- Choose the Key Management System (KMS) to encrypt your data.

Choose Cloud Region

Before you can use Cohesity DataProtect, you need to choose a cloud region for your data backups. Currently, Cohesity DataProtect supports:

- US East (Ohio)
- US East (N. Virginia)
- US West (Oregon)
- US West (N. California)
- Canada (Central)
- Asia Pacific (Sydney)
- Europe (Frankfurt)

IMPORTANT: Once data is backed up to one region, you cannot move it to another. To back your data up in another region, you can add that region and start protecting the data there.

Choose a Key Management System (KMS)

In Cohesity DataProtect, all the data is encrypted both in-flight and at rest. Choose which Key Management System (KMS) to use to encrypt your data:

- **Cohesity-managed KMS**. Built-in with Cohesity DataProtect.
- **Self-managed KMS**. You can also use your AWS KMS for encryption instead. To use your own AWS KMS, enter your AWS Key ARN for the region you selected, copy the generated JSON, and add it to the Encryption Key Policy in your AWS account.

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

Connect

To register sources in your data center with Cohesity DataProtect, you need to use a SaaS Connection to establish connectivity between your source and the service. A SaaS Connection consists of one or more SaaS Connector VMs that run in your data center to move the data.

Requirements

To create a SaaS Connection, you deploy a SaaS Connector installer OVA in your VMware environment, on a vCenter or ESXi host in your data center that has access to your data sources and meets the SaaS Connection system, network, and sizing requirements listed in the Cohesity Help.

Create a SaaS Connection

Once deployed, each SaaS Connector is a virtual machine that runs on a vCenter or ESXi host in your data center.

> **TIP**: For better performance and redundancy, Cohesity recommends you deploy at least two or more SaaS Connectors for each SaaS Connection in your data center. To create multiple SaaS Connectors in the same SaaS Connection, use the same Connection Token in the procedure below.

> **NOTE**: All the data that a SaaS Connection handles, from your sources to the cloud storage where your backups reside, is encrypted in-flight and at rest.

To create a SaaS Connection:

1. Navigate to **Sources** and click **Add** (**+**).
2. Select a workload type (**Hypervisor** or **NAS**).
3. In the form, click **Create New Connection**.
4. Select a **Connection Region** for your data backups.
5. Prepare to deploy the SaaS Connector in your data center:
   a) **Copy** the OVA URL or **Download** the OVA file.
   b) **Copy** or **Download** the **Connection Token**.

   > **NOTE**: SaaS Connectors that use the same Connection Token are considered part of the same SaaS Connection. This enables them to perform load balancing among them.
6. To deploy the SaaS Connector OVA in your virtual data center, see VMware's Deploy a Virtual Machine from an OVF or OVA File in the VMware Host Client or follow these steps:

a) Log in to your vCenter host.

b) Right-click an inventory object and select **Deploy OVF Template**.

c) In the **Deploy OVF Template** wizard, enter the OVA URL or specify the location of the OVA you downloaded. Then configure more settings in the next few screens:

   i. **Select a compute resource** for the SaaS Connector VM and click **Next**.

   ii. **Review details**. Verify the SaaS Connector information.

   iii. **Configure**. Select the SaaS Connection configuration.

   iv. **Select storage**. Select a datastore with at least 20 GB disk space.

   v. **Select Networks page**. Select a network.

   vi. **Customize template**. Enter the **Network IP Address**, **Network Netmask**, and **Default Gateway**.

   vii. **Ready to complete**. Review the summary and click **Finish**.

d) Once the VM is created, power it on. Note that it can take a few minutes for the VM to boot.

7. Open your web browser and connect to the SaaS Connector VM IP and log in as admin/admin. On initial login, change the default password and log in again with your new password. Enter the **Connection Token** and common configuration settings (DNS servers, domain name, etc.) and click **Save**.

   NOTE: It can take several minutes for the services in your SaaS Connector to start up and authenticate to the Cohesity DataProtect service.

8. Once the SaaS Connector authenticates successfully, return to the **Create New Connection** dialog and click **Verify Connection**.

Your new SaaS Connection is available under **Use Existing Connection** to register your VMware and NAS (generic or Dell Isilon) sources.

Manage SaaS Connections

To add or remove a SaaS Connector, see Manage Your SaaS Connections in the Cohesity Help.

Protect VMware

To start protecting your VMware VMs, you need to register your data sources.

NOTE: To connect with sources in your data center, you'll need to use a SaaS Connection (or create one) to establish connectivity between the sources and the Cohesity DataProtect service.

Requirements

To register your VMware sources, confirm that you meet the VMware requirements in the Cohesity Help for software version and user account role privileges.

Register VMware

To start protecting your VMware VMs, you need to register your data sources. To register a vCenter or Standalone ESXi host:

1. Navigate to **Sources** and click **Add** (**+**).
2. Select workload type **Hypervisor**.
3. In the form, choose **Use Existing Connection** and select one that is marked **Healthy**, or click **Create New Connection** and follow the instructions above, in Create a SaaS Connection.
4. Select the **Hypervisor Source Type**: **vCenter** or **Standalone ESXi Host**.
5. Enter the hypervisor's **Hostname or IP Address**.
6. Enter the **Username** and **Password**.
7. Click **Save**.

Protect VMware VMs

Use Cohesity DataProtect to protect the virtual machines (VMs) and files in your VMware environment.

To protect a VMware source:

1. Register your vCenter Server or ESXi host as a **Hypervisor** in **Sources**.
2. Go to **Sources**.
3. Select the **Source** name.
4. Use the filters, search box, and views at the top to narrow your search.
5. Use the checkboxes to select the VMs for protection. To protect the whole source, click the checkbox above the column.

> **NOTE**: When you check a parent object, you can choose:
>
> - **Select All Child Objects**. To capture the tree *as it currently exists*, or
> - **Auto Protect**. To capture the tree *and any future additions*. You can auto-protect at different levels such as vCenter, VDC, host, folder.

6. Choose a policy to specify backup frequency and retention. If you don't have a policy, you can create one.
7. Click **Protect**.

Cohesity DataProtect starts backing up the VMs you selected.

Recover VMware

After you protect a VMware source, you can recover the VMs and files from your backups, to their original or a new location.

Setup Recovery

To recover protected VMs or files:

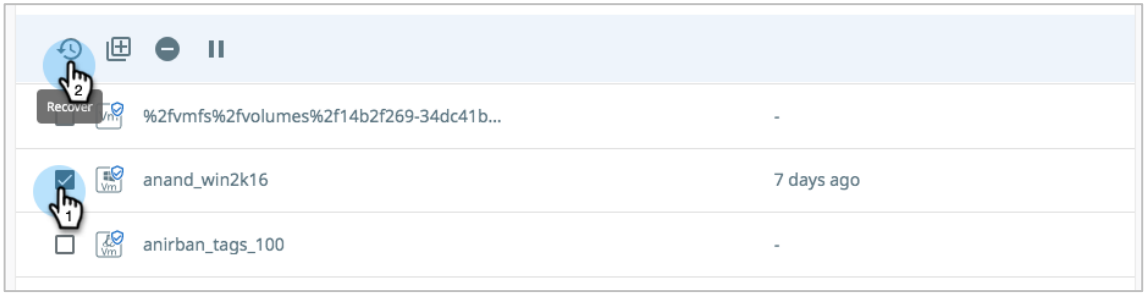
1. Navigate to **Sources**.
2. Click into the **Source** name.
3. Above the tree, select **Show All > Protected** and click the **List** view icon on the right.
4. Use the filters, search box, and views to locate the objects or files you need.
5. To recover:
   - **Objects continue** with the Recover VMs procedure below.
   - **Files and folders**, continue with the Recover Files and Folders procedure below.

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

Recover VMs

To recover protected VMs:

1. Locate and select them, and then click **Recover** at the top to open the **New Recovery** form with the **Latest** snapshot (protection run).



2. If you need to recover from an earlier snapshot, click the **Edit** icon to select a new recovery point.
   a) For each object under **Selected**, you can click the **Edit** icon to open the **Recovery Point** calendar. Click **List** to view the available recovery points by timestamp and click one.
   b) Click **Select Recovery Point**.
   c) Click **Next: Recover Options** to return to the form.
3. Under **Recover To**, select **Original Location** or **New Location**. **For NAS volumes**: If you choose **New Location**, select a **Registered Source** and the **Volume**.
4. Select your **Recovery Options** (for object recovery).
5. Click **Start Recovery**.

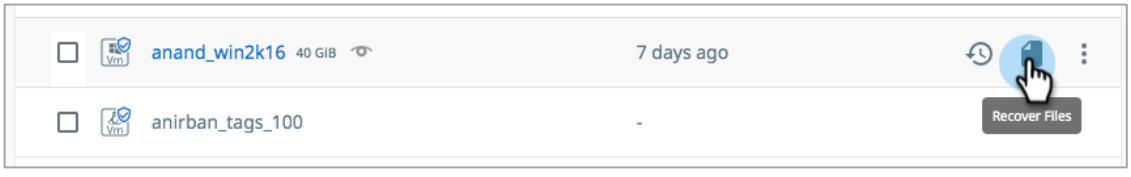
Cohesity DataProtect opens the **Activity** page, showing your file recovery task as it runs, along with the recovery progress on the right.

> **TIP:** The **Activity** page also shows the entire history of all protection runs and recovery tasks.

Recover Files and Folders

To recover a specific file or files (or the folders containing them) from a protected VM:

1. Locate the VM containing the files and click **Recover Files** on the row for that VM to open the **Select Files** form.



2. If you need to recover from an earlier snapshot, click the **Recovery Point** calendar drop-down to select the recovery point.

a) Click **List** to view the available recovery points by timestamp and click one.

b) Click **Apply**.

3. Click into the path to find the files and add them to the **Selected Items** list.
4. Choose how to recover your files: download locally or recover.

a) Click **Download Files** to open the **Activity** page, showing your file recovery task. Click into the recovery task and click **Download Files** a second time to save them to your local system.

b) Click **Save** to open the **New Recovery** form. Under **Recover To**, select **Original Location** or **New Location**.

c) If you choose **Original Location**, enter a **Username** and **Password** that has access to the original server. You can also enable **Recover to Alternate Path** to enter a new path on the original server.

d) If you choose **New Location**, select a registered **Source** and a **Target** VM. Enter a **Username** and **Password** that has access to that server and enter a **Recover To** path.

5. Select your Recovery Options (for file recovery).
6. Click **Start Recovery**.

Cohesity DataProtect opens the **Activity** page, showing your file recovery task as it runs, along with the recovery progress on the right.

> **TIP:** The **Activity** page also shows the entire history of all protection runs and recovery tasks.

Protect NAS

Use Cohesity Dataprotect service to protect the NAS volumes, files, and folders in your data center. You can protect any generic NAS, a Dell EMC Isilon, and NetApp Ontap.

Protect Generic NAS

You can register any generic NAS source via mount point. Confirm that you meet the requirements and follow the steps below.

Generic NAS Requirements

Ensure that the TCP/UDP ports 445, 8080, 111, and 2049 are open in the firewall between the SaaS Connector and your NAS device.

Register Generic NAS

Use NFS or SMB to connect a generic NAS source to Cohesity DataProtect as a mount point.

To register your generic NAS source via NFS or SMB:

1. Navigate to **Sources** and click **Add** (**+**).
2. Select workload type **NAS**.
3. In the form, choose **Use Existing Connection** and select one that is marked **Healthy**, or click **Create New Connection** and follow the instructions above, in Create a SaaS Connection.
4. Under **NAS Source Type**, select **Mount Point**.
5. Under **Mode**, choose **NFS** or **SMB**.
6. Enter the **Mount Path**.
   - For **NFS**, enter the **hostname** or **IP:/Volume**.
   - For **SMB**, enter the **\\hostname** or **IP\Share Path**.
7. If you are confident the mount point is correct, you can enable **Skip Mount Point validation during registration**. (*Optional*.)
8. Add a **Description** to make it easier to recognize this source. (*Optional*.)
9. If you chose **SMB** above, enter the **Username** and **Password** required to access the SMB share.
10. Click **Save**.

Your NAS device is now a registered source in your Cohesity DataProtect service and ready to be protected.

Protect Dell Isilon

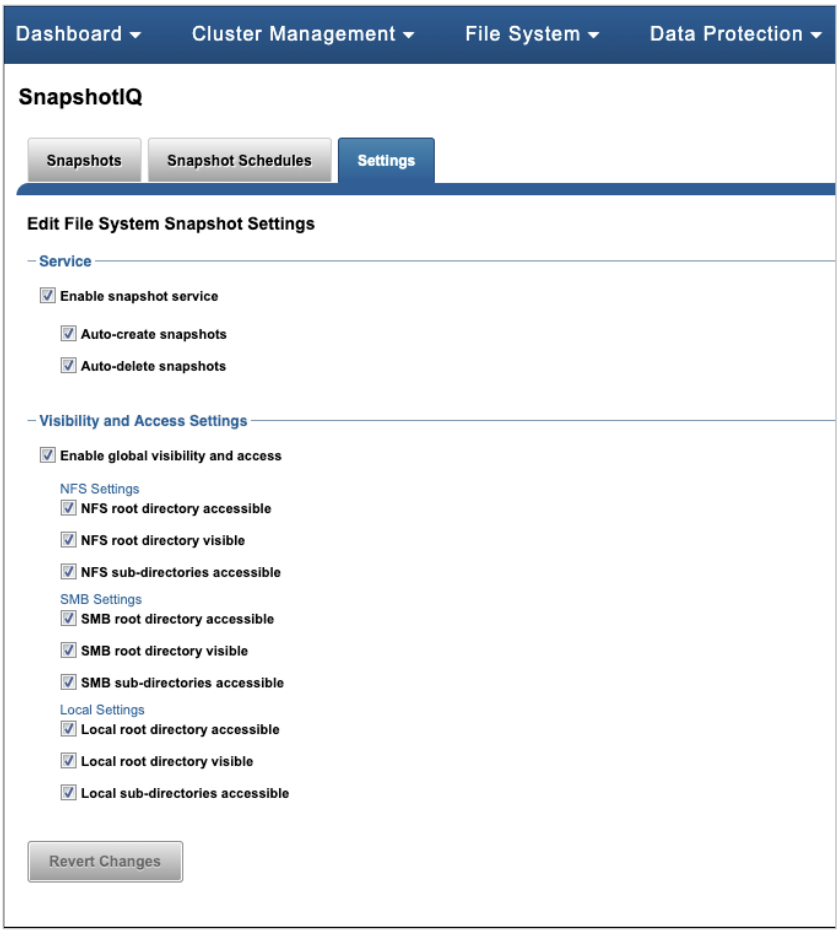
Before you register an Isilon cluster with Cohesity DataProtect, confirm that you have met the Isilon requirements and permissions below.

Dell Isilon Requirements

- Ensure that the TCP/UDP ports 445, 8080, 111, and 2049 are open in the firewall between your SaaS Connector and Cohesity DataProtect.
- Isilon OneFS version 8.0.x or 8.2.x.
- NFS v3 for NFS export backups.

  NOTE: Cohesity DataProtect uses NFS v3 and SMB v1, v2, or v3 for data protection.

- On Isilon NFS shares, enable the "Mount access to subdirectories" flag. Cohesity DataProtect requires this setting to mount the **.snapshot** directory of the shared path.
- SnapshotIQ license enabled on Isilon, with these settings:



Minimum Isilon User Permissions

Cohesity DataProtect accesses your Isilon cluster using an Isilon user account. The user account must have the following permissions to back up and restore your Isilon data via SMB or NFS.

- **Read-only Access Permissions**:
  - **Platform API**. For access to Isilon's APIs.
  - **Auth**. To verify users and passwords.
  - **Cluster**. To obtain cluster identity and settings.
  - **Network**. To obtain the network interfaces.
  - **SMB**. To read the settings in the SMB server.
- **Read/Write Access Permissions**:
  - **Job Engine**. To read and write Changelist jobs.
  - **Snapshot**. To fetch, create, and delete snapshots for shares and exports.
  - **NFS**. To read and write settings to and from the NFS server.

    NOTE: This setting modifies the NFS export used to mount, such as **/ifs**

Register Dell Isilon

To register your Isilon cluster:

1. Navigate to **Sources** and click **Add** (**+**).
2. Select the workload type **NAS**.
3. In the form, choose **Use Existing Connection** and select one that is marked **Healthy**, or click **Create New Connection** and follow the instructions above, in Create a SaaS Connection.
4. Under **NAS Source Type**, select **Isilon (Cluster)**.
5. Enter the Isilon cluster's **Hostname or IP Address**.
6. Enter the **Username** and **Password** that you configured earlier, in Minimum Isilon User Permissions above.

7. If you are backing up SMB volumes or mixed-mode volumes, enable **Backup SMB Volumes** and enter the local or Active Directory (AD) **Username** and **Password** required for at least **read** access to the Isilon SMB share.

   NOTES:

   - You can assign the local or AD user to the built-in "BackupAdmin" role to permit that user to read the SMB data for backup without modifying the access control lists (ACLs).
   - To provide access at the share level, grant the "Run as root" and "Full Control" permissions at the share level.
   - The user must have full control on the restore target during recovery.

8. To exclude IP addresses or subnets from the communications between Cohesity DataProtect and the Isilon cluster, enable **Exclude IPs** and enter those IPs.
9. Click **Save**.

Your Isilon cluster is now a registered source in your Cohesity DataProtect service and ready to be protected.

Recover NAS

After you protect a source, you can recover the objects and files from your backups, to their original or a new location.

Setup Recovery

To recover protected NAS volumes or files:

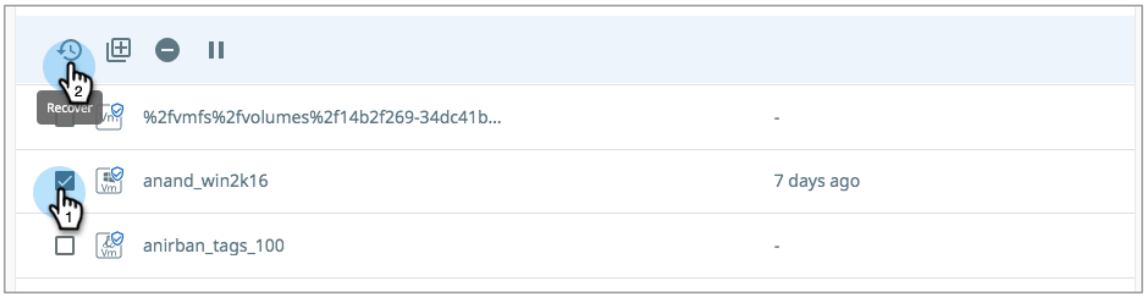
1. Navigate to **Sources**.
2. Click into the **Source** name.
3. Above the tree, select **Show All > Protected** and click the **List** view icon on the right.
4. Use the filters, search box, and views to locate the objects or files you need.
5. To recover:
   - **Objects**, continue with the Recover Objects procedure below.
   - **Files and folders**, continue with the Recover Files procedure below.

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

Recover Volumes

To recover protected objects (VMs or NAS volumes):

1. Locate and select them, and then click **Recover** at the top to open the **New Recovery** form with the **Latest** snapshot (protection run).



2. If you need to recover from an earlier snapshot, click the **Edit** icon to select a new recovery point.
   a) For each object under **Selected**, you can click the **Edit** icon to open the **Recovery Point** calendar. Click **List** to view the available recovery points by timestamp and click one.
   b) Click **Select Recovery Point**.
   c) Click **Next: Recover Options** to return to the form.
3. Under **Recover To**, select **Original Location** or **New Location**. **For NAS volumes**: If you choose **New Location**, select a **Registered Source** and the **Volume**.

4. Select your Recovery Options (for object recovery).
5. Click **Start Recovery**.

Cohesity DataProtect opens the **Activity** page, showing your file recovery task as it runs, along with the recovery progress on the right.

> **TIP:** The **Activity** page also shows the entire history of all protection runs and recovery tasks.

Recover Files and Folders

To recover a specific file or files (or the folders containing them) from a protected NAS source volume:

1. Locate the volume containing the files and click **Recover Files** on the row for that volume to open the **Select Files** form.

2. If you need to recover from an earlier snapshot, click the **Recovery Point** calendar drop-down to select the recovery point.
   a) Click **List** to view the available recovery points by timestamp and click one.
   b) Click **Apply**.
3. Click into the path to find the files and add them to the **Selected Items** list.
4. Choose how to recover your files: download locally or recover.
   a) Click **Download Files** to open the **Activity** page, showing your file recovery task. Click into the recovery task and click **Download Files** a second time to save them to your local system.
   b) Click **Save** to open the **New Recovery** form. Under **Recover To**, select **Original Location** or **New Location**.
   c) If you choose **Original Location**, enter a **Username** and **Password** that has access to the original server. You can also enable **Recover to Alternate Path** to enter a new path on the original server.
   d) If you choose **New Location**, select a registered **Source** and a **Target** (VM) or **Volume** (NAS). Enter a **Username** and **Password** that has access to that server and enter a **Recover To** path.
5. Select your **Recovery Options** (for file recovery).
6. Click **Start Recovery**.

Cohesity DataProtect opens the **Activity** page, showing your file recovery task as it runs, along with the recovery progress on the right.

> **TIP:** The **Activity** page also shows the entire history of all protection runs and recovery tasks.

Protect Microsoft SQL Server

Cohesity DataProtect Service uses Microsoft SQL Server Virtual Device Interface (VDI) to perform backups of databases on a registered SQL Server instance.

Requirements

To register your Microsoft SQL Server sources, confirm that you meet the MS SQL requirements in the Cohesity Help for software version and user account role privileges.

Register MS SQL

To start protecting an MS SQL Server database, once you meet the MS SQL requirements, you need to register the SQL Server as a source.

> **NOTE**: To connect with sources in your data center, you'll need to use a SaaS Connection (or create one) to establish connectivity between the sources and the Cohesity DataProtect service.

To register an MS SQL server, check that it meets the prerequisites below and then add it as a source in DataProtect.

Prerequisites

Before you proceed to registering the SQL Server as a source, make sure you've satisfied the following conditions:

- Verify MS SQL Server services are running.
- On the server's Windows system, set the **Power Plan** to **High performance**.
- On the SQL Server where you have installed the Cohesity Agent, open the following ports:
  - **50051**, for backup operations (incoming).
  - **11113** and **11117**, for VDI-based backup and restore (outgoing).
  - If you're using the Windows Firewall, set:

    Inbound rules:
  - Add a rule to accept SQL Server traffic and TCP connections on local port 1433.
  - Set **Remote Port** to **All Ports**.

    Outbound rules (for MS SQL Server 2016 running on Windows 2016): Update the "Block network access for R local user accounts in SQL server instance MSSQLSERVER" rule by navigating to **General** > **Action window** and selecting **Allow the connection**.

Register an MS SQL Server Source

To add an MS SQL Server as a Cohesity DataProtect source:

1. Confirm that you meet the MS SQL requirements for software version and user account minimum permissions.
2. Navigate to **Sources** and click **Register Source**.
3. Select workload type **MS SQL Server**.
4. In the form, choose **Use Existing Connection** and select one that is marked **Healthy**, or click **Create New Connection** and follow the instructions in Create a SaaS Connection.
5. Enter the MS SQL server **Hostname** or **IP Address**, the FQDN of the server, or the VIP of the SQL FCI.
6. Click **Save**. Cohesity DataProtect auto-discovers the entire MS SQL topology on the Windows cluster.
7. From the topology list, select **Register all MSSQL Nodes** to register the MS SQL nodes as individual MS SQL sources.
8. Click **Complete Registration**.

Protect MS SQL Server Source

Once you have registered an MS SQL server as a source, you're ready to use Cohesity DataProtect to protect the MS SQL databases on that server.

To protect your MS SQL databases:

1. Under **Sources**, find the MS SQL source, click the **Actions** menu (⋮), and select **Protect**.
2. Click **Add Objects.** Browse through the SQL Server instances and select the databases that you want to protect. Click **Continue**.
3. Choose a policy to specify backup frequency and retention.* If you don't have a policy, you can easily create one.
4. Click **More Options** and review the following MS SQL Settings:
   a) **Make Full Backups Copy-only.** Enable if you want full backups to be copy-only backups so they do not affect the differential base. Note that copy-only full backups do not take log backups even if the policy schedules them.
   b) **WITH Clause.** Define the WITH clause that you want to use to customize the backup. For more information, see BACKUP (Transact-SQL) in the Microsoft documentation.
   c) **Number of Streams**. Define the number of **.bak** files you want to create for better backup performance. By default, Cohesity DataProtect creates three **.bak** files for each database backup for better backup performance.
5. Click **Protect**.

Cohesity DataProtect starts backing up the databases you selected.

*__NOTE__: When choosing or configuring your policy, ensure the full, incremental (SQL Differential), and T-Log backup retention periods are properly configured. The retention period requirements for SQL VDI are identical to those for SQL native backups. For example, Cohesity recommends aligning your retention periods for each backup type along these lines:

- **Full Backups**. Daily at 1am with a 7-day retention.
- **Incremental Backups** (equivalent to SQL Differential backups). Every 12 hours with a 3-day retention.
- **T-Log Backups**. Every 15 minutes with a 1-day retention.

Recover MS SQL Server

After you protect your MS SQL databases, you can recover them from Cohesity DataProtect, to their original or a new location.

To recover protected MS SQL databases:

1. Go to **Sources** to set up your recovery task.
2. Click into the **Source** name.
3. Above the tree, select **Show All > Protected**.
4. Use the filters, search box, and views to locate and select the SQL databases you need.

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

5. Click **Recover** at the top to open the **New Recovery** form with the **Latest** snapshot (protection run). If you need to recover from an earlier snapshot, click the **Edit** icon to open the **Recovery Point** calendar. Click **List** to view the available recovery points by timestamp and click one.
   - Click **Select Recovery Point**.
   - Click **Next: Recover Options** to return to the form.
6. Under **Targets**, select **Recover as a new Database** or **Overwrite Original Database**. If you choose:
   - **Recover as a new Database**, select a registered **MS SQL Instance** *or* **Restore to Original SQL Server Instance**.
   - **Overwrite Original Database**, DataProtect will overwrite the original SQL Server instance. Note that this is a destructive action that cannot be undone.
7. If necessary, under **Database File Paths**, you can:
   - Update the **Database Files** and **Log Files** paths.
   - Enter additional **File Path Rules**.

8. Select your **Recovery Options**:
    - **Rename**. Choose whether to **Bulk Rename** with a **Suffix** or **Rename Individual Objects**.
    - **WITH RECOVERY**: By default, an MS SQL restore WITH RECOVERY is performed. You can optionally toggle this off to perform a restore WITH NORECOVERY.
    - **Keep CDC**: Use this option to restore a backed-up database with the change data capture (CDC) enabled. By default, the Keep CDC switch is **ON**. If the backed-up database is not CDC enabled and the user tries to restore it with Keep CDC, the database will be restored without CDC.
    - **WITH Clause**: Specify the WITH clause that you want to use for the restore.
    - **Capture Tail Logs**: You can optionally choose to **Capture tail logs**. Tail logs capture records that have not yet been backed up. They are captured to ensure all transactions are backed up before restoring the database.
    - **Task Name**. Change the default name of the recovery task.
9. Click **Start Recovery**.

Protect Microsoft 365

Microsoft 365 is a SaaS application that is a bundle of messaging and collaboration applications such as Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Groups and Microsoft Teams. Cohesity DataProtect provides enterprise-grade backup and recovery solutions for Microsoft 365.

Requirements

Before you start the Microsoft 365 protection with Cohesity, confirm that you meet the Microsoft 365 requirements in the Cohesity Help.

Register Microsoft 365

To start protecting Microsoft 365 applications, you need to register the Microsoft 365 domain as a source in Cohesity DataProtect.

To register your Microsoft 365 domain:

1. Navigate to **Sources** and select **Register Source** > **Microsoft 365**.
2. In the **Source Details** section, enter the Microsoft 365 **Username** and **Password**.
3. *Optional*. Toggle the **Enable OAuth** option on if you have enabled OAuth authentication for EWS for Exchange Online in Microsoft 365.

   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**.
4. Select the **Destination cloud region**.
5. Click **Register**.

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

Protect Exchange Online

Cohesity DataProtect offers seamless backup and recovery for your Exchange Online mailboxes.

Protect Mailbox

Once you have registered your Microsoft 365 domain as a source, you're ready to use Cohesity DataProtect to protect the user Mailboxes in your domain.

To protect your M365 Mailboxes:

1. Under **Sources**, find the Microsoft 365 source, and click into it.
2. 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.
3. Click the **Protect** icon above the list.
4. Choose a policy to specify backup frequency and retention. If you don't have a policy, you can easily create one.
5. Under **Settings**, edit the **Start Time** if necessary.
6. Under **Additional Settings**, you can configure a specific **End Date**, **Alerts**, and other additional settings.
7. Click **Protect**.

Recover Mailbox

After you protect your users' M365 Mailboxes, you can recover them from Cohesity DataProtect.

> **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.

To recover protected Microsoft 365 user Mailboxes:

1. Go to **Sources** to set up your recovery task.
2. Click into the **Source** name.
3. Above the tree, select **Show All > Protected**.
4. Find the Mailbox 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 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 DataProtect will still attempt to recover the other selected Mailboxes.
    - **Task Name**. Change the default name of the recovery task.
8. Click **Start Recovery**.

Protect OneDrive For Business

Cohesity DataProtect offers seamless backup and recovery for your OneDrive storage.

Protect OneDrive For Business

Once you have registered your Microsoft 365 domain as a source, you're ready to use Cohesity DataProtect to protect the user drives in your domain. For more information, see Protect M365 OneDrive for Business.

Recover OneDrive for Business

After you protect your users' OneDrive, you can recover them from Cohesity DataProtect. For more information, see Recover M365 OneDrive for Business.

Protect SharePoint Online

Cohesity DataProtect offers seamless backup and recovery for your SharePOint Online Sites.

Protect Sites

Once you have registered your Microsoft 365 domain as a source, you're ready to use Cohesity DataProtect to protect the user drives in your domain. For more information, see Protect M365 SharePoint Online.

Recover Sites

After you protect your SharePoint Online Sites, you can recover them from Cohesity DataProtect. For more information, see Recover M365 SharePoint Online Sites.

Protect Microsoft Teams

Cohesity DataProtect offers seamless backup and recovery for your Microsoft Teams data.

*Protect Teams

Once you have registered your Microsoft 365 domain as a source, you're ready to use Cohesity DataProtect to protect the user drives in your domain. For more information, see Protect M365 Teams.

Recover Teams

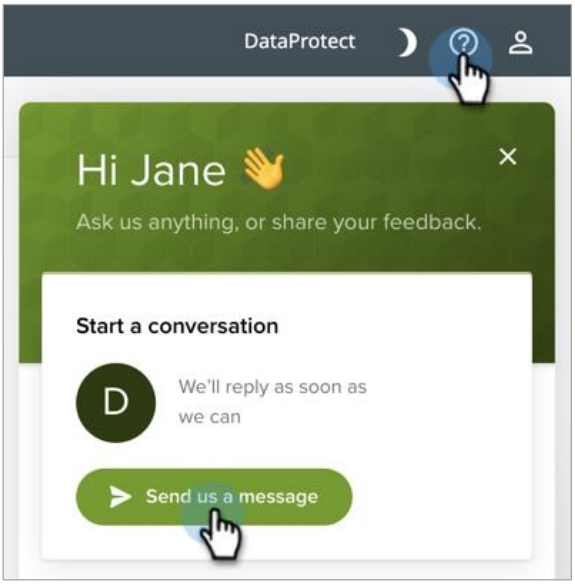
After you protect your SharePoint Online Sites, you can recover them from Cohesity DataProtect. For more information, see Recover M365 Teams.

Help and Support

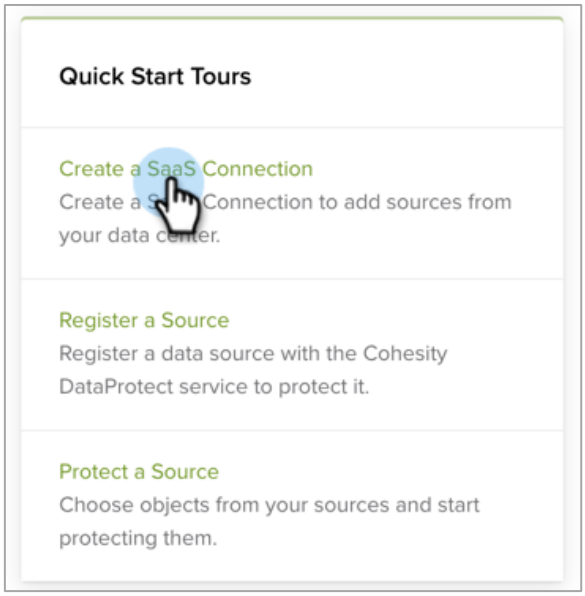
We are committed to providing the best in-class support experience to our customers. As part of that goal, we greet our customers with in-app Help.

Click the **Help** button ( ) in the top-right corner to open:

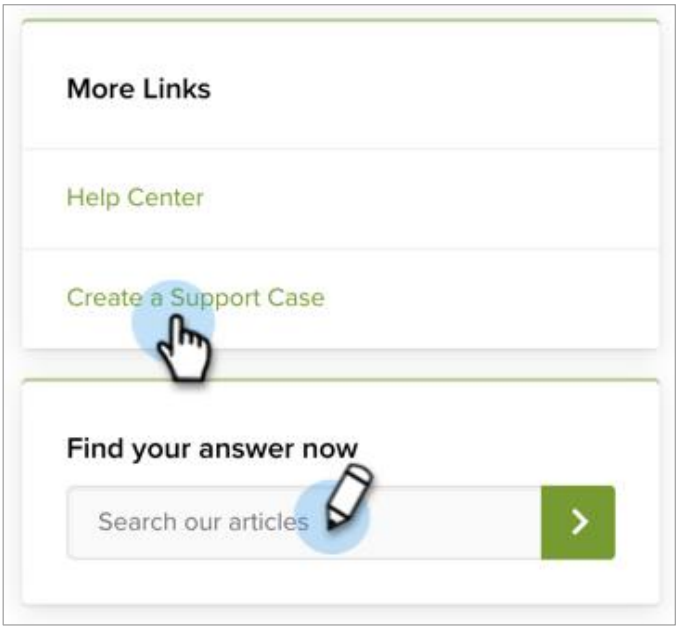
- An AI-powered chatbot to help you answer your questions quickly and connect you to our support team when you need more help. Click **Send us a message** to get started!



- Guided tours to help you connect and protect quickly.



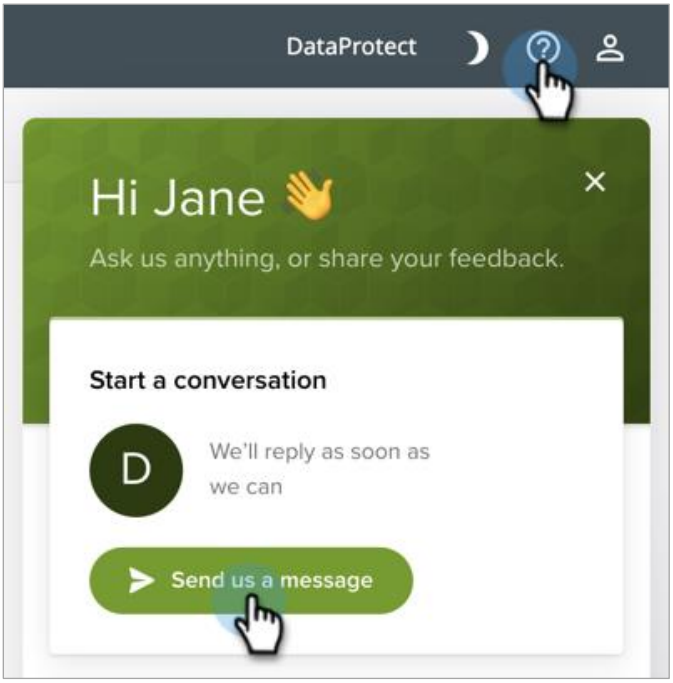
- Our **Help Center** articles and a link where you can **Create a Support Case** for additional help. You can also search our Help articles directly from the panel.



Feedback

We would love to hear your feedback on your experience with the product.

To submit feedback, go to **Help** > **Send us a message**.



Upgrade to Paid Subscription

Your free trial is limited to 30 days, 200 objects, and 5TB of front-end capacity. To continue using the service or to expand the capacity you need to support your backups, consider upgrading to a paid subscription.

The data that you backed up during the free trial will still be available after you convert to a paid subscription.

You have two options to upgrade to a paid subscription:

- **Subscribe on AWS Marketplace**: AWS Marketplace Cohesity DataProtect
  a) Click **Continue to Subscribe** and complete your subscription on AWS Marketplace.
  b) You are then redirected to the Cohesity DataProtect 'Register now' form.
  c) Once the 'Register now' form is complete, you will receive a Cohesity DataProtect welcome email.
  d) Use your free trial login information to activate your Cohesity DataProtect subscription.
- **Purchase via Cohesity Reseller**: Contact commercial-sales---americas@cohesity.com to get a quote.
  a) A purchase order is submitted to Cohesity via the reseller or distributor.
    i. After your purchase order is processed by Cohesity, you will receive a Cohesity DataProtect welcome email.
    ii. Use your free trial login information to activate your Cohesity DataProtect subscription.
  b) AWS private offer issued by partner & Cohesity via AWS.
    i. Use the private offer link provided by your reseller and click **Continue to Subscribe** to complete the subscription on AWS Marketplace.
    ii. You are then redirected to the Cohesity 'Register now' form.
    iii. Once the Cohesity 'Register now' form is complete, you will receive a Cohesity DataProtect welcome email
    iv. Use your free trial login information to activate your Cohesity DataProtect subscription.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Saurabh Singh is a Staff Technical Solutions Engineer at Cohesity. In his role, he focuses on Cohesity Cloud Services, secure multi-tenancy, and SaaS backup.

Other major contributors included:

- Douglas Ko, Director, Product Marketing
- Bart Abicht, Sr. Technology Editor

Document Version History

VERSION	DATE	DOCUMENT HISTORY
3.2	June 2023	Rebranding updates
3.1	July 2022	Minor updates
3.0	June 2021	Added new region information, added remaining Microsoft 365 applications
2.0	April 2021	Added Microsoft 365 and MS SQL deployment details
1.0	Jan 2021	First release

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.