Cohesity Alta SaaS Protection Administrator's Guide

VERITAS™
now part of Cohesity

Last updated: 2026-08-31

Last updated: 2026-08-31

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. 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.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. COHESITY SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

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.

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 the 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 and 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.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.veritas.com/support

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Technical Support
  - Recent software configuration changes and network changes

Licensing and registration

If your product requires registration or a license key, access our technical support Web page at the following URL:

www.veritas.com/support

Customer service

Customer service information is available at the following URL:

www.veritas.com/support

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Advice about technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact us regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Contents

Chapter 1 Introduction to Cohesity Alta SaaS Protection 13

About Cohesity Alta SaaS Protection 13
Features of Cohesity Alta SaaS Protection 15
Architecture of Cohesity Alta SaaS Protection 17
Operational workflow 20
Extra Data Backup (EDB) 23

Chapter 2 Cohesity Alta SaaS Protection Copilot (AI chatbot) 29

Cohesity Alta SaaS Protection Copilot (AI chatbot) 29

Chapter 3 Cohesity Alta SaaS Protection Administrator portal (Web UI) 31

About Cohesity Alta SaaS Protection Administration portal 31
Configure Cohesity Alta SaaS Protection Administration portal 33
View upgrade history 36

Chapter 4 Supported SaaS workloads 37

Supported SaaS workloads and backup capabilities 37

Chapter 5 Workflow to protect data using Cohesity Alta SaaS Protection 45

Workflow to protect data using Cohesity Alta SaaS Protection 45
Know your subscription details 46

Chapter 6 Manage users and roles 47

Role-based access control 47
Permissions tab 48
Users and groups page 51
Roles page 53
Unrecognized users page 54

Settings page 55

Chapter 7 API permissions 56

API permissions for Microsoft 365 workloads 56
API permissions for Gmail and Google Drive 64
System and API permissions for Salesforce 65
API permissions for Entra ID 74
App permissions of Web App 79

Chapter 8 What is a connector? 80

What is a connector? 81
About transient errors 82
Overview of adding connectors 82
Configure General settings 83
Configure Capture scope 83
Configure User filter 85
Configure Group filter 86
Configure Folder filter 87
Configure credentials 88
Assign Microsoft 365 apps registration 89
Microsoft 365 apps registration status 90
Manually approve Microsoft 365 apps registration 91
Approve Microsoft 365 apps using the App Consent Grant utility 92
Microsoft 365 apps recovery 93
Configure Custom backup policy and guidelines 93
Configure Delete policy for SharePoint Online and guidelines 95
Configure Stubbing policy 100
Guidelines to configure Stubbing policy for SharePoint Online 102
Schedule a backup 115
Configure email addresses to get notifications 116
Review configuration and edit/save/initiate backup 116
Connectors page 117
Connector status 119
Edit connector configuration 121
Delete connectors 121

Chapter 9 Pre-requisites to setup protection for M365 122

Pre-requisites to setup protection for M365 122

Chapter 10 Protect Microsoft 365 Multi-Geo tenant 125

Considerations for adding SharePoint/Teams Sites/OneDrive connectors for Microsoft 365 Multi-Geo tenant 125

Chapter 11 Protect Exchange Online data 127

Setting up Exchange Online data protection with Cohesity Alta SaaS Protection 127
Configure capture scope for Exchange connectors 130

Chapter 12 Protect SharePoint sites and data 138

Setting up SharePoint Online protection with Cohesity Alta SaaS Protection 138
Configure capture scope for SharePoint connectors 141
Configure additional backup options for SharePoint/Teams site/ OneDrive connectors 142
Backup and restore support for SharePoint Online 143
Supported and unsupported SharePoint Objects, Properties, Settings, and Types for backup and restore 144
Supported Sites and List templates for backup and restore 146
Supported SharePoint permission objects for backup and restore 148
End-user SharePoint data access in Cohesity Alta SaaS Protection 148
Run the Delete and Stubbing policies to the SharePoint Online environment 151
Backup limitations for SharePoint Online 151

Chapter 13 Protect Teams sites 153

Setting up Teams Site protection with Cohesity Alta SaaS Protection 153
Configure capture scope for Team site collections connectors 155
Backup limitations for Teams site collections 156

Chapter 14 Protect OneDrive data 158

Setting up OneDrive protection with Cohesity Alta SaaS Protection 158
Configure capture scope for OneDrive connectors 160

Chapter 15 Protect Teams chats 162

Setting up Teams chat protection with Cohesity Alta SaaS Protection 162
Configure capture scope for Teams chat connectors 165
Backup limitations for Teams chat 166

Chapter 16 Protect Google Drive data 168

Prerequisites to setup Google Drive protection with Cohesity Alta SaaS Protection 168
Setting up Google Drive protection with Cohesity Alta SaaS Protection 169
Configure Capture scope Google Drive connectors 172
Backup limitations for Google Drive 175
FAQs 176

Chapter 17 Protect Gmail data 177

Prerequisites to setup Gmail protection with Cohesity Alta SaaS Protection 177
Setting up Gmail protection with Cohesity Alta SaaS Protection 178
Configure capture scope for Gmail connectors 180

Chapter 18 Protect Audit logs 184

Add Audit log connectors 184
Audit log connector limitations 185

Chapter 19 Protect Salesforce data and metadata 187

About Salesforce protection 187
Key considerations and prerequisites for adding Salesforce connectors 190
Configure User, Profile, and Connected App for Salesforce 196
Add Salesforce connectors 207
Limitations of Salesforce connectors 211
Salesforce Objects not supported for backup 211

Chapter 20 Protect Entra ID objects 217

Setting up Entra ID protection with Cohesity Alta SaaS Protection 217
Backup and restore limitations for Entra ID 219

Chapter 21 Protect Box data 221

Prerequisites for Box connectors configuration 221
Setting up Box protection with Cohesity Alta SaaS Protection 221
Configure capture scope for Box connector 224
Backup limitations for Box data 225

Chapter 22 Protect Email/Message data 226

Prerequisite for Email/message connector 226
Add Email/Messages file 226

Chapter 23 Configure Retention policies 228

About WORM policies 228
Ingestion WORM policies page 229
Add/edit Ingestion WORM retention policies and guidelines 230
Add/edit At-Rest WORM retention policies 232
Add/edit Deletion policies 234
View deletion history 236
How to edit the policy evaluation interval? 237
How to add a Location filter? 237
How to add a filter? 238

Chapter 24 Perform backups 239

Perform on-demand/ad-hoc backup 239
Video tutorial for connector troubleshooting 241
View backup events 241
About Event suppression 242
Create event suppression rules 242
Viewing backup tasks details 243

Chapter 25 View and share backed-up data 245

Browse backed-up data 245
Share data 245
Remove data sharing 246

Chapter 26 Analytics 247

About analytics 247
Analytics page and refresh behavior 249
Aggregation buckets 251
Gain insights into storage utilization 253

Gain insights into storage utilization for Entra ID and Salesforce connectors 254
Gain insights into blocked activities, most active users, and more 255
Gain insights into data volume (size and item count) on legal hold 257
Gain insights into data volume (size and item count) saved in different Enhanced cases 258
Gain insights into data volume (size and count) under different policies 259
Gain insights into data volume (size and item count) under different Tags 260
Gain insights into data volume (size and item count) under different Tags behaviors 261
Gain insights into storage savings after deduplication and compression 263
Gain insights into data ingestion trends 264

Chapter 27 Perform restores using Administration portal 265

About restore 266
Prerequisites for restore 266
Restore Exchange Online mailboxes 267
Restore SharePoint/OneDrive/Teams Sites and data 272
Restore of OneDrive, Microsoft 365 Group, and Microsoft Teams sites 282
Restore limitations for SharePoint Online 283
Restore Teams chat messages and Teams channel conversations 288
Restore limitations for Teams chat 290
Restore O365 audit logs 290
Restore Box data 290
Restore limitations for Box 292
Restore Google Drive data 292
Overwrite restore behavior for Box/Google Drive data 294
Restore Gmail data 294
About Salesforce Data, Metadata, and CRM Content restore and Sandbox seeding 296
Guidelines for Schema changes in Salesforce organization to prevent restore failures 298
Restore Standard and Custom objects (Structured data restore) 301
Custom Object restore - post processing steps 304

Restore specific Records (Structured data) using Query filters 305
Restore Salesforce CRM Content (Unstructured data restore) 309
Restore Salesforce files/documents in Public/Shared libraries (Unstructured data restore) 310
Limitations of Salesforce Data restore 313
Salesforce Objects not supported for restore 315
Key considerations for Salesforce Metadata restore 322
Restore Salesforce Metadata 323
Limitations of Salesforce Metadata backup and restore 325
About Entra ID (Azure AD) objects and records restore 327
Permissions requirement 327
Best practices to restore Entra ID objects 328
Restore an Entra ID object 328
Restore specific records within Entra ID objects 332
Restore Slack data 336
Restore data to File server 336
Set default restore point 337
Configure Restore all, Restore all versions, Point-in-time, and Specific range restore options 337
Configure email addresses for notifications 338
Downloading an item 338

Chapter 28 Restore dashboard 340

About Restore dashboard 340
Restore job statuses 341
How to cancel a restore job? 342
View the restore events 343

Chapter 29 Install services and utilities 344

About services and utilities 344
Pre-requisites to download and install services and utilities 345
Downloading services and utilities 346
Where to install the services and utilities 346
Installing or upgrading services and utilities 347
Configuring service accounts for services and utilities 348
About the Apps Consent Grant Utility 350
Downloading the Apps Consent Grant Utility 350
Installing or upgrading the Apps Consent Grant Utility 351
Post-installation activities for the Apps Consent Grant Utility 352

Chapter 30 Discovery 353

About eDiscovery/searches 353
Elasticsearch 354
Add search templates 354
Add Discovery cases 355
Perform ad hoc search and add data to Discovery cases 355
View data in Discovery cases 357
Edit Discovery cases 357
DeleteDiscovery cases 358
Assign Discovery cases to users 358

Chapter 31 Configure Tagging policies 359

About the Tagging policy 359
Add Tags 360
Add/edit Tagging policies 361
Adding regular expressions 362
RegEx and query examples for PII detection 363

Chapter 32 Configure Tiering policy 365

About the Tiering policy 365
Storage tiering and full-text search 367
User experience on storage tiering 368
Priority for storage Tiering 368
Add/edit Tiering policies 368

Chapter 33 Auditing 371

Auditing 371

Chapter 34 Manage Stors (Storages) 373

Viewing Stors (Storages) 373
Requesting a new Stor 374
General tab 374
Version control settings 378
Metadata tab 380
Statistical policies tab 381
Location-Mapping tab 381
Backup tab 381
Custodian Groups tab 382
Advanced tab 382
Analytics tab 383

Chapter 1

Introduction to Cohesity Alta SaaS Protection

This chapter includes the following topics:

- About Cohesity Alta SaaS Protection
- Features of Cohesity Alta SaaS Protection
- Architecture of Cohesity Alta SaaS Protection
- Operational workflow
- Extra Data Backup (EDB)

About Cohesity Alta SaaS Protection

Cohesity Alta SaaS Protection is a cloud-based data protection and management solution that is deployed on Microsoft Azure. With Cohesity Alta SaaS Protection, you can protect, analyze, search, and manage data with SaaS applications such as Microsoft 365, Box, Salesforce, Azure AD (Microsoft Entra ID) and so on, regardless of the scale and size of data. It provides granular data management, enterprise-grade security, high performance, and scalability while using the capabilities of Microsoft Azure.

Cohesity Alta SaaS Protection supports complete backup and archiving of the SaaS application data, fast and flexible data recovery, and decoupling of data from the storage layer as well as from the SaaS provider’s platform. It also supports a data management engine that supports eDiscovery, compliance, and data privacy.

Enterprise data protection ensures data security regardless of the company's size. This solution protects against evolving ransomware threats, ensuring data resilience and recovery ability even during attacks. To prevent SharePoint overages, Cohesity Alta SaaS Protection optimizes data usage within SharePoint, efficiently managing

and optimizing data to eliminate overages and significantly enhance overall efficiency.

For licensing details, refer to the following document:

Cohesity Alta SaaS Protection service description

Cohesity Alta SaaS Protection supports backup and recovery of the following SaaS applications:

Introduction to Cohesity Alta SaaS Protection

Table 1-1

SaaS applications	
Microsoft 365	■ Exchange Online mailboxes, folders, messages, and attachments ■ SharePoint Online sites, folders, files, permissions, and metadata ■ OneDrive for Business sites, folders, files, permissions, and metadata ■ Teams site, folders, files, permissions, and metadata ■ Teams messages, meeting recordings, and attachments
Google Workspace	■ Gmail mailboxes, folders, labels, messages, and attachments ■ Google Drive files, folders, permissions, and metadata
Box	Files, folders, permissions, and metadata
Salesforce	Objects, records, files, attachments, and metadata
Microsoft Entra ID	Users, Groups, Application Registrations, and Enterprises Applications

The following user interfaces are available with Cohesity Alta SaaS Protection:

Table 1-2

Applications	Description
For administration	**Administration portal** An Administrator or an authorized user can access the Administration portal using the supported web browser. The Administration portal is used to perform the following activities: ■ Add and manage connectors. ■ Perform ad hoc backups or schedule a backup. ■ Perform restore. ■ Manage user roles and permissions. ■ Create and apply policies such as deletion, retention, and tagging for data management. ■ Download the services and utilities. ■ Review Analytics by visualizing data. ■ Set Tiering policies to reduce cost. ■ Use eDiscovery to perform holds and searches. ■ Monitor the health of the tenant. ■ Access usage details and invoicing history.
	Apart from the Administration portal, Cohesity Alta SaaS Protection provides the following services for the following administrative activities: ■ Export Utility for bulk data restores. ■ **Apps Consent Grant Utility** to grant admin consent for multiple Microsoft 365 apps at once.
For end-users	**End-User portal** A user can access the user portal using a supported web browser with appropriate licenses. The End-User portal is used to perform the following activities: ■ View the data in Cohesity Alta SaaS Protection. ■ Download the data based on permissions. ■ Perform restore based on permission. ■ Share the data with other users.

Features of Cohesity Alta SaaS Protection

Cohesity Alta SaaS Protection includes the following features:

- **Single-tenant environment**
  Uses a single-tenant environment that provides isolated and dedicated cloud resources. It ensures data privacy and offers flexibility to scale the resources to meet specific performance requirements.
- **Enterprise-grade security**

Provides enterprise-grade security through modern authentication, end-to-end encryption, activity auditing, PII detection, and data loss prevention.

- **Autoscaling for connectors**
  This feature enables dynamic scaling of Cohesity Alta SaaS Protection infrastructure resources. As tenant load and data growth from customer workloads increase, the system automatically adjusts resources to ensure optimal performance and scalability.
- **Extra Data Backup (EDB)**
  Cohesity Alta SaaS Protection has the Extra Data Backup (EDB) feature, enabling customers to create an additional, air-gapped copy of their backup data for enhanced redundancy and disaster recovery. This secondary backup is stored in a geographically separated location, ensuring maximum data protection and isolation. Extra Data Backup is a paid service, with costs based on the front-end terabytes (FETB) of data copied.
- **Compliance EDB (Extra Data Backup)**
  The Compliance EDB feature provides the capability to recover your data from EDB (currently, EDB compliance is supported only for S3 on-premises EDB), ensuring data redundancy outside the hosted cloud environment. This feature ensures compliance by enabling secure data storage and retrieval options, giving users control and flexibility over their data management.
- **Single Sign-On (SSO)**
  An additional authentication that provides Single Sign-On functionality by leveraging Microsoft Entra ID for authentication, and includes built-in Role-Based Authorization Controls (RBAC). You can integrate Azure policies to support conditional access, multifactor authentication, and other requirements.
- **Enterprise-scale operations**
  Supports enterprise-scale, which enables the movement of a large amount of data per day. It manages storage containing a large number of objects.
- **End-User portal**
  A user can access the End-User portal using a supported web browser with appropriate licenses. It allows users to independently browse, search, share, and download data. Permissions from respective SaaS applications are synchronized, ensuring that you can only see data to which you have access in the application.
- **Administration portal**
  Supports data management and administration. The portal includes user management, backup configuration, monitoring, administrative restores, policy-based retention and deletion, eDiscovery, and compliance controls.
- **PII and Tagging**

Supports PII and Tagging that integrate with policy-based controls.

- **Disaster recovery**
  Supports a disaster recovery mechanism using data replication to secondary systems such as Azure regions, Amazon S3, and on-premises compliance copies.
- **Multi-regional deployment**
  Supports a multi-regional deployment topology with globally centralized user management to meet in-country data requirements or provide optimal latency.
- **Cost-effective storage Tiering**
  Offers cost-effective storage tiering options to meet different use cases.
- **Analytics**
  Analytics enables you to have insights into the size and volume of data being backed up for your tenant.

Architecture of Cohesity Alta SaaS Protection

The components in the Cohesity Alta SaaS Protection architecture are:

- **Tenant**
  An Azure account established for Cohesity Alta SaaS Protection provides a dedicated single-tenant instance. This setup ensures the segregation of data and supports secure multi-region data storage while adhering to data residency requirements.
- **Hub**
  Each tenant incorporates a single Hub database that contains global configuration details.
- **StorSite**
  Depending on requirements, a Hub may have one or multiple StorSites. While most tenants have a single StorSite, organizations with multiple office locations in different countries may have multiple StorSites aligned with Microsoft Azure regions to enhance scalability. Each StorSite includes at least one app service.
- **Stor**
  A target storage repository located within a StorSite. A StorSite may encompass one or multiple Stors, each featuring two dedicated Blob storages with tiering. The workloads of each tenant are allocated to one or more Stors as necessary. Blob storage supports data deduplication and encryption at rest, with the option for data redundancy through storage replication as preferred by customers.
- **SQL database**

Each tenant connects to a dedicated SQL database, complete with distinct settings for policies, storage redundancy, storage tier, encryption, and metadata.

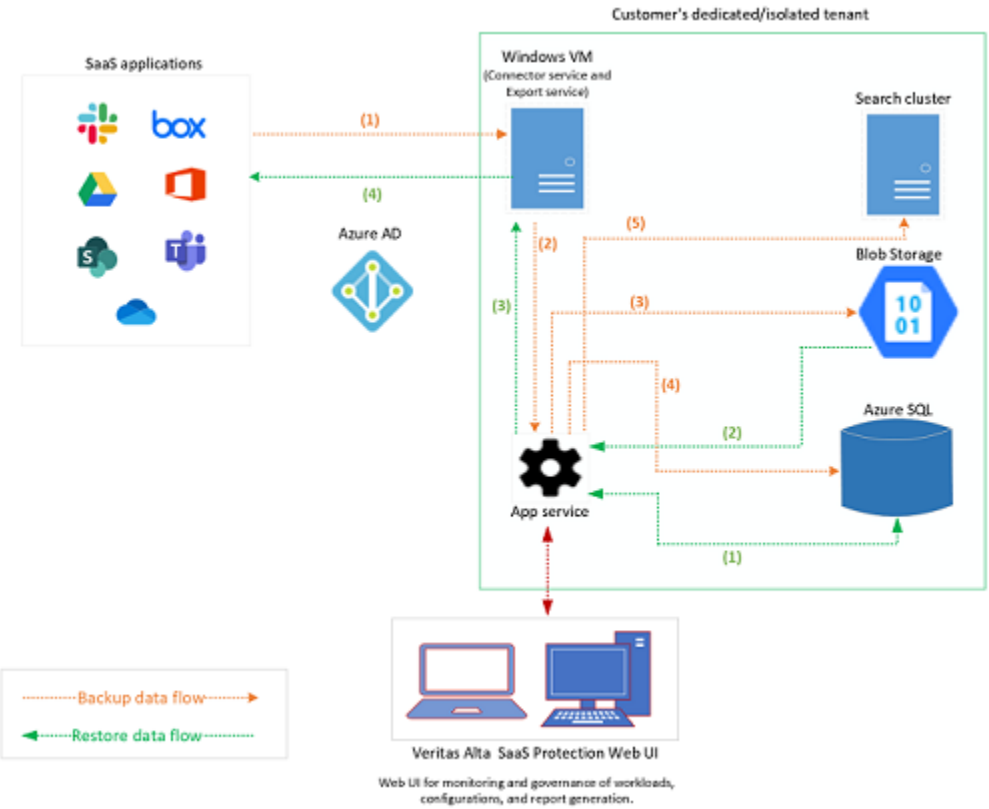
- **App service**
  Each Stor includes at least one App service, facilitating user access to the web UI. Cohesity Alta SaaS Protection offers two web UI alternatives: The Administration portal and the End-User portal.

  The App service component manages access to a Cohesity Alta SaaS Protection tenant and runs various Web jobs to update statistics, track activity, and execute policies. Although the App service does not store data and does not require backup or replication, it is essential for user access and data operations.

  Multiple App service instances can be deployed within a Cohesity Alta SaaS Protection tenant for scalability and high availability. In a geo-redundant configuration with a short recovery time objective (RTO), an App service can be provisioned in secondary regions to serve as a warm standby, supporting active storage accounts in that region.

Cohesity Alta SaaS Protection is integrated with Microsoft Entra ID. Cohesity Alta SaaS Protection supports multifactor authentication, Enterprise Single Sign-On (SSO), Access Control Lists, and granular role-based access control (RBAC).

Workflow for data back up and restore in Cohesity Alta SaaS Protection:



Backup data flow:

1. The required data is fetched by the Connector service installed on the Windows server from SaaS applications.
2. The Connector service establishes communication with the App service to acquire a token, enabling the App service to store data in the Blob Storage. Initially, data is written to the staging area, also referred to as 'Blob storage,' where the App service performs an integrity check before transferring it to the actual Stor.
3. The data is written to the Blob storage, and the App service performs deduplication before writing the data to the Blob storage.
4. The App service updates the database with essential metadata information.
5. The App service signals the preparation of indexes of the backed-up items within the Search Cluster.

Restore data flow:

1. The App service and the database connect to initiate a request for the necessary data.
2. The App service retrieves data from the Blob storage.
3. The data is transferred by the Export service to the target workload.
4. The Export service prepares a job and transfers the data into the SaaS applications according to the specified restore locations.

For additional information on managing Stors,

See "Viewing Stors (Storages)" on page 373.

Cohesity Alta SaaS Protection is bundled with services and utilities as part of the solution. You can download these utilities and services from the Administration portal and configure on the Windows VM (on-premises or in the cloud).

The following services and utilities are available:

- Connector service
- Export service
- Export utilities
- Retrieval service
- Slack administration utility
- Apps consent grant utility

Operational workflow

These are the typical tasks and activities you will perform as part of Cohesity Alta SaaS Protection operations, which can be communicated during the on-boarding process:

Table 1-3

Tasks	Reference links:
1:: Tenant deployment Cohesity will set up your tenant and environment within Cohesity Alta SaaS Protection to get you started.	

Table 1-3 *(continued)*

Tasks	Reference links:
2:: Pre-requisite Perform the pre-requisite activities depending on the workload you have subscribed to protect.	See "Pre-requisites to setup protection for M365" on page 122. See "Prerequisites to setup Google Drive protection with Cohesity Alta SaaS Protection" on page 168. See "Prerequisites to setup Gmail protection with Cohesity Alta SaaS Protection" on page 177. See "Key considerations and prerequisites for adding Salesforce connectors" on page 190. See "Prerequisites for Box connectors configuration" on page 221. See "Prerequisite for Email/message connector" on page 226.
3:: User role assignment ■ **Default role assignment**: (Applicable for Microsoft 365 workload backups) After Azure Active Directory (AD) synchronization, users are initially assigned the Default system role. This grants them access to the End-User portal, where they can search, share, and perform self-restores for their accessible content. ■ **Administrative role assignment**: Assign appropriate administrative roles to users responsible for managing Cohesity Alta SaaS Protection. These roles ensure that users have the required permissions aligned with their business responsibilities.	See "Role-based access control" on page 47.

Table 1-3 *(continued)*

Tasks	Reference links:
4:: Policy creation You are responsible for creating policies that define how data will be managed within Cohesity Alta SaaS Protection. These policies cover backup schedules, retention periods, and more, ensuring that the system aligns with your business and compliance requirements.	See "About WORM policies " on page 228.
5:: Connector creation You will need to create connectors to integrate Cohesity Alta SaaS Protection with your data sources, such as Microsoft 365, Google Drive, and other supported platforms. These connectors facilitate the secure backup of data from these sources into the Cohesity Alta SaaS Protection environment.	■ ■ ■ ■ ■ ■ ■ ■ See "Add Audit log connectors " on page 184. ■ See "Add Salesforce connectors" on page 207. ■ ■ ■ ■ See "Add Email/Messages file" on page 226.
6:: Data backup Once your connectors and policies are configured: ■ Perform secure data backups from connected sources. ■ Cohesity Alta SaaS Protection ensures that critical data is backed up according to your defined policies, preserving it for future restoration need.	See "Perform on-demand/ad-hoc backup" on page 239.

Table 1-3 *(continued)*

Tasks	Reference links:
7:: Data restore In the event of data loss, initiate the restore process through the following options: ■ **Administrator restores**: Restore backed-up data to its original or an alternate location, ensuring business continuity. ■ **End-User Self-Service restores**: End users can restore their own data and share it with others through the End-User portal.	■ See "Restore Exchange Online mailboxes" on page 267. ■ See "Restore SharePoint/OneDrive/Teams Sites and data" on page 272. ■ See "Restore Teams chat messages and Teams channel conversations" on page 288. ■ See "Restore Box data" on page 290. ■ See "Restore Google Drive data" on page 292. ■ See "Restore Gmail data" on page 294. ■ See "About Entra ID (Azure AD) objects and records restore " on page 327. ■ See "About Salesforce Data, Metadata, and CRM Content restore and Sandbox seeding" on page 296.

Extra Data Backup (EDB)

Cohesity Alta SaaS Protection has the Extra Data Backup (EDB) feature, enabling customers to create an additional copy of their backed-up data for enhanced redundancy and disaster recovery. This secondary backup is stored in a geographically separated location, ensuring maximum data protection and isolation. Extra Data Backup is a paid service, with costs based on the front-end terabytes (FETB) of data copied.

EDB is a secure, isolated copy of your SaaS application data, separate from the primary backup. This secondary copy remains inaccessible under normal circumstances and can only be used when necessary for data recovery.

To enable EDB for your environment, contact Cohesity Support.

For more details on supported devices, refer to the following link:

Extra Data Backup Configuration Guide

Cohesity Alta SaaS Protection Extra Data Backup

Pre-requisites

The following are the pre-requisites to configure S3 bucket to support EDB:

Table 1-4

Actions	Options
The options should be selected:	■ **ACL enabled** ■ **Bucket owner preferred**
The check box and the other checkboxes under this section should be cleared:	**Block all public access**

EDB can be configured on a per-Stor-type basis, letting you select specific data for backup. All associated backup data for the selected Stor types will be copied.

EDB supports all the workloads supported by Cohesity Alta SaaS Protection for protection except Salesforce and Entra ID.

When EDB is enabled for a workload, a replica of the data stored in those Stors is copied to the designated target location.

For example, copying all Exchange data would involve replicating all Exchange Stors. Similarly, all Teams chat Stors and site collection Stors would be copied for Teams data.

Compliance EDB

The Compliance EDB feature provides the capability to recover your data from EDB (currently EDB compliance is supported only for S3 on-premises EDB), ensuring data redundancy outside the hosted cloud environment. This feature ensures compliance by enabling secure data storage and retrieval options, giving users control and flexibility over their data management.

To enable EDB for your environment, contact Cohesity Support.

Key pointers:

- Self-service recoverability: You can recover data independently without needing to contact support.
- Setup: You can initiate setup by opening a support ticket.
- Licensing: An EDB license is required to access this feature.

Command line arguments

You can use the following command line argument:

- configFileLocation
  The file path for the configuration file.
  Example: "C:\ComplianceCopyConfigFiles\s3SourceConfig.json"
- agentType

The Corresponding HubStor Type
Example: "S3Bucket_OnPrem"

- earliestModificationTime
  The earliest file modification time needs to be considered for the retrieval.
  Example: "2024-02-01"
  This argument is optional and can be left as: “”
- latestModificationTime
  The latest file modification time needs to be considered for the retrieval.
  Example: "2024-06-03"
  This argument is optional and can be left as: “”
- earliestAccessTime
  The earliest file access time needs to be considered for the retrieval.
  Example: "2024-02-01"
  This argument is optional and can be left as: “”
- latestAccessTime
  The earliest file access time needs to be considered for the retrieval Example: "2024-02-01"
  This argument is optional and can be left as: “”
- earliestCreationTime
  The earliest file creation time needs to be considered for the retrieval.
  Example: "2024-02-01"
  This argument is optional and can be left as: “”
- latestCreationTime
  The earliest file creation time needs to be considered for the retrieval.
  Example: "2024-02-01"
  This argument is optional and can be left as: “”
- storSiteID
  The storSite number where the files should be sourced from Example: "1"
- storID
  The StorID number where the files should be sourced from Example: "2"
- destinationDirectory
  The path to the folder where the files will be housed.
  Example: "C:\MyComplianceCopy\Retrieval\Destination"
- targetLocation
  The ASP Content location where the files should be sourced from. All files and folders beneath this directory will be considered for data retrieval.

- s3TargetLocation
  The target location from the AWS s3 bucket where the files should be sourced from. All files and folders beneath this directory will be considered for data retrieval.

  Note: One of the parameters from targetLocation and s3TargetLocation can be empty or null, if both parameters are given then the priority will be given to s3TargetLocation.

  ---

  1. targetLocation: Copy the path from the ASP Content portal.
  Examples:
  New connector
  New connector\AdeleV@M365x49242125.OnMicrosoft.com
  2. s3TargetLocation: Copy the path from S3 bucket.
  Examples:
  EWSAllUsersVPNSP.Location_7736/admin@vpnsp.onmicrosoft.com.Location_7758/ActiveMailbox.Location_7987/Inbox.Location_8001”
- fileName
  A name similar to the files you want to retrieve.

To run the custom utility

- Cohesity will share the custom utility with you.
- You need to install the custom utility.
- Create a JSON file with the required parameters as follow:
  - InstanceID: A name to identify the application during run time.
  - AccessKeyID: The username / identity key for the application.
  - SecretAccessKey::The password for the application.
  - AWSRegion: The AWS Region associated with your EDB.
  - BucketName; The AWS bucket name associated with your EDB.
  - EndpointURL
  - UseHTTP: Specifies if HTTP should be used.
  - ForcePathStyle
  - IsOnPrem: Specifies if the application is on-premises.
  - Proxy Details:
    Do not include below fields if proxy is not enabled for the Web service or keep the field values as Null.

- ProxyHost: The Proxy Host property for the web service.
  Example: proxy.mycompany.com:8080
- ProxyBypassList: The proxy bypass list.
  Example: localhost;127.0.0.1; *.mycompany.local
- ProxyAuthenticationUserName: Proxy Authentication username.
- ProxyAuthenticationPassword: The decrypted password. Not serialized.

- Once the custom utility is installed, launch the Command Prompt from the C:\Program Files (x86)\HubStor\Custom folder.
- Run the commands with a series of arguments, each separated by a space. Refer to the following examples:

Example - 1:

To get the target location from the Cohesity Alta SaaS Protection Administration portal, go to the **Content** page. Select the required item or folder, click the info *i* icon, go to the **Details** section, and from the **Location** section, copy the path.

```
Hubstor.Utilities.EDBComplianceDataRetriever.exe
configFileLocation="C:\ComplianceCopyConfigFiles\s3SourceConfig.json"
storSiteID="1" storID="2" agentType="S3Bucket_OnPrem"
earliestModificationTime="" latestModificationTime=""
earliestAccessTime="" latestAccessTime="" earliestCreationTime=""
latestCreationTime="" fileName="My File Name"
destinationDirectory="C:\Temp\EDBCompliance Data Retrieval"
targetLocation="Dan NewExchange
Connector\admin@M365x04142374.onmicrosoft.com"
```

Example - 2:

To get the target location from S3, go to the S3 Browser. Click the required bucket, click the **Compliance Store** folder. Browse to the item that needs to be restored, and copy the path starting from the connector name. Do not copy the */* at the end.

```
Hubstor.Utilities.EDBComplianceDataRetriever.exe
configFileLocation="C:\ComplianceCopyConfigFiles\s3SourceConfig.json"
storSiteID="1" storID="2" agentType="S3Bucket_OnPrem"
earliestModificationTime="" latestModificationTime=""
earliestAccessTime="" latestAccessTime="" earliestCreationTime=""
latestCreationTime="" fileName="My File Name"
destinationDirectory="C:\Temp\EDBCompliance Data Retrieval"
targetLocation="" S3TargetLocation =
```

```
"EWSAllUsersVPNSP.Location_7736/admin@vpnsp.onmicrosoft.com.Location_7758/Active
Mailbox.Location_7987/Inbox.Location_8001"
```

C:\Windows\System32\cmd.exe

```
C:\Program Files (x86)\HubStor\Custom>Hubstor.Utilities.EDBComplianceDataRetriever.exe confi
\Documents\New folder\s3SourceConfig.json" storSiteID="1" storID="248" agentType="S3Bucket_C
="" latestModificationTime="" earliestAccessTime="" latestAccessTime="" earliestCreationTime
ame="" destinationDirectory="C:\backup12" targetLocation="" s3TargetLocation="filewpatch.Loc
```

Chapter 2

Cohesity Alta SaaS Protection Copilot (AI chatbot)

This chapter includes the following topics:

- Cohesity Alta SaaS Protection Copilot (AI chatbot)

Cohesity Alta SaaS Protection Copilot (AI chatbot)

By default, this feature is enabled. To disable the feature, navigate to **Administration** > **General settings**. Clear the **Enable Copilot (AI chatbot)** check box.

The knowledge scope of this AI chatbot includes the Admin Guide and knowledge base articles created for this Cohesity Alta SaaS Protection.

The following features are now available:

Table 2-1 Cohesity Alta SaaS Protection available features

Features	Description
Get answers to your questions.	This Cohesity Alta SaaS Protection can help answer questions related to Cohesity Alta SaaS Protection. Alta Copilot generates step-by-step procedures in response to your queries, providing guidance on performing specific tasks. It also includes citations and references to the relevant product documentation for additional details. ■ How do I set up a SharePoint connector or manage existing ones for backups? ■ How do I create or manage retention and deletion policies for my data? ■ How can I set up stubbing and archiving for my SharePoint environments?
Cohesity Alta SaaS Protection conversation history	Cohesity Alta SaaS Protection includes a chat history feature that lets you review past conversations. The chat history is displayed in chronological order and grouped by time. While you can view and reuse the same chat, note that Copilot does not retain memory of previous interactions within that chat. This feature lets you: ■ Access historical conversations. ■ Delete a specific or all conversation history or rename the title of the history. ■ Clear the older chat and start a new conversation. You can also use the thumbs-up or thumbs-down options to let us know whether your question was answered correctly. This feedback helps us improve your experience with Cohesity Alta SaaS Protection.

Chapter 3

Cohesity Alta SaaS Protection Administrator portal (Web UI)

This chapter includes the following topics:

- About Cohesity Alta SaaS Protection Administration portal
- Configure Cohesity Alta SaaS Protection Administration portal
- View upgrade history

About Cohesity Alta SaaS Protection Administration portal

The Administration portal is a web-based portal for administrators and other privileged users that is used to perform backups, perform restores, and other administrative tasks as follows:

- Adding and managing connectors
- Downloading the services and utilities.
- Performing ad hoc backups.
- Scheduling backups.
- Performing restores.
- Managing user roles and permissions.
- Creating and applying policies.

- Performing data searches.

Important: The Cohesity Alta SaaS Protection Administration portal is available in English. The Cohesity Alta SaaS Protection End-User portal is available in English and French.

To access the Administration portal:

You get the Administration portal URL for your tenant in the Welcome email at the time for provisioning. You can access the URL on the supported web browser (Google Chrome and Microsoft Edge). Enter valid credentials to log on. After successful logon, the home page of the portal is displayed.

The customer with a fixed price model and full permissions can see the following modules on the home page:

Table 3-1

Modules	Description
Administration	This option lets you perform the following: ■ Manage storage. See "Viewing Stors (Storages)" on page 373. ■ Manager users and roles. See "Permissions tab" on page 48. ■ Manage connectors. See "What is a connector?" on page 81. ■ Configuring general setting on the Administration portal. See "Configure Cohesity Alta SaaS Protection Administration portal" on page 33. ■ Viewing upgrade history and the corresponding release notes. See "View upgrade history " on page 36. ■ Software download. ■ Configuring auditing. See "Auditing" on page 371.
Analytics	It helps you view the data statistics. See "About analytics " on page 247.
Tiering	It helps you manage tiering policies. See "Add/edit Tiering policies" on page 368.

Table 3-1 *(continued)*

Modules	Description
Retention	It helps you manage retention and deletion policies. See "Add/edit Ingestion WORM retention policies and guidelines" on page 230. See "Add/edit At-Rest WORM retention policies" on page 232. See "Add/edit Deletion policies " on page 234.
Tagging	It helps you manage tagging policies. See "Add/edit Tagging policies " on page 361.
Discovery	It helps you manage searches, Discovery cases, and data under legal hold. See "About eDiscovery/searches" on page 353.
License	It helps you view the license of your tenant.
Content	It helps you perform data restores. See "About restore" on page 266.
System	It helps you monitor overall health of your tenant.

Note: You can see fewer pages and options depending on permissions, the billing model, and enabled SKUs.

Two options are displayed at the upper right corner of the portal; one is the current user's name, and another takes you to the help document of Cohesity Alta SaaS Protection.

The **Help** option opens the Administrator's Guide for Cohesity Alta SaaS Protection. The **knowledge base** link opens the support site, where you can see all the Knowledge Articles for Cohesity Alta SaaS Protection. The **About** option opens the page with details such as the current version and details on the third-party licenses.

Configure Cohesity Alta SaaS Protection Administration portal

Configuring the General settings in the Administration portal involves enabling specific options and settings to suit the tenant's requirements within the portal interface.

To configure General settings of the Administration portal

1. Open a web browser and access the Administration portal URL.

   The home page of the Administration portal is displayed.

2. Click **Administration**.

3. On the left, click **General settings**.

4 Configure the following settings:

Admin Portal settings:

Enable this feature	Click the option to allow the user to set the web portal banner settings. **Note:** Banners are used to notify the portal users about any updates based on the defined notification frequency.
Audit Admin portal page view	Select the check box to enable to audit all applications such as Content, Analytics and all of the Administration portal.
Allow Discovery raw searches	Select the check box to allow the search filter option in the Discovery cases.

End-User Portal settings:

Enable this feature	Click the option to allow the user to set the web portal banner settings. **Note:** Banners are used to notify the portal users about any updates based on the defined notification frequency.
Expire End-User shares by default	Select the check box to share the data only for the number days defined in the **Default share length settings (Days)** option.
Send share invitation emails by default	Select the check box to send a share invite email to users.
Default share length settings (Days)	Enter the number of days. By default, the data is shared for 30 days.
Exclude weekends	Select the check box to exclude weekends from the number of days defined in the **Default share length settings (Days)** option.
Send archive tier notifications emails	Select the check box and enter the domain name in the field next to the check box if you want to send an archive tier notification email to users who belong to the specified domain. The notification emails contain links for accessing the data on the End-User portal.

Remove End User Portal access links	This check box is displayed when the **Send archive tier notification emails** check box is selected. Select the check box if you want to remove the links in the notification email that provide access to the data on the End-User portal.

5 Click **Save**.

View upgrade history

Cohesity Alta SaaS Protection offers an AutoUpgrade feature, facilitating automated tenant upgrades. Once AutoUpgrade is activated for a tenant, a series of email notifications are triggered at specific intervals leading up to the upgrade. These notifications are sent to the technical support team and occur 30, 14, and 2 days before the scheduled upgrade.

An additional email notification is dispatched after an automatic upgrade is successfully completed. This notification includes comprehensive details and release notes regarding the completed upgrade. The Administration portal also allows users to access their upgrade history and gives them the flexibility to reschedule an upcoming upgrade. This rescheduling can be done using the **Schedule an upgrade** Date Picker option, allowing users to choose a date for their next upgrade. You can postpone the upcoming upgrade based on their preferences.

The following components can be upgraded as per the release:

- Connector service
- Export service
- Export utility
- Retrieval service
- Administration portal

The release notes contain the list of fixes and enhancements that are part of the new version.

Click the **Details** pane option to view the details of the selected version. You can click **Download** to download the details in the HTML format.

Chapter 4

Supported SaaS workloads

This chapter includes the following topics:

- Supported SaaS workloads and backup capabilities

Supported SaaS workloads and backup capabilities

Cohesity Alta SaaS Protection supports backup and restore for the following SaaS applications:

- Microsoft 365
  - Exchange Online
  - SharePoint Online
  - Teams sites
  - Teams chats
- Google
  - Google Drive
  - Gmail
- Box
- Salesforce
- Entra ID

Note: A Cohesity Alta SaaS Protection connector is a logical interface that links the source application to backup storage in Cohesity Alta SaaS Protection. You can create and configure connectors for each workload to meet your backup requirements.

:: Exchange Online

The users data in the Exchange Online environment is protected using the Cohesity Alta SaaS Protection Exchange connector with the following features:

- **Backup/restore capability**:
  Granular backup and restore is supported for the following items in the Exchange Online environment:
  - Mailboxes of users, groups, and Teams mailboxes.
  - Public Folders
  - Archive mailboxes
  - Shared mailboxes
  - Contacts and calendars
  - Tasks and notes
  - Mailbox Rules
  - Junk Email and Deleted Items: Junk email and deleted items folders to restore accidentally deleted or wrongly categorized emails.

    Note: The emails in the EWS environment are backed as `.eml` files. Cohesity Alta SaaS Protection receives these .eml files from Exchange, containing the original email as an encrypted attachment and a message body indicating that the email is encrypted. To view these .eml files, they must be downloaded/restored from Cohesity Alta SaaS Protection and opened in Outlook by a user with the necessary permissions.

  - Soft deleted mailboxes (can be configured using the Connector service).
  - Recoverable items folder
  - Public folders
  - Archived mailboxes
    An option to back up archived mailboxes, ensuring that all user data, including archived content, is backed up.
  - Groups created using the Role assigned and Dynamic users options.

  - Microsoft 365 Group and Teams mailboxes.

- **Configuration options:**
  The following configuration options are available for customizing SharePoint backup:
  - Flexible backup options
    Back up all user mailboxes or selectively back up specific mailboxes (granular backup) based on backup requirements.
  - Rolling Mailbox Scope to distribute the backup load across jobs.
    Important: With the 2.32.1 release, this option will not be available for new connectors. For existing connectors, this option will appear as read-only.
  - Alphabetical Mailbox Scope to back up mailboxes based on alphabetical name ranges.
    Important: With the 2.32.1 release, this option will not be available for new connectors. For existing connectors, this option will appear as read-only.
  - Domain-based mailbox backup
    Back up of mailboxes belonging to specific email domains.

:: SharePoint Online

The users data in the SharePoint Online environment is protected using the Cohesity Alta SaaS Protection SharePoint Online connector with the following features:

- **Backup/restore capability**:
  Granular backup and restore is supported for the following items in the SharePoint Online environment:
  - Documents
  - List items
  - Versions
  - Site pages
  - Site collections
  - Sub-site settings
  - Site and sub-site columns
  - Site and sub-site content types
  - List settings
  - List columns
  - List content types

- Permission objects such as groups
- Role definitions
- Role assignments
- See "Supported and unsupported SharePoint Objects, Properties, Settings, and Types for backup and restore" on page 144.
- See "Supported Sites and List templates for backup and restore" on page 146.
- See "Supported Sites and List templates for backup and restore" on page 146.

Configuration options:

The following configuration options are available for customizing SharePoint backup:

- **Custom backup policy**
  Define specific data types, versions, permissions, columns, and content types to back up.
- **Delete policy**
  Define a Delete policy to manage storage by removing unnecessary items from the source SharePoint Online environment while retaining backups in Cohesity Alta SaaS Protection.
  See "Configure Delete policy for SharePoint Online and guidelines" on page 95.
- **Stubbing policy**
  Define a Stubbing policy to replace original items with stubs (shortcuts) in the SharePoint Online environment, which helps reduce storage usage while maintaining access to data.

:: OneDrive

The users data in the OneDrive environment is protected using the Cohesity Alta SaaS Protection OneDrive connector with the following features:

- **Backup/restore capabilities**:
  The OneDrive for Business connector is used to back up the users' My Sites or OneDrive for Business data. It includes the documents and other important files in the user's OneDrive account, apart from other SharePoint data in the user's OneDrive site.
  - **Files and Documents**: All files and documents stored in the user's OneDrive account, including documents, spreadsheets, presentations, images, videos, and any other file types.
  - **Folders and Folder Structures**: Folder hierarchy and structure.
  - **Shared Files and Folders**: Shared files or folders.

- **Version History**: Version history of files.
- **Metadata and File Properties**: Metadata associated with files, such as file names, creation dates, modification dates, and other custom properties.
- **Permissions and Sharing Settings**: Permissions and sharing settings applied to files and folders, including user access rights, and permissions inheritance.

:: Teams sites

The users data in the **Teams, its private channels, and Microsoft 365 groups** is protected using the Cohesity Alta SaaS Protection Teams site collection connector.

:: Teams chat

You can protect the following data in the Team chat environment using the Cohesity Alta SaaS Protection Teams chat connector:

- **Backup/restore capabilities**:
  - Chat conversations: All chat conversations that occur within the Teams chat environment, including one-on-one chats and group chats.
  - Media files: Media files that are shared within Teams chat, such as images, videos, and audio files.
  - Emojis, GIFs, and Stickers: Links, emojis, GIFs, stickers, or other visual element.
  - Chat history: Chat history for each user.
  - **Configuration options**:
    The following configuration options are available for customizing backup:
- An option to back up one-on-one and group chat data for all users.
- An option to back up one-on-one and group chat data for specific users.
- An option to back up all chats in Teams channels.
- An option to limit the backup to a specific number of days.

:: Google Drive

You can protect the users data in Google Drive environment using the Cohesity Alta SaaS Protection Google Drive connector.

- **Backup/restore capability of the GoogleDrive connector**:
  You can back up the following data in the Google Drive environment:

- **Files and documents**: All files and documents that are stored in Google Drive, including documents, spreadsheets, presentations, images, videos, and any other file types.
- User drives and Shared drives: Drives dedicated to each user and common shared Drives.
- **Version history**: Version history of files.
- **Deleted files**: Deleted files.
- **Metadata and file properties**: Metadata and properties, such as owner information, last modified date, and custom metadata fields associated with Google Drive.

- **Configuration options:**
  The following configuration options are available for customizing backup:
  - An option to back up all or specific users' Google Drive data.
  - An option to include or exclude deleted items in the backup.
  - An option to include or exclude the permissions on the items.
  - An option to back up Shared drives.

:: Gmail

You can protect the users data in the Gmail environment using the Cohesity Alta SaaS Protection Gmail connector.

- **Backup/restore capability of Gmail connector**:
  Cohesity Alta SaaS Protection supports the backup of the following Gmail data:
  - **Emails**: All emails in the Gmail account, including inbox messages, sent items, drafts, and archived emails.
  - **Attachments**: Attachments associated with emails.
  - **Labels and Folders**: Labels and folders.
  - **Deleted Emails**: Deleted emails.
  - **Configuration options**:
    The following configuration options are available for customizing backup:
    - An option to back up all or specific users' data.
    - An option to exclude certain users from the backup by adding their email addresses to the excluded users list.
    - An option to include or exclude deleted items and the items in the Spam folder.

:: Entra ID

You can protect the data in the Entra ID environment using the Cohesity Alta SaaS Protection Entra ID connector.

- **Backup/restore capabilities of Entra ID connector**:
  - **Users**
    It includes backing up the user-related data such as profiles, settings, permissions, and other user-specific information.
  - **Groups**
    It includes backing up the structure, memberships, and settings associated with the groups.
  - **Application Registrations**
    It includes backing up the configurations, settings, and information associated with applications registered within the Entra ID environment.
  - **Enterprises Applications**
    It includes backing up the configurations, settings, and data associated with enterprise-level applications registered and used within the Entra ID environment.

:: Box

You can protect the users data in the Box environment using the Cohesity Alta SaaS Protection Box connector.

- **Backup/restore capabilities of Box connector**:
  - **Files and folders**
    - All files and folders for all users, or a set of specified users, including documents, spreadsheets, presentations, images, videos, and other file types.
    - All folders and files shared with the user being processed. For instance, all data accessible to a user is backed up in the context of that user. If the same folder is shared with ten users, it is backed up ten times (once per user). Deduplication ensures that only one physical copy is stored.
  - **Version history**
    The version history of files, including all previous revisions and versions that have been trashed.
  - **Access control**
    Set the Access Control List (ACL) for backed-up content to the user whose account the content belongs to. Similar to O365 mailboxes and OneDrive for Business, existing ACLs are ignored, and a specific user's ACL is applied.

- **Metadata**
  All tags applied to files.
- **Notes**
  Notes for collaborative note-taking. The raw Boxnote file is backed up and can be restored properly.
- **Deletion policy**
  Delete file versions and files that match the deletion policy. If the last version of a file is deleted, the file is removed. An option to purge deleted content (bypassing the Box trash) is available.
- **Restore of folders and files back to Box**
  - Missing files can be restored with their entire version history.
  - Existing files will have only the latest version restored from the backup and made the current version.

:: Salesforce

This data in the Salesforce environment is protected using the Cohesity Alta SaaS Protection Salesforce connector. It supports the backup and restore of the following:

- Data
- File/attachments/Salesforce CRM
- Metadata

Chapter 5

Workflow to protect data using Cohesity Alta SaaS Protection

This chapter includes the following topics:

- Workflow to protect data using Cohesity Alta SaaS Protection
- Know your subscription details

Workflow to protect data using Cohesity Alta SaaS Protection

Cohesity Alta SaaS Protection enables the backup and restore of data from various SaaS applications, including Microsoft 365, Box, Salesforce, and Azure AD (Microsoft Entra ID). To protect your SaaS applications included in your subscription, follow these steps:

- **Verify your subscription details.**
  Ensure that you understand the details of your Cohesity Alta SaaS Protection subscription.
  See "Know your subscription details" on page 46.
- **Complete the prerequisites for each SaaS application.**
  Before configuring backups, ensure that all necessary prerequisites are met for each application.
- **Create and configure connectors.**
  Set up Cohesity Alta SaaS Protection connectors for each SaaS application that requires protection.

See "What is a connector?" on page 81.

Note: Connectors act as a logical interface between the source SaaS application and Cohesity Alta SaaS Protection storage. You can create one or multiple connectors for each workload based on your backup requirements.

- **Set up data retention policies.**.
  Define retention policies to manage how long data is stored and protected.
  See "Add/edit Ingestion WORM retention policies and guidelines" on page 230.
- **Run an initial backup.**
  Perform an initial backup to copy data from the source SaaS applications to Cohesity Alta SaaS Protection storage.
  See "Perform on-demand/ad-hoc backup" on page 239.
- **Restore data whenever required from the backup.**
  See "About restore" on page 266.

Know your subscription details

Before starting with data protection activity, go to the **License** page to know your subscription details. On the **License** page you can see the following details:

- License package: Enterprise, Enterprise Plus, or Enterprise Elite
- License renewal type: Auto or manual
- License activation date
- License renewal date

The available features are highlighted in the respective column of the selected license package.

SKU (Stock Keeping Units) subscription

In addition to the core features, the user must subscribe for the required SKUs (Stock Keeping Units). SKUs are the workloads that the customer wants to protect, for example, Microsoft O365, Google Drive, Teams chat, and so on. The SKU section displays the storage(in Terabytes, which is allocated to backup per user or per workload (Google Drive, Teams Chat, and so on.)

License renewal

The license renewal date either auto renews by itself (License renewal type = Auto), or the customer needs to contact Cohesity Support to renew the license manually (License renewal type = manual).

Chapter 6

Manage users and roles

This chapter includes the following topics:

- Role-based access control
- Permissions tab

Role-based access control

Role-based access control (RBAC) in the Cohesity Alta SaaS Protection environment enables you to manage resource access by assigning roles to individual users. Resources include backed-up content, connectors, policies, and more in this context. The roles define users' access to these resources, with permissions governed by the assigned roles. RBAC allows for the customization of roles to meet specific business needs. Roles can be modified or deleted as requirements change, ensuring that only authorized users can access them. Users within the same group inherit the assigned role, enabling them to perform the same operations on the resource.

After Active Directory (AD) synchronization with your environment, all users and groups become recognized by Cohesity Alta SaaS Protection. These users are displayed on the **Users and groups** page in the Cohesity Alta SaaS Protection Administration portal. The users synchronized from the customer's AD are classified as **internal users**, while those added directly through Cohesity Alta SaaS Protection and outside the customer's domains and the users who are deleted from your AD are referred to as **external users**. Both the internal and external users are assigned the **Default** system role, which provides access to the End-User portal. This Default role grants permissions to search, share, and perform self-restores for content they have access to.

Permissions tab

Cohesity Alta SaaS Protection offers the capability to implement role-based access control (RBAC) for its tenants. RBAC lets you grant users access and permissions according to their specific organizational roles.

The following table describes the permissions in Cohesity Alta SaaS Protection.

Table 6-1 General settings permissions

General settings	Description
Access all items	It permits the user to access and restore all content of the tenant. Also, by selecting the following respective checkboxes, you can prevent the user from sharing, downloading, restoring, and restoring to an alternative location. ■ **Prevent administrative sharing**. ■ **Prevent Item Preview and Download**. ■ **Prevent restore**. ■ **Prevent restore outside of original location**.
Full admin	It permits the user with all permissions except Access All Items, Add Content, and API Impersonation. To mitigate the risks associated with the Full Admin account, provision this account only on-demand to prevent account sharing.
Add content	The assigned user can add new content to the tenant, typically the Service account.
View only	It permits the user to sign in to the Administration portal without the ability to add, modify, or delete anything.
Delete content	It permits the user to delete backed-up items.

Table 6-2 End-User permissions

End-User settings	Description
End-User SharePoint stubbing restore	It permits an end-user to restore a stubbed item by clicking on it using the End-User portal.
End-User retrieval and download	It permits an end-user to download a stubbed item by clicking on it using the End-User portal.
End-user portal	It permits an end-user to perform the following action on the End-User portal: ■ Search for the required item. ■ Share items internally and externally. ■ Restore the items.

Table 6-3 Administration portal permissions

Administration portal settings	Description
Administration App	It permits the user to sign in to the Administration portal. You can select the following checkboxes for the permissions you want to grant the user. ■ **Manage permissions**: It permits the user to manage permission and roles for other users. ■ **Provisioning**: It permits the user to perform the initial provisioning operations (used by the Cohesity Alta SaaS Protection team only). ■ **View auditing**: It permits the user to access the **Auditing** module and enable auditing as required. ■ **Manage connectors**: It permits the user to add connectors. Important: A user who is a member of a Custodian group should not be assigned this permission.

Table 6-3 Administration portal permissions *(continued)*

Administration portal settings	Description
Manage Scope	It permits the user to view and manage Scopes. ■ If a user is added to a Scope and does not have Managed Scope permission, then the user can only see the connectors that are part of the Scope to which the user is added. ■ If the user is assigned with the Managed Scope permission (it does not matter if the user has Scopes), then the user can see all connectors, including those created using a Scope.
Analytics App	It permits the user to access the **Analytics** module.
Tagging App	It permits the user to access the **Tagging** module.
Discovery app	It permits the user to access the Discovery module. You can select the following checkboxes for the permissions you want to grant the user: ■ **Create cases**: It permits a user to create Discovery cases. ■ **All cases full admin**: It permits a user to view and manage all Discovery cases with full rights.
Retention App	It permits the user to access the **Retention** module.
License App	It permits the user to access the **License** module.
System App	It permits the user to access the **System** module.
Chargeback App	It permits the user to access the **Chargeback** module.
Storage Tiering App	It permits the user to access the **Tiering** module.

Table 6-3 Administration portal permissions *(continued)*

Administration portal settings	Description
Monitoring App	It permits the user to view the **Monitoring** module.

Table 6-4 API settings

API settings	Description
API	It permits the user to access a wide range of general API. This permission is required for all Service accounts.
API Blobless Archive	It permits the user to allow the Connector service to operate with the Blobless Archive option on a connector. It is advisable to grant and use this permission solely in a drive-shipping scenario.
API Impersonation	It permits the user to impersonate another user by the API.

The **Permissions** tab lets you manage user access and roles, with options for user and group management, roles administration, managing unrecognized and external users.

Users and groups page

The **Users and groups** page lets you add, view, and manage user details, export user lists, and configure permissions.

See "Permissions tab" on page 48.

You can perform the following actions:

Table 6-5

Actions	Description
To see existing users.	Use the **View all users and groups** option.
To search for a specific user.	Use the **Refine search** option for complex queries.
To start the user creation process.	Click **New**.

When you click the **View all users and groups** option, you can perform the following:

Table 6-6

To see existing users.	Use the **View all users and groups** option.
To search for a specific user.	Use the **Refine search** option for complex queries.
To start the user creation process.	Click **New**.
To export the list to CSV.	Click **Export**.
To edit the user's details.	Click the name of the user.
To view the user's details.	Click within the row of the user.

To assign permissions to the user, follow the procedure outlined on this page or watch the video tutorial below.

http://video.symantec.com/services/player/bcpid292374537001?bckey=AQ~~,AAAABuIiy9k~,I8Bhas-Vwr9zYL9V36WFi86fR_NoePscn&bctid=6362510937112

Video tutorial to assign permissions

You can add users to Cohesity Alta SaaS Protection and assign roles to the users. You can use the following procedure to add users.

To add users and assign permissions

1. Access the Administration portal.
2. Click **Administration**.
3. On the left, expand **Permissions** and click **Users and groups**.
4. Click **New User**.
5. On the **New User** page, do the following:
   - Enter a name for the user.
   - Toggle the **State** option to enable the user.
   - In the **Identifier** field, enter the Microsoft email address of the user.
   - Click **Manage permissions**.
   - On the **Manage permission** page, select the required permission, and then click **Assign**.

See "Permissions tab" on page 48.

- Click **+ Assign permissions**.
- On the **Assign permissions** page, select the required Discovery case from the dropdown list, and provide the required permission on the selected case and click **Assign**.
- Select the required roles for the user from the **Roles** dropdown list.
- Assign the following permissions as required:

Stor Admin permissions	Enabling this permission allows Stor Admins to manage settings and policies for assigned Stors only. They can only manage Stors within this scope. This permission does not affect users' ability to browse or search content. To allow this permission to the user: ■ Click **Enable this feature**. ■ From the **Select one or more Stors**, click the required Stors.
Custodian Group Admin permissions	To allow this permission to the user: ■ Click **Enable this feature**. ■ From the **Select one or more Custodian Groups**, click the required Stors.
Location permissions	Enabling Location permissions allows users to manage content only within assigned locations. To allow this permission to the user: ■ Click **Enable this feature**. ■ Click **Add locations**. ■ On the **Select locations** page, select the locations to be assigned for the users, and click **Select**.

- Click **Save**.

Roles page

The **Roles** page lets you add, manage, and assign roles, allowing you control permissions and access across your tenant.

On the **Roles** page, you can perform the following actions:

Table 6-7

Actions	Description
To see existing roles and their permissions.	
To start the role creation process.	Click **New Role**.
To search for a specific role.	Enter the name of the role in the **Filter by name** field.
To manage role.	Click within the row of the role and can perform the following actions: ■ View the details of the role. ■ Click **Copy** to duplicate the existing role. ■ Click **Delete** to remove the role.

A role is a collection of permissions that can be assigned to a user or a group of users. You can use the following procedure to add roles.

To add roles

1. Access the Administration portal.
2. Click **Administration**.
3. On the left, expand **Permissions** and click **Roles**.
4. Click **New Role**.
5. On the **New Role** page, do the following:
   - Enter a name for the role.
   - Click **Manage permissions**.
   - On the **Manage permission** page, select the required permission, and then click **Assign**. See "Permissions tab" on page 48.
   - Click **+ Assign permissions**.
   - On the **Assign permissions** page, select the required Discovery case from the dropdown list, and provide the required permission on the selected case and click **Assign**.
   - Click **Save**.

Unrecognized users page

Cohesity Alta SaaS Protection performs a data-level security check for a retrieval request. For this verification, Cohesity Alta SaaS Protection must have details of the user and verify it against the permissions on the requested item. The user must

have domain accounts, and the accounts must be synchronized with the Active Directory.

The user must be in the Access Control List (ACL) for authorization to succeed. If the user is not in the Microsoft Entra ID, then the user cannot open a stubbed item because of an authorization error. If you want to allow any of the users, select the associated check box of the user and then click **Allowlist users**.

Settings page

You can globally allow or remove the ability for external users to authenticate even when content has been shared with them. Enabling this setting allows all external users to authenticate and access shared content in Cohesity Alta SaaS Protection.

When the Only permit external full administrator users to authenticate option is enabled, only external users with Full Admin permissions can authenticate. This setting is disabled by default, and users with Full Admin permissions must enable it to authenticate.

Chapter 7

API permissions

This chapter includes the following topics:

- API permissions for Microsoft 365 workloads
- API permissions for Gmail and Google Drive
- System and API permissions for Salesforce
- API permissions for Entra ID
- App permissions of Web App

API permissions for Microsoft 365 workloads

If you use the Microsoft 365 App Registrations mode to configure Microsoft 365 connectors, such as Exchange, SharePoint, Teams Site, OneDrive, and Teams Chat, Cohesity Alta SaaS Protection requires specific permissions to back up and restore content at the source location. A single app is created for the Microsoft 365 tenant for all the Microsoft 365 workloads. You will need to grant consent for this app, ensuring that it has the following permissions:

Table 7-1

Microsoft 365 workloads	Claim names	Permissions	Description by Microsoft	User by Cohesity Alta SaaS Protection...
Exchange Web Services API access for Exchange.	`MailboxSettings.Read`	Read all user mailbox settings.	Allows the app to read user's mailbox settings without a signed-in user. Does not include permission to send mail.	To read mailbox type when using the Graph Management API mode.
	`Group.ReadWrite.All`	Read and write all groups.	Allows the app to create groups, read all group properties and memberships, update group properties and memberships, and delete groups. Also allows the app to read and write conversations. All of these operations can be performed by the app without a signed-in user.	To add impersonation accounts as members to Microsoft 365 Groups/Teams to back up and restore their mailboxes in the Graph Management API mode.
	`Directory.Read.All`	Read directory data.	Allows the app to read data in your organization's directory, such as users, groups and apps, without a signed-in user.	To fetch a list of users within a tenant and obtain a list of mailboxes using the Graph Management API mode.
	`Reports.Read.All`	Read all usage reports.		

Table 7-1 *(continued)*

Microsoft 365 workloads	Claim names	Permissions	Description by Microsoft	User by Cohesity Alta SaaS Protection...
			Allows an app to read all service usage reports without a signed-in user. Services that provide usage reports include Office 365 and Azure Active Directory.	To get the Exchange growth report from Exchange Online.
	`RoleManagement.ReadWrite.Directory`	Read and write role management data for Microsoft Entra ID.	Allows the app to read and manage the role-based access control (RBAC) settings for your company's directory, without a signed-in user. This includes instantiating directory roles and managing directory role membership, and reading directory role templates, directory roles and memberships.	To add impersonation accounts as administrators to role-assigned Microsoft 365 groups to backup and restore their mailboxes using Graph Management API mode.

Table 7-1 *(continued)*

Microsoft 365 workloads	Claim names	Permissions	Description by Microsoft	User by Cohesity Alta SaaS Protection...
Application permissions for Exchange	full_access_as_app	Use Exchange Web Services with full access to all mailboxes.	Allows the app to have full access by Exchange Web Services to all mailboxes without a signed-in user.	To backup/ and restore data from all types of mailboxes. No other granular permissions are provided by Microsoft for Exchange Web Services.
	Exchange.ManageAsApp	Manage Exchange as an application.	Allows the app to manage the organization's Exchange environment without any user interaction. It includes mailboxes, groups, and other configuration objects. To enable management actions, an admin must assign the appropriate roles directly to the app.	To allow Exchange Online PowerShell access for the following operations when the PowerShell Management API mode is used: ■ Gather a list of mailboxes and their details. ■ Add impersonation accounts to Microsoft 365 Group/Teams mailboxes. ■ Get permissions assigned to mailboxes to capture ACLs.

Table 7-1 *(continued)*

Microsoft 365 workloads	Claim names	Permissions	Description by Microsoft	User by Cohesity Alta SaaS Protection...
Microsoft Graphs API permissions for SharePoint/Teams Site/OneDrive.	`Sites.ReadWrite.All`	Read and write items in all site collections.	Allows the app to create, read, update, and delete documents and list items in all site collections without a signed in user.	To fetch list items from lists in SharePoint sites/Teams sites and One Drives during incremental backups.
	`Directory.Read.All`	Read directory data.	Allows the app to read data in your organization's directory, such as users, groups and apps, without a signed-in user.	To fetch channel information for backup and restore of Teams Wikis.
	`Reports.Read.All`	Read all usage reports.	Allows an app to read all service usage reports without a signed-in user. Services that provide usage reports include Office 365 and Azure Active Directory.	To get a SharePoint growth report from SharePoint Online.
	`User.Read.All`	Read all user's full profiles.	Allows the app to read user profiles without a signed in user.	To fetch owners information for Team Sites. **Note:** This is required only with Modern OAuth authentication mode.

Table 7-1 *(continued)*

Microsoft 365 workloads	Claim names	Permissions	Description by Microsoft	User by Cohesity Alta SaaS Protection...
CSOM and PowerShell access for SharePoint Teams OneDrive	TermStore.ReadWrite.All	Read and write managed metadata.	Allows the app to write enterprise-managed metadata and to read basic site info without a signed-in user.	To backup and restore managed metadata for SharePoint list items.
	Sites.Manage.All	Read and write items and lists in all site collections.	Allows the app to read, create, update, and delete document libraries and lists in all site collections without a signed in user.	To create SharePoint lists during restore.
	Sites.ReadWrite.All	Read and write items in all site collections.	Allows the app to create, read, update, and delete documents and list items in all site collections without a signed in user.	To backup, restore, and stub list items SharePoint sites/Teams sites and One Drives.
	Sites.FullControl.All	Have full control of all site collections.	Allows the app to have full control of all site collections without a signed-in user.	To backup and restore role assignments of objects in SharePoint sites/Teams sites and One Drives Capture ACLs for various SharePoint objects.

Table 7-1 *(continued)*

Microsoft 365 workloads	Claim names	Permissions	Description by Microsoft	User by Cohesity Alta SaaS Protection...
Microsoft Graphs API permissions for Teams Chat.	`ChannelMessage.Send` (Delegated Permissions)	Send channel messages.	Allows an app to send channel messages in Microsoft Teams, on behalf of the signed-in user.	To restore channel messages back to the destination channel. (User impersonated as channel member.)
	`ChatMessage.Send` (Delegated Permissions)	Send user chat messages.	Allows an app to send one-to-one and group chat messages in Microsoft Teams, on behalf of the signed-in user.	To restore chat messages back to the destination chat. (User impersonated as a chat member.)
	`ChatMember.ReadWrite.All`	Add and remove members from all chats.	Add and remove members from all chats, without a signed-in user.	To retrieve the members of a chat, and during the restore process, add a member to the chat. This added member is used on behalf of that user for further chat message restoration.
	`Directory.Read.All`	Read directory data.	Allows the app to read data in your organization's directory, such as users, groups and apps, without a signed-in user.	To get a list of users whose chats need to be backed up in a tenant to be backed up.

Table 7-1 *(continued)*

Microsoft 365 workloads	Claim names	Permissions	Description by Microsoft	User by Cohesity Alta SaaS Protection...
	`TeamMember.ReadWrite.All`	Add and remove members.	Add and remove members from all teams, without a signed-in user. Also allows changing a team member's role, for example from owner to non-owner.	To add a member to Team, required during restore of message for public channels.
	`Chat.Read.All`	Read all chat messages.	Allows the app to read all 1-to-1 or group chat messages in Microsoft Teams.	To read chat messages during backup using Microsoft Teams Export API. Also used to get information like chat name.
	`ChannelMember.ReadWrite.All`	Add and remove members from all channels.	Add and remove members from all channels, without a signed-in user. Also allows changing a member's role, for example from owner to non-owner.	To add member to channel during restore of message for private channels.
	`ChannelMessage.Read.All`	Read channel messages.	Allows the app to read all channel messages in Microsoft Teams.	To read channel messages during backup using Microsoft Teams Export API.

Table 7-1 *(continued)*

Microsoft 365 workloads	Claim names	Permissions	Description by Microsoft	User by Cohesity Alta SaaS Protection...
Application permission for Teams Chat	full_access_as_app	Use Exchange Web Services with full access to all mailboxes.	Allows the app to have full access by Exchange Web Services to all mailboxes without a signed-in user.	To back up group chats or Teams posts, fetch data from User or Teams mailboxes by reading Teams Message data. The process is not applicable when using the Export API for backup.

Note: If you are adding Exchange connectors using the management API as PowerShell with the Application registration as authentication, you must assign the following roles to the applications.

You must use the Connector service to create any connector using the management API as PowerShell, as the PowerShell management API authentication is not yet supported on the Administration portal. In case you have no access to the Connector service, contact the Cohesity Support team.

API permissions for Gmail and Google Drive

Cohesity Alta SaaS Protection requires API permissions on the target Google Drive and Gmail environment to backup and restore its data:

Table 7-2

API name	Requested scope	Used by Cohesity Alta SaaS Protection:	Description by Google
Directory API	https://www.googleapis.com/auth/admin.directory.user.readonly	To enumerate the organization's users and discover users of Google Drives and Gmail mailboxes.	Scope for only retrieving users or user aliases.

Table 7-2 *(continued)*

API name	Requested scope	Used by Cohesity Alta SaaS Protection:	Description by Google
Directory API	https://www.googleapis.com/auth/admin.directory.group.member.readonly	To get the list of members/users present in the group to verify if the user is part of the group. If the Shared drive admin is in the group then using this scope you can get one of the users from the group and generate a token to backup the Shared drive.	Scope for only retrieving users/members presents in the group.
Drive API	https://www.googleapis.com/auth/drive	To back up and restore Google Drive content.	View and manage all of your Drive files.
Gmail API	https://www.googleapis.com/auth/gmail.readonly	To back up Gmail content.	Read all (Gmail) resources and their metadata.
Gmail API	https://www.googleapis.com/auth/gmail.modify	To restore Gmail content.	All read/write operations except immediate, permanent deletion of threads and messages, bypassing Trash.

System and API permissions for Salesforce

To enable Salesforce protection in Cohesity Alta SaaS Protection, a dedicated 'ASP Backup Admin' user must be created by cloning the 'Salesforce System Administrator' profile. This is the recommended approach to ensure comprehensive protection of the Salesforce organization. The 'ASP Backup Admin' user must be assigned a Salesforce license, as Cohesity Alta SaaS Protection does not currently support the Salesforce API Integration License, which has limited access to objects and features.

If an organization's security policies prohibit cloning the 'System Administrator' profile, a set of required permissions can be assigned to a permission set linked to the 'ASP Backup Admin' user created with a Standard user profile. It is strongly recommended to enable all the permissions listed here. If permission(s) are skipped, Cohesity will assume that customer fully understands its implications of the same and may not be able to help with issues arising out of such exclusions.

When using the Permission Set based approach to assign permissions, the ASP Backup Admin user must be assigned the Permission Set containing all the permissions listed herein before assigning the user to the Connected App created for Cohesity Alta SaaS Protection. In this case, instead of using System Admin

Profile, use a Standard User profile. Refer to the KB article for Connected App creation, Setting up a Connected App in Salesforce for use by Cohesity Alta SaaS Protection. You need to assign the new Permission Set to the 'ASP Backup Admin' user instead of creating the user using 'System Administrator' profile. and provide the following:

- Object permissions: 'Modify All' and 'Create' for all objects in the Salesforce organization (Standard and Custom).
- Field permissions: 'Read Access' and 'Edit Access' for all fields in all objects (Standard and Custom).
- Record Type permissions: 'Read' and 'Edit' access for all record types across all objects (Standard and Custom).

Ensure that all necessary feature licenses (for AppExchange products installed, if any) and feature PermissionSets are also assigned to the user.

Some permissions, such as 'Modify All Data,' will automatically enable other permissions. Additionally, other permissions not listed here may also be auto-enabled and must remain active for Cohesity Alta SaaS Protection to function properly.

Table 7-3

Permissions	Data/Metadata	Salesforce description	Used by Cohesity Alta SaaS Protection for
System Permissions			
Access Activities.	Data	Access tasks, events, calendar, and email.	Protection (backup and restore) of Tasks, Events, Calendar, and Email.
Access Libraries.	Data	Access libraries.	Protection of Libraries.
Apex REST Services	Data	Allow access to Apex REST services.	Access to Salesforce APIs
API Enabled.	Data and Metadata	Access any Salesforce.com API.	To access Salesforce APIs for backup and restore of Data and Metadata.
Assign Topics.	Data	Assign existing topics to feed items. Remove topics from feed items.	Restore of FeedItem (while assigning a topic to FeedItem)

Table 7-3 *(continued)*

Permissions	Data/Metadata	Salesforce description	Used by Cohesity Alta SaaS Protection for
Author Apex.	Metadata	Create Apex classes and triggers.	Restore of Apex classes and Triggers.
Change Dashboard Colors.	Metadata	Choose a dashboard color theme and palette.	Restore of Dashboards.
Chatter Internal User.	Data	Use all Chatter features.	Protection of Chatter Objects.
Create and Own New Chatter Groups.	Data	Create and own new Chatter groups.	Restore of Chatter Groups (CollationGroup Standard object).
Create Content Deliveries.	Data	Create content delivery links to share files that aren't managed by a library. To let a user create content deliveries for files in a library, enable Deliver Content for that user in the library.	Protection of Salesforce Orgs where the Content Delivery feature is enabled. Restore of public link Field for the Document/Attachment requires this.
Create Folders for Lightning Email Templates.	Metadata	Create Folders for Lightning Email Templates.	Restore of Email Template (in Folder).
Create Public Links.	Data	Let users create links to share files externally. Unlike content deliveries, public links can't be password protected. To let a user create links to files in a library, enable Deliver Content for that user in the library.	Restore of Public Links of Documents / Attachments / Files.

Table 7-3 *(continued)*

Permissions	Data/Metadata	Salesforce description	Used by Cohesity Alta SaaS Protection for
Create Topics.	Data	Create new topics by assigning them to feed items.	Restore of FeedItem (while assigning a topic to FeedItem).
Customize Application.	Metadata	Customize the organization using App Setup menu options.	'Required for 'Connected App' backup. Restore of various Metadata types, for example Custom Fields, Page Layout, and so on.
Edit HTML Templates.	Metadata	Edit Classic HTML Email Templates.	Restore of Email Templates.
Edit Read-Only Fields.	Data	Edit fields that are read only due to page layouts or field-level security.	Restore values back into some fields that are read-only due to page layout or field-level security.
Edit Tasks.	Data	Create, edit, and delete tasks.	Restore of Tasks.
Edit Topics.	Data	Edit topic names and descriptions.	Restore of Topics.
Manage All Private Reports and Dashboards.	Metadata	Allows full access to reports and dashboards in all other users' private folders (API only).	Restore to reports and dashboards in all other users' private folders (API only).
Manage Auth. Providers.	Metadata	Create and edit Auth. Providers.	Restore of Auth Providers.
Manage Certificates.	Metadata	Ability to manage certificates.	Protection of Certificates.
Manage Chatter Messages and Direct Messages.	Data	Access all users' messages sent in Chatter.	Protection of Chatter data.

Table 7-3 *(continued)*

Permissions	Data/Metadata	Salesforce description	Used by Cohesity Alta SaaS Protection for
Manage Connected Apps.	Metadata	Manage, create, edit, and delete connected applications.	Restore of Connected Apps.
Manage Custom Permissions.	Metadata	Create, edit, and delete custom permissions.	Restore of PermissionSets and Profiles.
Manage Custom Report Types.	Metadata	Create, edit, and delete custom report types.	Restore of Custom Reports.
Manage Dashboards in Public Folders.	Metadata	Create, edit, delete dashboards, and manage their sharing in all public folders.	Restore of Custom Dashboards.
Manage Data Categories.	Metadata	Create, edit, and delete data categories.	Protection of 'DataCategoryGroup' backup.
Manage Data Integrations.	Data	Monitor or abort Bulk API jobs.	Bulk API management (during backup and restore).
Create Libraries.	Data	Create libraries.	Restore of Library.
Manage Letterhead.	Data and Metadata	Create, edit, and delete letterheads for HTML emails.	Protection of Email Letterheads.
Manage Multi-Factor Authentication in API.	Metadata	Use the API to manage user identity verification methods for multi-factor authentication.	Required for Metadata Backup.
Manage Public Classic Email Templates.	Metadata	Create, edit, and delete text emails, mail merge templates, and folders for public email templates.	Restore of Email Template in Folder.

Table 7-3 *(continued)*

Permissions	Data/Metadata	Salesforce description	Used by Cohesity Alta SaaS Protection for
Manage Public Documents.	Data	Create, edit, and delete folders for public documents.	Restore of Folders for Documents.
Manage Public List Views.	Metadata	Create, edit, and delete public list views.	Restore of List Views.
Manage Reports in Public Folders.	Metadata	Create, edit, delete reports, and manage their sharing in all public folders.	Restore of Reports in Public Folder.
Manage Unlisted Groups.	Data	View and moderate unlisted Chatter groups.	Protection of Unlisted Groups.
Manage Users.	Metadata	Create, edit, and deactivate users, and manage security settings, including profiles and roles.	Restore of Users.

Table 7-3 *(continued)*

Permissions	Data/Metadata	Salesforce description	Used by Cohesity Alta SaaS Protection for
Modify All Data.	Data	Create, edit, and delete all organization data, regardless of sharing settings.	Needed for auto-inclusion of new objects and related objects. Third-party product objects, custom objects as and when they get added to the Org, they will get picked up by ASP only if this permission is given. Some objects (TopicAssignment, FeedRevision, FeedAttachment, Announcement, FeedComment, EntitySubscription) require this permission for query. A few other objects require this permission for Metadata restore.

Table 7-3 *(continued)*

Permissions	Data/Metadata	Salesforce description	Used by Cohesity Alta SaaS Protection for
Modify Metadata through Metadata API Functions.	Metadata	Create, read, edit, and delete org metadata. Users must have appropriate access rights to the metadata they're trying to modify. Be careful if delegating this permission. Some metadata runs in a system context, when object permissions, field-level security, and sharing rules that apply to the user are ignored. For example, Apex runs in a system context.	Metadata restores.
Update Email Messages.	Data	Modify certain email message-related records.	Restore of EmailMessages.
View All Custom Settings.	Metadata	Let users view all custom setting data directly and by the API.	Protection of Custom Settings.
View All Lookup Record Names.	Data	View the record names in lookup fields regardless of sharing settings. Lookup fields include system fields, such as Created By and Last Modified By.	Backup of System Fields.
View All Profiles.	Metadata	View all user profiles, regardless of profile filtering setting.	Backup of Profiles.

Table 7-3 *(continued)*

Permissions	Data/Metadata	Salesforce description	Used by Cohesity Alta SaaS Protection for
View All Data.	Metadata and Data	View all organizational data, regardless of sharing settings.	Backup of Data and Metadata.
View And Edit Converted Leads.	Data	View and edit converted lead records.	Restore of Converted Leads.
View Developer Name	Data	View the DeveloperName field by the API.	Backup of Developer Name field.
View Encrypted Data	Data	View the value of encrypted fields in plain text.	Protection of Encrypted Fields.
App permissions			
Edit Case Comments.	Data	Edit their own case comments but not other user's comments.	Restore of CaseComment.
Import Solutions	Data	Import solutions for the organization.	Protection of Solutions.
Manage Cases.	Data	Administer case settings, including Email-to-Case and mass transfer of cases.	Protection of Cases.
Manage Categories.	Data	Define and modify solution categories settings.	Define and modify solution categories settings.
Manage Entitlements.	Data	Enable, create, and update entitlement management items.	Enable, create, and update entitlement management items.

Table 7-3 *(continued)*

Permissions	Data/Metadata	Salesforce description	Used by Cohesity Alta SaaS Protection for
Manage Content Permissions.	Data	Create, edit, and delete library permissions in Salesforce CRM Content.	Create, edit, and delete library permissions in Salesforce CRM Content.
Manage Content Properties.	Data	Create, edit, and delete custom fields in Salesforce CRM Content.	Create, edit, and delete custom fields in Salesforce CRM Content.
Manage Flow.	Data	Allow users to view, create, edit, delete, and activate all flows and flow types in Lightning Experience apps and Setup.	Protection of Workflows
Manage record types and layouts for Files.	Data and Metadata	Create, edit, and delete content types in Salesforce CRM Content.	Create, edit, and delete content types in Salesforce CRM Content.
Manage Salesforce CRM Content.	Data	Create, edit, and delete libraries and library memberships.	Create, edit, and delete libraries and library memberships.
Query All Files	Data	Allows View All Data users to SOQL query all files in the org.	Protection of Documents / Attachments / Files / Salesforce CRM Content.

API permissions for Entra ID

The following API permissions are required for Entra ID backup operation.

Table 7-4

API name	Claim name	permissions	Description my Microsoft	Used by Cohesity Alta SaaS Protection
Microsoft Graph	Group.Read.All	Read all groups	Allows the app to read group properties and memberships, and read conversations for all groups, without a signed-in user.	Used to read group information
	User.Read.All	Read all users' full profiles	Allows the app to read user profiles without a signed-in user.	Used to read user profile details during backup.
	ApplicationReadWriteAll	Read and write all applications	Allows the app to create, read, update and delete applications and service principals without a signed-in user. Does not allow management of consent grants.	Used to read application settings and to get Token issuance policies and token lifetime policies during backup.
	Directory.ReadAll	Read directory data	Allows the app to read all directory data.	Used to read directory data, including user, group, and app information.
	Policy.Read.All	Read your organization's policies	Allows the app to read your organization's policies.	Used to read organizational policies during backup.

The following API permissions are required for Entra ID restore operation.

Table 7-5

API name	Claim name	Permissions	Description my Microsoft	Used by Cohesity Alta SaaS Protection
Microsoft Graph	Directory.ReadWrite.All	Read and write directory data.	Allows the app to read and write data in your organization's directory, such as users, and groups, without a signed-in user. Does not allow user or group deletion.	To restore directory data, including user and group.
	User.ReadWrite.All	Read and write all users' full profiles.	Allows the app to read and write user profiles without a signed-in user.	To restore user profile details during recovery workflows.
	Group.ReadWrite.All	Read and write all groups.	Allows the app to create groups, read all group properties and memberships, update group properties and memberships, and delete groups. Also allows the app to read and write conversations. All of these operations can be performed by the app without a signed-in user.	To restore groups, group properties and memberships for groups.
	Application.ReadWrite.All	Read and write all applications.	Allows the app to create, read, update and delete applications and service principals without a signed-in user. Does not allow management of consent grants.	To create & restore the application registration during recovery processes.

Table 7-5 *(continued)*

API name	Claim name	Permissions	Description my Microsoft	Used by Cohesity Alta SaaS Protection
	GroupMemberReadWriteAll	Read and write all group memberships.	Allows the app to list groups, read basic properties, read and update the membership of the groups this app has access to without a signed-in user. Group properties and owners cannot be updated and groups cannot be deleted.	To update & restore the group membership.
	Device.ReadWrite.All	Read and write devices	Allows the app to read and write all device properties without a signed in user. Does not allow device creation, device deletion or update of device alternative security identifiers.	To add group members of Device type during recovery processes.
	OrgContact.Read.All	Read organizational contacts.	Allows the app to read all organizational contacts without a signed-in user. These contacts are managed by the organization and are different from a user's personal contacts.	To read the organizational contacts during recovery workflows.
	AppRoleAssignmentReadWriteAll	Manage app permission grants and app role assignments.		

Table 7-5 *(continued)*

API name	Claim name	Permissions	Description my Microsoft	Used by Cohesity Alta SaaS Protection
			Allows the app to manage permission grants for application permissions to any API (including Microsoft Graph) and application assignments for any app, without a signed-in user.	To manage app roles and permission grants during recovery operations.
	[illegible]	Read and write all directory RBAC settings.	Allows the app to read and manage the role-based access control (RBAC) settings for your company's directory, without a signed-in user. This includes instantiating directory roles and managing directory role membership, and reading directory role templates, directory roles and memberships.	To restore RBAC settings during recovery workflows.
	[illegible]	Read and write your organization's application configuration policies.	Allows the app to read and write your organization's application configuration policies, without a signed-in user.	To restore application configuration policies during recovery processes.

App permissions of Web App

The following optional claims are included in the access token. Cohesity Alta SaaS Protection uses an OpenID Connect-based authentication layer, where these claims support effective authentication and authorization, especially for SIEM integrations. These claims provide information about the user but do not grant additional access. They are required if a Web App is deployed.

Table 7-6

API Name	Claim value	Permission	Description by Microsoft	Used by Cohesity Alta SaaS Protection
User.Read	User.Read	Delegated	Sign in and read the user profile.	To include in the access token.
profile	profile	Delegated	View users' basic profile.	To include in the access token.
openid	openid	Delegated	Sign users in.	To include in the access token.
offline_access	offline_access	Delegated	Maintain access to data you have given it access to.	To include in the access token.

Chapter 8

What is a connector?

This chapter includes the following topics:

- What is a connector?
- About transient errors
- Overview of adding connectors
- Configure General settings
- Configure Capture scope
- Configure User filter
- Configure Group filter
- Configure Folder filter
- Configure credentials
- Configure Custom backup policy and guidelines
- Configure Delete policy for SharePoint Online and guidelines
- Configure Stubbing policy
- Guidelines to configure Stubbing policy for SharePoint Online
- Schedule a backup
- Configure email addresses to get notifications
- Review configuration and edit/save/initiate backup
- Connectors page
- Connector status

- Edit connector configuration
- Delete connectors

What is a connector?

A Cohesity Alta SaaS Protection connector is a logical interface that links source applications to backup storage in Cohesity Alta SaaS Protection. You can create and configure multiple connectors for each workload to meet your backup requirements.

Key features of Cohesity Alta SaaS Protection connectors:

- **Custom backup policies**
  Configure backup policies to align with your organization's specific requirements.
- **Data deletion policies**
  Manage data deletion for SharePoint Online, Teams Sites, and OneDrive using configurable policies.
- **Source archiving**
  Optimize storage management by configuring archiving policies for SharePoint Online, Teams Sites, and OneDrive.
- **Scheduled backups**
  Automate backups based on your organization's preferred frequency to ensure continuous data protection.
- **Exclusions**
  Exclude specific files, folders, user data, or data types to refine your backup strategy.
- **Automated alerts**
  Receive email notifications about backup statuses to stay informed and responsive.
- **App registration**
  Approve multiple Microsoft 365 app registrations simultaneously using the App Grant utility.
- **Real-time monitoring**
  Gain real-time insights into backup status, health, and progress for complete visibility.

About transient errors

While backing up or restoring data from/to workloads like Exchange, SharePoint, OneDrive, and Teams, Cohesity Alta SaaS Protection may encounter the errors which are transient in nature. The errors can be due to various factors like network issues, load on workload or services. If errors continue to occur on subsequent operations, they can be treated as persistent errors and need user intervention to fix them.

Overview of adding connectors

The procedure for adding connectors is outlined as follows:

- **Step 1: Configure general information**
  In this step, you must specify basic details, including the connector name, storage location for backed-up data, and other settings.
- **Step 2: Configure capture scope**
  In this step, you need to define what to back up by selecting all items or specific ones. Apply filters to restrict backups to particular users and folders.
- **Step 3: Configure authentication**
  In this step, enter credentials for authentication. You can use Microsoft 365 apps added by Cohesity Alta SaaS Protection and grant admin consent.
- **Step 4: Configure policies**
  In this step, you can set backup policies. For SharePoint Online, configure stub and delete policies to manage data archiving at the source.
- **Step 5: Configure the backup schedule**
  In this step, you need to define the backup schedule based on your organization's needs.
- **Step 6: Review and save configuration**
  In this step, you can review the settings and either save the configuration or start the backup.

Related topics:

-
-
-
-
-

Configure General settings

The first step in adding a connector is to configure the general settings. If the required Stor or Connector service is unavailable, contact Cohesity Support.

To configure the general settings

1. In the **Connector name** field, enter a name for the connector.
2. The **Type** field displays the connector type.
3. In the **Stor** dropdown list, select the designated storage location for backed-up data.
4. The **Machine** field displays the Connector service that will host the connector. If necessary, select a different service from the list. Contact Cohesity Support to make this change.

   Note: When the Pre-ingest encryption key is applied to the connector, the Full-text search feature, which affects Discovery and End-User search functionality, is disabled. You cannot preview or download items from the Administration and End-User portal. For more information, refer to the following tech note: About the Encryption Key

5. (Optional) **Select Enable email notification** to receive alerts when the predefined error threshold is exceeded during backup. Enabling this option adds the **Email notification** tab to the connector setup.
6. Click **Next**to configure capture scope.

   See “Configure Capture scope” on page 83.

Note: If your tenant is configured using the scope feature, the **Scope** dropdown list is displayed when you add a connector. You need to select the required scope from the **Scope** dropdown list. For more information, contact Cohesity Support.

Configure Capture scope

To configure the capture scope for the workloads according to your backup requirements, refer to the following corresponding link:

Table 8-1

Connectors	Reference links
Exchange connector	To configure the capture scope for the Exchange connector according to your backup requirements. See "Configure capture scope for Exchange connectors" on page 130.
Sharepoint connector	Decide whether to backup all sites or only specific sites. See "Configure capture scope for SharePoint connectors" on page 141.
Teams site connector	You can have different use cases to back up Teams site collections and its data. See "Configure capture scope for Team site collections connectors" on page 155.
OneDrive	You can have different use cases to back up OneDrive for Business sites and its data.
Teams chat connector	See "Configure capture scope for Teams chat connectors" on page 165.
Audit log connector	See "Add Audit log connectors " on page 184.
Google Drive connector	See "Configure Capture scope Google Drive connectors " on page 172.
Gmail connector	See "Configure capture scope for Gmail connectors" on page 180.
Box connector	See "Configure capture scope for Box connector" on page 224.
Slack connector	
Entra ID connector	See "About Salesforce protection" on page 187.
Email/message connector	See "Add Email/Messages file" on page 226.

Configure User filter

When configuring the capture scope, you can limit the backup to specific users using Azure AD (Entra ID) extended attributes. This filter allows you to target only the required set of users, ensuring efficient backup management.

This connector backs up user data based on a specified attribute and its value, excluding data from users who do not match the criteria.

To filter users based on Entra ID (Azure AD) extended attributes

1. In the **User filter** section, click **Enable this feature**.
2. In the **Attribute name** field, enter the attribute's name to apply the filter—for example, *department*.
3. Click **+ Add extended AD attributes filters**.
4. On the **AD Attribute filter** page, enter the attribute value to filter users—for example, *account*.
5. Click **Add**.
   - Extended Entra ID attribute filters match a user or group based on its attribute value.
   - These filters are case-insensitive and support wildcard usage.
   - Regular expressions are supported by prefixing the filter string with Regex.

Other filters to further refine the backup scope:

- **Group filter** to filter by group membership.
  See “Configure Group filter” on page 86.
- **Folder filter** to filter by specific folders.
  See “Configure Folder filter” on page 87.

Related topics:

- See “Configure capture scope for Teams chat connectors” on page 165.
- See “Configure Capture scope Google Drive connectors ” on page 172.
- See “Configure capture scope for Gmail connectors” on page 180.
- See “Configure capture scope for Box connector” on page 224.

Configure Group filter

When configuring the capture scope, you can limit the backup of specific users for particular workloads using Azure AD (Entra ID) group membership. This action ensures that only the required set of users' data is backed up.

Key considerations:

- From Cohesity Alta SaaS Protection version 2.20 onwards, you must have an **include list**; you cannot create only an **exclude list**.
- Workaround for versions before 2.20 (if only an exclude list exists):
  - Create a group in Azure AD (Entra ID).
  - Add all users to this group.
  - Add this group to the include list.
- Starting from Cohesity Alta SaaS Protection version 2.30, if a group is empty, no mailboxes will be backed up.

To filter users based on Entra ID group membership

1. In the **Group filter** section, click **Enable this feature**.
2. Click **+ Add group filter**.
3. Do any of the following:

Actions:	Include groups,	Exclude groups,
Steps:	■ Click **Include**. ■ Enter the name of the group to be included. The list is populated based on the search. ■ Click the required group. ■ Click **Add**.	■ Click **Exclude**. ■ Enter the name of the group to be excluded. The list is populated based on the search. Click the required group. ■ Click **Add**.
Behaviors:	Only the data of users in the included groups is backed up.	All users' data is backed up except those in the excluded groups.

The page displays the added groups and their corresponding actions, which can be included or excluded. You can remove the group from the list using the **Remove** option.

Other filters to further refine the backup scope:

- **User filter** to filter users based on Entra ID (Azure AD) extended attributes.
  See "Configure User filter" on page 85.
- **Folder filter** to filter by specific folders:
  See "Configure Folder filter" on page 87.

Related topics:

- See "Configure capture scope for Exchange connectors" on page 130.
- See "Configure capture scope for OneDrive connectors" on page 160.

Configure Folder filter

When configuring the capture scope for a connector, you can limit the backup scope to specific folders within the source workload. This filter helps in targeting only the relevant data for backup.

Folder filter matching methods:

Folder filters work based on:

- Exact match
- Wildcard match
- Regular expressions

To configure filter folders:

1. In the **Folder Filters** section, click **Enable this feature**.
2. Click **+ Add Folder Filter**.
3. On the **Folder Filter Properties** page, do any of the following:

Actions:	**To include folders**:	**To exclude folders**:
Steps:	■ Select **Include**. ■ In the **Pattern Type** box, enter the item using wild card or regular expression type. ■ Click **Add**.	■ First, you need to include the folder from which you want to filter a specific folder. ■ Select **Exclude**. ■ In the **Pattern Type** box, enter the item using wild card or regular expression type. ■ Click **Add**.

Behaviors:	The connector backs up the included folders.	The connector excludes the folder from the backup.

To exclude a folder within an already included folder, ensure that you first include the parent folder and then exclude the specific subfolder.

Filter behavior:

- The connector backs up only the folders included in the filter.
- The connector excludes folders marked with the exclude filter.
- Use **Move Up** and **Move Down** to prioritize filters in the list.
- Use the **Remove** option to delete any selected filter.

Other filters to further refine the backup scope:

You can also use the following filters to refine the backup scope further:

- **User filter** to filter users based on Entra ID (Azure AD) extended attributes.
  See "Configure User filter" on page 85.
- **Group filter** to filter by group membership.
  See "Configure Group filter" on page 86.

Related topics:

- See "Configure capture scope for Exchange connectors" on page 130.
- See "Configure capture scope for SharePoint connectors" on page 141.
- See "Configure capture scope for Team site collections connectors" on page 155.
- See "Configure capture scope for OneDrive connectors" on page 160.
- See "Configure capture scope for Teams chat connectors" on page 165.
- See "Configure Capture scope Google Drive connectors " on page 172.
- See "Configure capture scope for Gmail connectors" on page 180.
- See "Configure capture scope for Box connector" on page 224.

Configure credentials

Once the capture scope is defined, you must configure authentication credentials on the **Credentials** page to allow Cohesity Alta SaaS Protection to access and protect your SaaS workloads.

You can perform the following actions on the **Credentials** page:

- **Assign Microsoft 365 app registrations**
  - Cohesity has provisioned Microsoft 365 app registrations for your tenant.
  - These preconfigured apps include the necessary permissions required for backup and restore operations.
  - You need to assign the required number of apps to the connectors.

  See "Assign Microsoft 365 apps registration" on page 89.
- **Approve Microsoft 365 app registrations**

  By default, the provisioned Microsoft 365 app registrations remain inactive. They must be approved by a Global Administrator in your organization.

  There are two ways to approve app registrations:
  - **Manual approval**:

    The Global Admin can approve each app manually.

    See "Approve Microsoft 365 apps using the App Consent Grant utility" on page 92.
  - **Using the App Consent Grant Utility**:

    The Global Admin can use this tool to automate the approval process.

    See "Manually approve Microsoft 365 apps registration" on page 91.

Learn more:

Refer to the following links to know the permission requested by Cohesity Alta SaaS Protection for authentication:

- See "API permissions for Microsoft 365 workloads" on page 56.

Assign Microsoft 365 apps registration

When assigning Microsoft 365 app registrations, the apps will initially be in an inactive status. A Global Admin from your organization must approve the admin consent before the apps can be used for backup and restore operations.

To assign Microsoft 365 apps registration

1. On the **Credentials** page, click **M365 app registrations**.
2. Click **+ Assign M365 apps**.
3. On the **Assign new M365 apps** page, enter the following details:

Tenant Domain	Select the tenant's domain name from the dropdown list. If the domain name is not listed, contact Cohesity Support.

Number of apps to provision

Enter the number of apps to be provisioned for this connector. The number of apps provisioned ensures that the required performance is achieved.

- For Audit Log connector - One app only
- For Entra ID connector - Five hundred apps
- For Teams chat connector - One app only

Guidelines to assign Microsoft 365 apps registration for SharePoint Online connector:

- For license count less than 1000, then provision 1 to 3.
- For license counts between 1000 and 5000, provision 4 to 8
- For license counts between 5000 and 15000, provision 9 to 15.
- For license counts between 15000 and 50000, provision 16 to 25.

4 Click **Assign**.

5 If the app status is displayed as **Inactive**. The Global Admin from your organization is required to approve these apps by accepting the admin consent.

Note that the backup cannot start unless the Global admin accepts the admin consent and the apps are in an active state.

Do any of the following to activate the apps:

- Approve the admin consent request now.

- Proceed with connector creation by clicking **Next** and later return to this page to approve the admin consent.

Next step:

See "Manually approve Microsoft 365 apps registration" on page 91. or See "Approve Microsoft 365 apps using the App Consent Grant utility" on page 92.

Related topics:

- See "API permissions for Microsoft 365 workloads" on page 56.
- See "Microsoft 365 apps registration status" on page 90.

Microsoft 365 apps registration status

The Microsoft 365 apps registration status indicates their assignments and consent status within Cohesity Alta SaaS Protection.

Table 8-2

Microsoft 365 apps registration statuses	Description
Unassigned	The apps that are not assigned to any connector or an Export location.
Assigned	The apps that are assigned to a connector or an Export location.
Inactive	The apps that are assigned to a connector or an Export location but the admin consent for these apps is not yet granted.
Active	The apps for which admin consent is granted and is ready for use.

Manually approve Microsoft 365 apps registration

When Microsoft 365 apps registrations are assigned, they are initially in an inactive state. A Global Administrator in your organization must approve admin consent to activate these apps. This approval can be done either manually or using the App Consent Grant Utility (See "Approve Microsoft 365 apps using the App Consent Grant utility" on page 92.).

Approving admin consent grants the necessary permissions and access rights to perform backup and restore operations. Follow these steps to manually approve (grant admin consent) for Microsoft 365 app registration.

To manually approve Microsoft 365 apps registration

1. On the **Credentials** tab, click the **Accept** link next to the app you want to activate.
2. On the logon window, log on with a user (Global administrator of your organization) who has administrative access.
3. The permissions are listed on the pop-up. Verify the permissions and then click **Accept**.
4. Go to the **Credentials** tab.

   The app status should be displayed as active.
5. Select the app and click **Next**.

Next step:

Configure Custom backup policy.

See "Configure Custom backup policy and guidelines" on page 93.

Approve Microsoft 365 apps using the App Consent Grant utility

When Microsoft 365 apps registrations are assigned, they are initially in an inactive state. A Global Administrator in your organization must approve admin consent to activate these apps. This approval can be done either manually (See "Manually approve Microsoft 365 apps registration" on page 91.) or using the App Consent Grant Utility (See "Approve Microsoft 365 apps using the App Consent Grant utility" on page 92.).

Approving admin consent grants the necessary permissions and access rights to perform backup and restore operations. Follow these steps to manually approve (grant admin consent) for Microsoft 365 app registration.

Before you begin

- You must have Global Administrator permissions in Microsoft Entra ID (Azure AD) to approve app registration.
- The App Consent Grant Utility must be installed on a Windows computer with the required administrative rights.
- Ensure pop-ups are allowed in the browser, as Microsoft's sign-in page may require additional authentication steps.

To approve Microsoft 365 apps using App Consent Grant utility

1. On the Windows computer on which the utility is installed, click **Start** > **Cohesity Alta SaaS Protection** > **Apps Consents Grant Utility**.

   Note: If the currently logged-on user is not the computer administrator, run the utility **as Administrator**.

   The **Apps Consents Grant Utility** window opens.

2. Click **Next**.
3. On the **Process apps** window, do the following:
   - From the **Microsoft 365 domain** dropdown list, select the required domain for which the application requires consent.
   - Click **Fetch Inactive Apps**.
     The inactive applications in the selected domain are listed on the **Fetching Inactive Apps(s)** window.
   - Click **Close**.
     All the inactive applications are listed on the **Process apps** window, with IDs and names.

- Click the apps that are to be granted and click **Grant Consent**.
- On the logon window, enter credentials for the Microsoft 365 Global Administrator and then click **Sign in**.
- Click **Close**.
  The **Apps consents grant summary** field displays the summary, such as which application's granting is completed successfully and which is not.
  The event logs are displayed on the window.
- Click **Close**.
  The granted applications are listed as **Active** applications on the **Credentials** tab.

Next step:

- Open the Cohesity Alta SaaS Protection Administration Portal.
- On the **Credentials** page, select the required active apps.
- Click **Next** to configure custom backup policies.
  See "Configure Custom backup policy and guidelines" on page 93.

Microsoft 365 apps recovery

If the registered Azure apps are accidentally deleted, recovery is still possible if the apps are not removed from the tenant.

Go to the **Credentials** tab, access the app activation link, and grant Admin consent. After this activity, the app is active again.

Configure Custom backup policy and guidelines

On the **Policy configuration** page, you can configure a custom backup policy for any connector for more granular backup needs.

Guidelines to configure a custom backup policy

Before configuring a custom backup policy, consider the following:

- By default, all items in the source workload are backed up. A custom backup policy allows you to specify which items to back up.
- This policy applies to all SaaS workloads except Teams Chat, Audit Log, Slack, Salesforce, Email/message files, and Files.
- The policy applies only to new items and does not affect previously backed-up items.

- You can customize backup criteria based on size, last modified date, and item type.
- You can define any or all of these criteria as per your specific backup requirements.
- Any folder exclusion criteria set on the **Capture scope** page override those defined in the custom backup policy.

To configure a Custom backup policy

1. Go to the **Policy configuration** page.
2. Select the **Items <*Last modified*> date older than<-->days** check box.
3. Enter the number of days to specify the modified items that you want to back up.

   This option applies regardless of the item's size and type.
4. Select the **Items size larger than __<-->** check box to back up the items that are larger than the specified size.

   This option applies regardless of the item's last modified date and type.
5. Select the **<*Include/Exclude*>items of type<*Enter a file extension*>** check box and enter the extensions that should be included or excluded.

   Note: This option is applied regardless of the items' Last modified status and size.

   Note: This option is not applicable to the Google Drive connector.
6. To exclude specific folders, use the **Locations to exclude** option.
   - Any folder that matches the specified name (including subfolders) is excluded.
   - Matching is case-insensitive, and you can use wildcards.
   - Folder filter settings for the connector take precedence over this exclusion.
   - Do the following:
     - Click **+Add location**.
     - On the **Location name** page, enter the name of the folder to exclude.
     - Click **Add**.

The custom backup policy is now configured.

Next step:

- If applicable, configure Delete and Stubbing policies.
  See "Configure Delete policy for SharePoint Online and guidelines" on page 95.
  See "Configure Stubbing policy" on page 100.
- Alternatively, click **Next** to schedule a backup job.
  See "Schedule a backup" on page 115.

Configure Delete policy for SharePoint Online and guidelines

The SharePoint Online connector can be configured with a Delete policy to manage storage by removing unnecessary files from the source SharePoint Online environment while retaining backups in Cohesity Alta SaaS Protection.

Before configuring the Connector Delete policy, you must read the following guidelines to understand its implications. Cohesity is not responsible for any loss of functionality in SharePoint caused by of actions of this policy.

The delete policy can only be customized based on the following criteria:

- Size
- Last modified date
- Type

You can define **any** or **all** these criteria according to your specific requirements.

Delete Policy setup guidelines

Before configuring the Delete policy, you must read the following guidelines to understand its implications:

- Start by testing the policy in a small or less-used environment. This will help Administrators and End Users understand how the policy works before it is deployed widely.
- Check the section 'Considerations Before Enabling the Delete Policy' to understand the implications of deletion of files at source. This will help you decide the correct policy settings and exclude the Sites and Locations where deletion should not be performed.
- Decide on one of the following:
  - Only to archive certain items into Cohesity Alta SaaS Protection and delete them from SharePoint.
  - Back up all the data in SharePoint Sites/OD while also deleting certain files.

- If only deleting certain files (that is you have decided for 'Only to archive certain items into Cohesity Alta SaaS Protection and delete them from SharePoint'), make it so that you have a Custom Backup Policy and Delete Policies should match each other for the connector.
  - Consider prioritizing larger files: For faster space savings, target larger files first (for example, files over 5 MB modified more than a year ago, or whatever is your date criteria).
  - Adjust criteria over time: Later, adjust both Custom Backup and Delete policies to suit your ongoing plan (for example, files over 1 MB modified more than a year ago).
- If deleting files based on policy and backing up all files (that is the other option 'Back up all the data in SharePoint Sites/OD while also deleting certain files'.), follow the guidelines in step 4; however, when setting the ongoing criteria, clear out the settings in the Custom Backup Policy so that all files will be part of the backup, but only files that meet the delete policy are eligible for deletion.

Considerations Before Enabling the Delete Policy

Since this process deletes data at source, it is important to understand the implications of the Cohesity Alta SaaS Protection process before enabling the policy. Cohesity will be unable to help or support in case of unsupported scenarios and hence it will not be Cohesity's responsibility to recover from the situation.

General considerations:

- Cohesity Alta SaaS Protection deletes files from the SharePoint Online after creating a primary backup copy in its storage. No additional copies are maintained by default, so it's crucial to avoid accidental deletion of the primary backup, for example, due to a misconfigured Cohesity Alta SaaS Protection deletion policy (used to manage retention of data within Cohesity Alta SaaS Protection storage, not to be confused with connector delete policy).

  You can consider purchasing the Extra Data Backup (EDB) option to maintain a secondary backup copy.
- Sometimes automated processes within SharePoint online OR external applications integrated with SharePoint Online rely on a file to be present for their functioning. Such processes OR applications can be disrupted due to this deletion of the file. Such locations should be excluded from the delete policy.
- If the policy deletes files based on the last modified date, frequently accessed but unmodified content may also be deleted.

  Carefully consider whether such content should be deleted, as it can lead to frequent restore requests.

- Evaluate what should be retained at the source before enabling this policy to configure the deletion exclusions properly.

  If files are accidentally deleted, administrators may need to perform mass restores through the Cohesity Alta SaaS Protection Administration portal, which can be time-consuming and impacts the user experience.

Scope of application in SharePoint:

- Cohesity Alta SaaS Protection only deletes files and not sites, lists, and folders.
- The policy applies only to files within the libraries, which are based on document libraries (for example, whose list base type is a document library).
- The following items cannot be deleted using the connector delete policy:
  - ASPX files
  - Items in hidden lists or catalog lists.
  - Files which have been stubbed by Cohesity Alta SaaS Protection and have the '.stub.url' extension.

    Important – It is important to understand the implications of the above, when applying this policy. Cohesity is not responsible for any loss of functionality in SharePoint because of actions of this policy.
  - If the meet the criteria specified in the deletion policy, it may stop working if files associated with them are deleted.
  - IRM-Enabled Lists: Files that meet deletion criteria will be deleted.
    - They cannot be opened if downloaded from Cohesity Alta SaaS Protection.
    - Restores of such files only work if the IRMS settings of the source list stay unmodified.
  - Retention policies and legal holds: Files which have Retention Labels or reside in a site which have a Retention Policy or Legal Holds will be deleted from their primary locations.
    - They will be retained in the Preservation Hold library and hence may not result in space savings.
    - Deletion of such files may not be desired as this may conflict with any compliance policies at source.
  - Sensitive encrypted labels: Files encrypted with sensitive labels will be deleted. Currently restores of these files have limitations.

    • For the files with Sensitivity labels configured for encryption, only restores from scratch for a single version can be performed.

• Restoring multiple versions and overwrite restores are not supported, as SharePoint does not allow the creation of a new version on top of such files.

- Deletion can disrupt functionality for Loop integration and InfoPath integration.
- Files which are in Site Assets, Site Pages, SharePoint designated System Lists may also be deleted.
- This is not an exhaustive list, and Cohesity is not liable for any undocumented functionality loss.

Connector Delete Policy Evaluation, Configuration, and Interaction:

- Configure exclusions based on last modified date or size (last accessed time is unsupported).
- The policy is applied from the second full backup, after all the data is successfully backed up by the first full backup. This is not applicable to incremental backups.
- The connector delete policy applies only to full backups and does not apply to incremental backups occurring between two full backups.
- Cohesity Alta SaaS Protection will not remove the current version of a file in SharePoint unless it is the only version of the file still in SharePoint. It leads to the following behavior when both versions of a file in SharePoint with two versions match a delete policy:
  - Backup 1: The older version is deleted. The current version is left.
  - Backup 2: The file is deleted.
- If both the delete and stubbing policies apply to the same file, the delete policy takes precedence, permanently deleting the file from SharePoint.

Interaction with Cohesity Alta SaaS Protection deletion policies (used for retention of data within Cohesity Alta SaaS Protection)

- Cohesity Alta SaaS Protection marks files as Removed from source if they're no longer found in the same location during a subsequent backup after the initial one.

Note: Files deleted at the source by a connector delete policy will also be marked as Removed from source in Cohesity Alta SaaS Protection in the following backup. Cohesity Alta SaaS Protection does not distinguish between deletions made by the connector delete policy or independent deletions at source.

Note: Cohesity Alta SaaS Protection deletion policies (used for retention of data within Cohesity Alta SaaS Protection) can be configured to delete files in Cohesity Alta SaaS Protection marked as Removed from source. As noted above, Cohesity Alta SaaS Protection cannot differentiate between what was deleted at source by Cohesity Alta SaaS Protection (by a connector delete policy) and what was deleted at source by end user action, based on the 'Removed from source' property. This makes it challenging to set up such Cohesity Alta SaaS Protection deletion policies, if there is a need to differentiate the origin of deletions.

Copy/Move of locations containing Files deleted by Cohesity Alta SaaS Protection:

- If a location which previously had files deleted by Cohesity Alta SaaS Protection through a connector delete policy is copied or moved in SharePoint, the currently present data at the source at the copied/moved location be backed to the new location.

Note: Any data that was previously deleted by Cohesity Alta SaaS Protection will remain at the old location.

Backup of Previously Deleted Restored Files:

- After file is restored, Cohesity Alta SaaS Protectionn treats it as a new file during the next backup, resulting in two records. The original file marked as Removed from source (deleted by the connector policy) and the newly ingested file.

End User Access:

- End users can access Cohesity Alta SaaS Protection data through the End-User portal, but their permission level must have the Open Items List Permission in SharePoint. If users' permission level only have View Items or View Application Pages permissions (such as in Restricted View, View Only, or Download Only permission levels), they won't have access to deleted files in the portal.
- For details on how Cohesity Alta SaaS Protection synchronizes permissions, refer to See "End-user SharePoint data access in Cohesity Alta SaaS Protection" on page 148.
- Any enhancements/fixes made by Cohesity Alta SaaS Protection to capture new/existing permissions will not be reflected on files which have already been captured and deleted at source from SharePoint.
- End users can download or restore data, but can only restore files to SharePoint sites where they are primary administrators.

Files Synchronized with laptops, PCs, and Sharing links:

- These will stop working.

To configure Delete policy

1. Click **Enable this feature** on the **Policy configuration** tab.
2. Do the following:
   - Select the **Items <*Last modified*> date older than <--> days** check box and enter the number of days to specify the modified items that must be backed up.
     This option is applied regardless of the items' size and type.
   - Select the **Items size larger than __<-->** check box to back up the items that are larger than the specified size.
     This option is applied regardless of the items' last modified date and type.
   - Select the **<*Include/Exclude*> items of type <*Enter a file extension*>** check box and enter the extensions that should be included or excluded.
     This option is applied regardless of the items' Last modified status and size.
     This option is not applicable to the Google Drive connector.
   - Use the **Locations to exclude** option to exclude specific folders.
     Any folder that matches the provided name is excluded from the backup with its subfolders. The matching process is case-insensitive, and wildcards can be used.
     The exclusion criteria that are set in the **Folder filter** section for this connector take precedence over the criteria that is set here.
     - Click **+Add location**.
     - On the **Location name** page, enter the name of the folder that is to be excluded.
     - Click **Add**.

     The folders to be excluded are listed at the bottom of this section.

   The Delete policy is configured.

   If you want to configure Stubbing policy, See "Configure Stubbing policy" on page 100.

Configure Stubbing policy

The SharePoint Online connector can be configured with a stubbing policy to optimize storage in the SharePoint Online environment. When enabled, the backup process replaces backed-up items with stubs (shortcuts) and deletes the original item versions.

Stubs appear in SharePoint Online as URL files with the *.stub.url* extension. When users click a stub, they can:

- Download the data from Cohesity Alta SaaS Protection to their local device.
- Restore the stubbed items to their original location in SharePoint Online (this behavior is configurable by the Cohesity Alta SaaS Protection administrator).

Important: Before enabling the Stubbing policy, you must read the SharePoint Stubbing policy guidelines to understand its implications. See "Guidelines to configure Stubbing policy for SharePoint Online" on page 102.

To configure Stubbing policy

1. On the **Stubbing policy** section, click **Enable this feature**.
2. Configure the following options:
   - **Items *<Last modified>* date older than <--> days**: Select the check box and enter the number of days.
     This option applies regardless of item size and type.
   - **Items size larger than __<-->**: Select the check box and enter the size limit.
     This option applies regardless of the item's last modified date and type.
   - ***<Include/Exclude>* items of type *<Enter a file extension>***: Select the check box and enter the file extensions to include or exclude.
     - This option applies regardless of the item's last modified date and size.
     - This option is not applicable to the Google Drive connector.
   - To exclude specific folders, use the **Locations to exclude** option, and do the following:
     - Select **+ Add location**.
     - On the **Location name** page, enter the folder name to exclude.
     - Select **Add**.
       Excluded folders are listed at the bottom of this section. The Stubbing policy is now configured.
     - Click **Next**.

Note: Th **Archival details** section on the **Content** page, **Item details** pane to displays the stub movement type.

Next step:

Schedule a backup job. See "Schedule a backup" on page 115.

Guidelines to configure Stubbing policy for SharePoint Online

The SharePoint Online connector can be configured with a policy to perform stubbing. Stubbing helps to reduce storage in the SharePoint Online environment. When enabled, during the backup process, backed up items are changed to stubs (shortcuts) and original item versions are deleted. Stubs appear in SharePoint as URL files ending in the `.stub.url` extension. By clicking on the stub an end-user can either download the data from Cohesity Alta SaaS Protection locally or restore the stubbed items back to its original location in the SharePoint site (this behavior is configurable by an Cohesity Alta SaaS Protection administrator).

Cohesity Alta SaaS Protection supports archiving and stubbing for the following workloads:

- SharePoint Online
- Team Sites
- OneDrive

The stubbing policy can be customized based on the following criteria:

- **Size**
- **Last modified date**
- **Type**

You can define any or all of these criteria according to your specific data retention requirements.

Stubbing policy setup guidelines

- It's advisable to first test the impact of your stubbing policy in a small or less frequently used environment before rolling it out widely. This will help administrators and end-users become familiar with how stubbed files behave. It's important to note that stubbed files do not directly replace the original file in terms of supporting the same functionality within SharePoint.
- Review the **Considerations Before Enabling Stubbing** section to understand the implications of configuring stubbing and can select Sites and Locations eligible for stubbing, with the appropriate stubbing policy.

- Determine whether you plan to use Cohesity Alta SaaS Protection only to stub certain SharePoint/OneDrive items based on policy, or to back up all data in SharePoint Sites/OneDrive while also stubbing certain items.
- If you plan for only stubbing, ensure that your Custom Backup Policy and Stubbing Policy align with each other.
  - To achieve savings sooner, target larger items first (for example, items > 5 MB, with last modified > 1 year, or whatever your date criteria may be).
  - Later, adjust the criteria for both the Custom Backup Policy and Stubbing Policy to what you plan to use on an ongoing basis (for example, items > 1 MB with last modified > 1 year).
- If stubbing items based on policy while also backing up all items, follow the guidelines in step 2. When setting the ongoing criteria, clear the settings in the **Custom Backup Policy** so that all items are included in the backup, but only items meeting the stubbing policy criteria are eligible for stubbing.

Considerations before enabling stubbing

As the stubbing process deletes data at the source and replaces it with URLs, it is important to understand the implications of the Cohesity Alta SaaS Protection process before enabling the stubbing policy. Cohesity cannot help or support the customer if they exercise or run into unsupported scenarios. It will be the customer's responsibility to recover from the situation.

General considerations:

- Cohesity Alta SaaS Protection stubs an item after the data is moved to Cohesity Alta SaaS Protection storage, depending on the options configured in the connector and its backup policies. By default, Cohesity Alta SaaS Protection does not maintain any other copies of the item. Therefore, Cohesity Alta SaaS Protection stubs items only after creating a primary backup copy. Care should be taken to ensure that this primary copy is not deleted, for example, due to a misconfigured Cohesity Alta SaaS Protection deletion policy.
  Additional options, such as Extra Data Backup, need to be purchased if you want Cohesity Alta SaaS Protection to maintain a separate secondary copy.
- Only a file can be stubbed. A folder, library or a site cannot be stubbed.
- There may be automated processes within SharePoint Online or third-party software integrated with SharePoint Online that rely on the actual file being present to achieve certain objectives/workflow within site collections, for example, Akumina. Such functionality can be disrupted because of Cohesity Alta SaaS Protection stubbing. Such locations should be excluded from stubbing manually.
- There may also be automated processes within SharePoint Online or by the third-party software that copy, move, or create libraries and folders where

potentially stubbed files can reside. These locations should also be excluded from stubbing manually.

- If stubbing is based on the 'last modified' date, note that the content, which is frequently accessed but not modified will still be stubbed. Careful consideration should be given to whether such content should be stubbed, as keeping it as stubs may not be desired and can lead to frequent requests to restore the original content.
- For the above reasons, it is crucial to thoroughly evaluate what should not be stubbed before initiating the stubbing process. This careful planning ensures that the stubbing policies are configured correctly, preventing any inadvertent issues.

  If sites or libraries are accidentally stubbed, administrators will have to resort to doing restores by the admin portal. Depending on the number of sites and lists, the need for mass un-stubbing restores may arise. This can take time and may result in a diminished end-user experience.
- Considerations for the restores when stub policy is based on ‘Last modified time’. When doing restores, if the stub recall options have:
  - Restore: When content is recalled by clicking on the stub, Cohesity Alta SaaS Protection updates the modification time to prevent the item from being stubbed again immediately.
  - Download Only: End users can download the file, but restores can only be performed from the Administration Portal. By default, when restoring from the Administration Portal, the original last modified time is restored, meaning that the restored content can be stubbed again. To prevent this:
    - Exclude the content from stubbing after it has been restored.
    - When restoring from the Admin Portal, select the option Reset 'last modified time' of restored items to time of restore.
- Stubbing is not supported for Project Web Access sites. These sites must be manually excluded from the stubbing policy.
- Interaction of Cohesity Alta SaaS Protection stubbing in sites with the SPO features like, DLP, SharePoint Workflows is not supported. Sites with these functionalities should be excluded from stubbing manually.

Stubbed item deletion, movement, and interaction with Cohesity Alta SaaS Protection deletion policies:

- This section describes the behavior of a stub and its corresponding item in Cohesity Alta SaaS Protection under specific scenarios as follows:
  - **Stub deletion**

- If a stub is deleted, Cohesity Alta SaaS Protection marks the corresponding item as **Removed from source** in Cohesity Alta SaaS Protection storage during the next backup cycle.

  Note: Removed from source indicates that Cohesity Alta SaaS Protection recognizes the item is no longer present in its original location. This is important as Cohesity Alta SaaS Protection deletion policies are often configured to delete items marked as **Removed from source**.

- When the stub is restored to its original location from the Recycle Bin, in Cohesity Alta SaaS Protection's next scan the **Removed from Source** flag will be cleared, and access permissions (in Cohesity Alta SaaS Protection) will be updated based on existing permissions on source item.

- **Stub movement**
  - If an end-user copies or moves stub in SharePoint Online, Cohesity Alta SaaS Protection backup scans detect the change and perform the following:
    - Copies the original item backed up in Cohesity Alta SaaS Protection to a corresponding new location in Cohesity Alta SaaS Protection and sets an **Archival Type**.
    - Modifies the stubs in the destination SPO location to point to the newly copied item in Cohesity Alta SaaS Protection. Same is now referred to during the item restore or download.
  - The **Archival type** of the stub item is labeled as **Moved stub**, **Copied stub**, or **Moved or Copied stub** based on the detected action as describe in the following table.

Scenario	Behavior	Archival method type
Stub is moved	The original item along with all its versions are copied to the new location in Cohesity Alta SaaS Protection.	Moved stub
Stub is copied	Only the latest version of the original item is copied to the new location in Cohesity Alta SaaS Protection.	Copied stub

Scenario	Behavior	Archival method type
The action (move or copy) is undetermined. This behavior can be observed when stubs are moved across sites. Some scenarios in which Cohesity Alta SaaS Protection cannot detect whether a stub was moved or copied in SharePoint. It includes the following: ■ The stub is copied from a library without versioning to another library (with or without versioning). ■ The stub is moved to a library with versioning, and then its properties are changed in SharePoint.	Cohesity Alta SaaS Protection treats it as a move and copies the item.	Moved or copied

- The **Archival method type** of an item in Cohesity Alta SaaS Protection is fixed once set. It does not change after the stub is restored.
- Each time a stub is moved or copied, a copy of the item is created in Cohesity Alta SaaS Protection. This copy counts toward the licensed storage used by Cohesity Alta SaaS Protection.
- If the stub copy or move operation fails to update the stub in SharePoint (for example, due to SharePoint restrictions), users may experience the behaviors described in points a and b below when accessing the stub from SharePoint. In such cases, the Administration portal can be used to access or restore the items directly from Cohesity Alta SaaS Protection.
- If copied or moved stubs are not detected during incremental backups, Cohesity Alta SaaS Protection will process them during the next full backup scan.
- For moved stubs in SharePoint Online, the original item in Cohesity Alta SaaS Protection will be marked as **Removed from Source** only during full backup scans.

- The **Removed from Source** flag will not be carried over to the versions of the copied item.
- If an end-user tries to restore or download items from a copied or moved stub in SharePoint before the item is copied to the new location in Cohesity Alta SaaS Protection, the following may occur:
  - The user may see an Access Denied error if they don't have permission to access the original item in Cohesity Alta SaaS Protection.
  - If the user does have permission to the original item and tries to restore it:
    - (a). The **Copy pending** file will be restored to the original location.
    - (b). The copied or moved stub in SharePoint remains unchanged.
  - If the restore is executed from the Administration portal with the **Restore only stub** option, before the item is copied to the new location in Cohesity Alta SaaS Protection, stubbed files may not be restored at the destination in SharePoint where they were moved or copied.
- In SharePoint, if a retention label is applied to a copied or moved stub at the destination, Cohesity Alta SaaS Protection will not delete the existing version of the stub in SharePoint after updating it.
- If a stub is copied or moved to a library with moderation, minor versioning, or required checkout enabled, the **Modified By** field of the stub in SharePoint will be set to **SharePoint App** during the copy operation.
- The copied items, in Cohesity Alta SaaS Protection, do not retain the Cohesity Alta SaaS Protection policies, legal holds, or retention settings applied to the original items. They are treated as newly backed-up items, and Cohesity Alta SaaS Protection applies policies based on the current configuration.
- The **Archived At** time for copied items in Cohesity Alta SaaS Protection reflects the time the copy operation occurred.
- Newly copied items in Cohesity Alta SaaS Protection will have the same access permissions from the stub at the destination in SharePoint Online.
- If the copy operation within Cohesity Alta SaaS Protection fails, a **Copy pending** flag will be set on the source item in Cohesity Alta SaaS Protection, along with the pending destination path. Items marked as **Copy pending** will be excluded from deletion when Cohesity Alta SaaS Protection deletion policies are run.

- If the stub copy operation fails, Cohesity Alta SaaS Protection will retry it during the next full backup scan. The copy pending path will be cleared after the item is successfully copied. The **Copy pending** flag will be removed only after all pending copies are completed.
- Cohesity Alta SaaS Protection needs to scan the destination location in SharePoint Online to perform the copy. Therefore, you may notice a delay before the copied stub appears in Cohesity Alta SaaS Protection, as it depends on the backup task copying the data and updating the stub.
- Backup task statistics will show details such as the number of updated stubs and the size of the copied data.
- Cohesity Alta SaaS Protection cannot copy an item if the original item is deleted from Cohesity Alta SaaS Protection before the backup task performs the copy. It is the user's responsibility to configure the Cohesity Alta SaaS Protection Deletion Policy properly, ensuring backup tasks have enough time to detect and process copied or moved stubs.

  Example: If a deleted stub in SharePoint is restored from the Recycle Bin after the corresponding item has already been deleted from Cohesity Alta SaaS Protection, the item cannot be copied, and the user will encounter copy errors for that stub.
- If a moved stub is detected to have returned to its original location in SharePoint (as known to Cohesity Alta SaaS Protection), only the **Removed from Source** flag will be cleared, and access permissions (in Cohesity Alta SaaS Protection) will be updated based on existing permissions on source item.
- When a stub is copied or moved across libraries, any columns in the source library that do not exist in the destination library cannot be restored.
- If a stub at a copy-pending path is deleted in SharePoint before Cohesity Alta SaaS Protection can copy the item, the copy pending path will remain on the source item in Cohesity Alta SaaS Protection. If Cohesity Alta SaaS Protection Deletion Policy does not remove such items, please contact support.
- It is not supported to configure the same site for stubbing in multiple connectors. Cohesity Alta SaaS Protection will not copy stubbed items from the same site across different connectors by default. A warning message will appear in the logs in such cases. Support should be contacted for guidance on next steps.
- Cohesity Alta SaaS Protection does not support copying items across different Cohesity Alta SaaS Protection tenants.

    - Backup tasks may take longer to complete if there are many stub move or copy operations in SharePoint that require item copying in Cohesity Alta SaaS Protection.
    - Once the feature is enabled, the backup task will attempt to retroactively correct any previously copied or moved stubs in SharePoint. If the destination SharePoint site, where stub is moved or copied cannot be configured for backup in Cohesity Alta SaaS Protection, then stub access/restore from the SharePoint site may not work.
      For more details, refer to the knowledge base article: Issues when accessing or restoring files from copied or moved stubs (.stub.url) in SharePoint Online.
  - **Stub rename**
    Cohesity Alta SaaS Protection does not support renaming .stub.url files. Renaming .stub.url files may cause issues when restoring the item from Cohesity Alta SaaS Protection.
  - **Modification in Version setting**
    If the versioning setting of a Document Library in SharePoint is changed from 'Create Major/Minor Version' to 'No Versioning' or vice versa, during the next backup cycle, the corresponding item in Cohesity Alta SaaS Protection is marked as **Removed from source**.
  - **Cohesity Alta SaaS Protection deletion policy and items marked as removed from source**
    - If an item in Cohesity Alta SaaS Protection storage qualifies for a Cohesity Alta SaaS Protection deletion policy for deletion, it will be deleted from storage without verifying whether it is stubbed at the source.
    - The **Removed from Source** property can also be used a criterion for Cohesity Alta SaaS Protection deletion policies. This means that deletion policies can remove items marked as **Removed from source** in Cohesity Alta SaaS Protection, even if they are still present at the source (due to certain scenarios described above for example the stub is moved and the location is yet to be scanned by Cohesity Alta SaaS Protection detect the change).
    - Recommendation: It is strongly recommended not to use Cohesity Alta SaaS Protection deletion policies that target content where stubbing is or was enabled at the source.

Connector management:

- For a site being backed up by a connector with a stubbing policy, and that contains stubbed items which have been stubbed by same connector, the stubs

should be restored before removing the site from the connector or deleting the connector.

- For a site being backed up by a connector with a stubbing policy, if the same site is added to a new connector, no data will be backed up for the data that was stubbed the previous connector by the new connector.
- Stubbing same site by multiple connector is not supported.

Item permissions:

- When an item is stubbed, its permissions are not changed. Any changes to the permissions after the item is stubbed are captured by Cohesity Alta SaaS Protection.
- When a stub is restored back to a file by Cohesity Alta SaaS Protection, the permissions the stub had prior to the restore are maintained by default.
- Cohesity Alta SaaS Protection only allows access to files for end-users with the specific SharePoint Permission Levels which contain the Open List Items permission. If a user or group only has SharePoint Permission Levels which contain View Items or View Application Pages permissions, Cohesity Alta SaaS Protection will not permit access to those files. Default SharePoint permission levels that use the View Items permission include Restricted View, View Only, and Download Only. By default such files are not stubbed. When files are stubbed, users with these permission levels will not be able to access the files from the stub.
- For more details on how Cohesity Alta SaaS Protection syncs end-user permissions, refer to the section **End-user SharePoint Data Access in** Cohesity Alta SaaS Protection.
- If Cohesity Alta SaaS Protection backs up and stubs SharePoint sites in two different AD tenants with shared users (for example, a user in Tenant A is also an external user in Tenant B), issues can arise for the shared user if they try to access an item in Cohesity Alta SaaS Protection, via its SharePoint stub in a site present in a tenant where that user is a external. Such a configuration should be avoided.

Item properties:

- When an item is stubbed, its properties and permissions are preserved.
- Any changes to properties made after the item is stubbed are not captured by Cohesity Alta SaaS Protection.
- When a stub is restored back to a file by Cohesity Alta SaaS Protection, the list column properties are restored to the state they were in when Cohesity Alta SaaS Protection initially backed up the item.

Stubbing policy evaluation, configuration, and interaction:

- When configuring exclusions based on type, you must also configure either the last modified date or size criteria.
- The connector stubbing policy will consider an item for stubbing only if all its captured versions meet the criteria configured in the policy.
- The stubbing policy is applied starting from the second full backup, after all data has been successfully backed up during the first full backup.
- The connector stubbing policy applies only to full backups and does not apply to incremental backups occurring between two full backups.
- If both the connector deletion and connector stubbing policies target the same item, the delete policy takes precedence and permanently deletes the item from the source SharePoint environment.

Scope of application of stubbing in SharePoint:

- The stubbing policy applies exclusively to files within document libraries and not to any other library types.
- The stubbing policy specifically applies to items derived from the Document SharePoint content type.

Exclusions from the stubbing policy:

- ASPX files
- Links with a *.url* extension
- Document libraries in SharePoint that have the **Require checkout** setting enabled.

  Some site templates, like Publishing Site, create document libraries with this setting enabled. As a result, items in these libraries cannot be stubbed.

  Contact Cohesity Support to enable stubbing for these items.
- Files in libraries and lists with the Information Rights Management (IRM) setting enabled.
- Items that are checked out.
- Thicket file.
- Starting from the 2.26.1 release, the following items cannot be stubbed using the Stubbing policy:
  - All items in sites, which are on legal hold or have a retention policy.

    You need to contact Cohesity Support to enable stubbing for these items.
  - Only when Legal Holds done through Microsoft Purview by link Create eDiscovery holds in an eDiscovery case Microsoft Learn, Cohesity Alta SaaS Protection can detect, and skip stubbing for such items. Any other way is unsupported. Legal holds applied through any other way are unsupported,

as a result Cohesity Alta SaaS Protection's stubbing process will not be able to detect legal holds and continue to stub the items in the site and may result in unsupported behavior (for example, items may appear as a stub but versions may still remain in SharePoint).

Contact Cohesity support team to stub other items in such sites.

- Starting from the 2.28.1 release, the following items cannot be stubbed:
  - Items with a sensitivity label configured for encryption cannot be stubbed.
  - Items in read-only sites.
  - Items marked with a retention label and still within the retention period.
- Starting from the 2.31.1 release, the following items cannot be stubbed:
  - Items in lists and libraries with the following version settings enabled in SharePoint Online:
    - Require content approval for submitted items.
    - Create major and minor (draft) versions (for example, 1.0, 1.1, 1.2, 2.0)
    - Some site templates, like Publishing Site, create document libraries with these settings, preventing stubbing in such libraries for the site.
  - Cohesity Alta SaaS Protection does not support the stubbing of Loop components in emails and Teams chats.

    For more information on Loop components, refer to the Microsoft knowledge base article: Overview of Loop Components in Microsoft 365.
- Starting from the 2.35.1 release, the items/files with **View only** permission will not be stubbed.
- OneNote notebooks.

Sharing links:

- Sharing links (by Teams, OneDrive, or SharePoint) for items created before and after stubbing may not work.

Accessing stubs via the SharePoint App on Mobile devices:

- Accessing stubs through the Microsoft SharePoint App on iOS and Android is not supported. Users can open the SharePoint site in Safari or Chrome, navigate to the library containing the stub, and click on it to access the data in Cohesity Alta SaaS Protection.

Files synchronized with Laptops and PCs:

- When files synchronized with laptops or PCs using the OneDrive client are stubbed, Cohesity Alta SaaS Protection replaces the items with internet shortcuts, adding the .stub.url extension to the item name.

- When an end user tries to access the stubbed file from File Explorer, they are navigated to a browser. Based on the settings configured in Cohesity Alta SaaS Protection for managing end-user experiences with stubs, appropriate actions will be taken. Refer to the **Managing End-User Experience with Stubbed Items** section for more details.
- When stubbing a file the OneDrive Sync client may add or/and change the stub file. Cohesity does not support the scenario, if the change disrupts the functioning of the stub.

Inconsistent stubbed files:

- Errors can occur at any stage of the stubbing process. The stubbing process attempts to recover from errors by either keeping the original file intact as much as possible or fully stubbing the item.
- For more information on how to handle these errors, refer to the tech note: Cohesity Alta SaaS Protection: Microsoft SharePoint Online Item Stubbing Errors.

Browser support:

- The following browsers are supported for accessing data in Cohesity Alta SaaS Protection by a stub:

Browser	Restore and Download stub	Download only
Chrome	Supported	Supported
Edge	Supported	Supported
Safari	Not supported	Supported

Stub modifications:

- If there are any external modifications to the stub by any processes other than Cohesity Alta SaaS Protection, this may lead to unsupported scenarios – for example, external processes like a different backup vendor, SharePoint workflows.

See "Run the Delete and Stubbing policies to the SharePoint Online environment" on page 151.

Handling of orphan stubs

- A Cohesity Alta SaaS Protection stub in SharePoint is orphaned when the data that it refers to in the backup storage is deleted from Cohesity Alta SaaS Protection. This can happen due to Cohesity Alta SaaS Protection deletion policies running in Cohesity Alta SaaS Protection or through a manual deletion

action from Cohesity Alta SaaS Protection. There is an option to clean up such stubs from SharePoint sites. This cleanup happens during a backup task. This is disabled by default. You can contact support to enable this feature. When enabled, this happens every 15 days, this interval can be changed.

- Orphan stub deletion is only performed during full backup tasks and not in incremental tasks.
- For a stub created for a file in a SharePoint versioned library, a stub is considered as orphan only if all versions in backup storage have been deleted from Cohesity Alta SaaS Protection. Note that SharePoint versions present in Cohesity Alta SaaS Protection but marked as **Removed from source** are also considered in the above check. So, if all available versions in Cohesity Alta SaaS Protection backup are marked as **Removed from Source**, the functionality will consider the stub as orphan and delete it from Site.

Managing end-user experience with stubbed items

- For more information on the end-user workflow when an end-user clicks on a stub, refer to the topic *Restore OneDrive/SharePoint stubbed items* in the Cohesity Alta SaaS Protection End User Guide.
- As an administrator, you can control the options available to the end-user. You can direct them to the End-User portal to restore the specific item or initiate the download when a stub is clicked. You can use the following permissions to manage the experience of the end user in restoring or downloading the stubbed items:
  - **End-User SharePoint stubbing restore**: With this permission, when an end-user clicks on the stubbed item, they are redirected to a webpage. On this webpage, an option is available to restore the item to its original location at the time of backup.
  - **End-User retrieval and download**: With this permission, when an end-user clicks on the stubbed item, they are redirected to a webpage. On this webpage, an option is available to download the last backed-up version of the SharePoint file to the local computer.

    If only this permission is assigned, the download starts when the user clicks the stub.

    Both of these permissions are inherently included in the **Default** role.
- You can monitor the restore progress on the **Restore dashboard**.

Notes on the restoration of stubbed items initiated by end-users

- A SharePoint user with the View permission can restore the file. The user retains the same permissions for the file after restoration as they had on the stub.

- If an end-user tries to restore or download items from a copied or moved stub in SharePoint before the item is copied to the new location in Cohesity Alta SaaS Protection, the restore operation may fail. for more details, refer to the Stub movement section.
- The last modified date is updated to the current time after restoration or download. This should prevent the item from being picked up by the configured Stub policy if configured based on the last modified time.
- Only the last backed-up version of the SharePoint item before the stubbing occurred is restored.

  When an end-user performs a restore to unstub an item, only the latest version is restored. All other versions are marked as 'Removed from source' during the next backup.
- You can monitor the restore progress on the Restore dashboard, but you cannot rerun the restore.
- If your tenant is Scope enabled, then clicking on a stub always download the last backed-up version of the SharePoint file to the local computer.

Schedule a backup

You can schedule automated backups to ensure that data is backed up at regular intervals.

To schedule a backup

1. Click **+ Add backup schedule**.
2. On the **+ Add backup schedule** page, configure the following options:
   - **Start time**: Enter the time to start the backup.
   - **Duration in hours**: Enter the number of hours the backup should run.
   - **Recurrence**: Set the recurrence option for the backup schedule.
3. Click **Add**.
4. Click **Next**.

Next step:

Perform any of the applicable:

- See “Configure email addresses to get notifications” on page 116.
- See “Review configuration and edit/save/initiate backup” on page 116.

Configure email addresses to get notifications

(Optional) If you have enabled the **Enable email notification options** option while configuring the general settings to receive notifications, do the following:

- Click **Enable this feature** > enter the email address of the user who should get notifications on connector creation and backup activities.
- Select the **Send an email when error count exceeds** check box > enter the number.
- Click **Next**.

Review configuration and edit/save/initiate backup

After configuring the connector, go to the **Review** tab and perform one of the following actions:

To edit the connector configuration

1. Click the **Edit** option next to the tab name.

   Click the **Edit** option located next to the tab name.
2. After making the edits, click **Review** on the left panel to proceed.

To save the connector configuration

1. Click **Save**.
2. Go to the **Connectors** page to verify the connector status.

   The status should be **Created**.

To save the connector configuration and run the initial backup

1. Click **Save and Backup**.
2. For Microsoft 365 connectors, ensure that the Microsoft 365 app registrations that are provisioned for the connector are in an **Active** state before running the backup.
   - If the assigned apps are not active, the connector status displays as **Pending app activation**, and backups cannot be initiated.
   - You must grant admin consent for the provisioned apps before starting backups.
3. Once the backup begins, go to the **Connectors** page to monitor the progress.
   - The status displays as **Initial Running (backup)** for the first backup.

- For subsequent backups, the status updates to **Running**.

If you choose not to run the backup during connector creation using the **Save and Backup** option, you can initiate the backup later from the **Connectors** page.

Related topics:

- See "Perform on-demand/ad-hoc backup" on page 239.
- See "Connectors page" on page 117.
- See "Connector status" on page 119.

Connectors page

The **Connectors** page displays all the connectors added to Cohesity Alta SaaS Protection, along with details such as their status, next backup schedule, and more. You can also use this page to add new connectors.

You can perform the following actions on the page:

Table 8-3

Actions	Description
View connector details.	Click the connector name to view its details.
Add a new connector.	Click **New connector** to start the connector creation process.
Filter the connector list.	Use the **All** dropdown list to filter the list by connector type or status.
Search for a connector.	Enter the name of the connector in the **Filter by name** field.
Edit a connector.	Click the name of the connector to start the edit workflow.
Initiate a backup.	Click within the row of the required connector > **Backup now**.
Manage a connector.	Click within the row of the connector > click the action menu (**...**) and perform the following actions: - Click **Copy** to create a duplicate connector. - Click **Delete** to remove the connector.

Table 8-3 *(continued)*

Actions	Description
View tasks performed on a connector.	Click within the row of the connector > **Tasks**.
View backup events.	Click within the row of the connector > **Events**.

Tasks tab

The **Tasks** tab provides detailed information about all backup-related tasks associated with the selected connector.

Task Details: Upon selecting a specific task, users can view comprehensive task-related data, including:

- Backup Statistics
- Backup Details
- Bulk Item Details
- Item Details
- Location Details

Error Logs

Within the Tasks section, there is an Error Logs tab that redirects to a dedicated page displaying detailed log information. This page provides visibility into:

- Site collections that completed with errors
- Successfully completed backups
- Failed backups
- Items that were not processed

Users can apply filters to view:

- All Errors
- Persistent Errors (recurring issues)

Events Tab

The **Events** tab provides insights into connector-level events and offers multiple filtering and viewing options. It consists of the following sub-tabs:

- Last Backup: Allows the user to select a specific backup (based on date and time) and view all associated event details, including errors and other event types related to that backup.

- All Types: Enables the user to filter and view events by category. Available options include:
  - All Types
  - Error
  - Warning
  - Informational
  - Verbose
  - Diagnostic

  The event list updates dynamically based on the selected filter.
- Errors: Provides the option to view either:
  - All Errors
  - Persistent Errors
- General Event: Details For each event, detailed information is displayed, including:
  - Event Type
  - Timestamp
  - Message
  - Exception Details

Related topics:

- See "Connector status" on page 119.

Connector status

You can view the status of the connector on the **Connectors** page.

Table 8-4

Columns on the Connectors page		Description
Status	**Pending app activation**	It indicates that the Microsoft 365 apps are activated by granting the admin consent.
	Created	It indicates that the connector is successfully added but the backup is not yet started.
	Initial Running (backup)	It indicates that the backup is run on the newly created connector for the first time. Any subsequent backups will have the status as **Running**.
	Running	It indicates that the backup is running.
	Completed	It indicates that the backup is completed without errors.
	Completed with errors	It indicates that the backup is completed with errors. Errors should be investigated and suppressed if they appear.
	Stale	It indicates that the backup did not run during the last scheduled backup.
Last backup count	The total number of items or site collections that are backed up during the last backup.	
Type	The type of the source SaaS application, such as Exchange, SharePoint, and so on.	
Last backup statistics	The last capture count is broken down by: ■ Completed without errors (green) ■ Completed with errors (orange) ■ Pending (Connector is running) (gray) ■ Not processed (Connector is completed) (gray) The progress bar displays the progress based on the statistics.	
Last backup date	The duration since the last manual or scheduled backup.	
Next scheduled backup	The next scheduled backup time. A connector without a schedule will be blank.	

Edit connector configuration

You can modify an existing connector's configuration through the Administration portal.

To edit connector configuration

1. Access the Administration portal.
2. Click **Administration** > **Connectors**.
3. Click the connectors.
4. Make the required changes and then click **Save** to save the changes.

Note: The Capture scope of the connectors that are added or updated using the Connector service cannot be edited using the Administration portal.

Related topics:

- See "Connector status" on page 119.
- See "Connectors page" on page 117.

Delete connectors

The data backed up using the connector you deleted is marked as Removed from source.

To delete a connector

1. Access the Administration portal URL.
2. Click **Administration** > **Connectors**.
3. Click within the row of the connector, click the ellipses icon on the top, and then click **Delete**.
4. On the **Delete Connector** page, click **Delete** to continue with deleting the connectors.

Chapter 9

Pre-requisites to setup protection for M365

This chapter includes the following topics:

- Pre-requisites to setup protection for M365

Pre-requisites to setup protection for M365

The following Cohesity Alta SaaS Protection connectors are used to protect Microsoft 365 workloads:

- Exchange Online connector for Exchange Online mailboxes, folders, messages, and attachments.
- SharePoint Online connector for SharePoint Online sites, folders, files, permissions, and metadata.
- OneDrive for Business connector for OneDrive for Business sites, folders, files, permissions, and metadata
- Teams sites collection connector for Teams site, folders, files, permissions, and metadata
- Teams chat connector for Teams messages, meeting recordings, and attachments

For more details on the backup capabilities and limitation on these connectors, See "Supported SaaS workloads and backup capabilities" on page 37.

Pre-requisites

For Microsoft 365 workload protection, its is must to synchronize your Entra ID with Cohesity Alta SaaS Protection.

Entra ID synchronization is required to provide centralized identity management, enabling features like Single Sign-On (SSO), access control, and automated user provisioning. It ensures consistent user authentication across applications, enhances security with policies like multifactor authentication (multifactor authentication), and simplifies user management. Synchronization also supports compliance by maintaining up-to-date user directories and enforcing role-based access. Overall, it ensures a seamless and secure experience for users while maintaining control and compliance in cloud environments.

The Azure Global administrators receive an email notification from Cohesity, asking them to approve the Entra ID synchronization request. The email includes a link to approve the Entra ID synchronization app registration in the following format:

https://login.microsoftonline.com/contoso.onmicrosoft.com/adminconsent?client_id=25fb04f2-f2ac-405b-ac01-c39ad4ee6a26

Any of Azure Global administrators should do the following to synchronize Entra ID with Cohesity Alta SaaS Protection:

- Replace *contoso.onmicrosoft.com* in the above link with your primary domain.

  Note: Your primary domain is listed on the Microsoft Entra Overview page of the Azure portal.

- Approve the app with the `25fb04f2-f2ac-405b-ac01-c39ad4ee6a26` ID.

The Entra ID synchronization app requests the following permissions:

- **Directory.read.all**: This permission is required to read directory data.
- **User.read**: This permission is required to sign in and read the user profile.

Depending on the size of your data, synchronization may take several hours.

The synchronization process synchronizes the users and groups in your Entra ID to Cohesity Alta SaaS Protection. After synchronization is completed, Cohesity Alta SaaS Protection gets information of the users and groups in your Entra ID.

The following information is also synchronized along with the users and groups:

- User account status (enabled or disabled)
- Group memberships
- Extended Entra ID attributes such as user's department, job title, preferred data location, and so on. (If the extended Active Directory attribute is enabled in your Azure.)

Pre-requisites for Entra ID synchronization

The following are the prerequisites for Entra ID synchronization:

- You must have Entra ID deployed for your organization.
- You must enable Entra ID synchronization in Azure to synchronize your on-premises Active Directory with your Entra ID. The Microsoft Entra ID Connect tool is used to enable the Active Directory synchronization.
- You also need to enable the extended Azure Active Directory attributes in Azure to get all features related to SharePoint and OneDrive connectors of Cohesity Alta SaaS Protection.

Features that required Entra ID synchronization

Entra ID synchronization is a must process for the following features of Cohesity Alta SaaS Protection:

- End-User portal and End User file access through stub:
  Accessing the SharePoint stubs configured with multiple Active Directories can cause issues.
  See "End-user SharePoint data access in Cohesity Alta SaaS Protection" on page 148.
- Link-based storage tiering
- Location-mapping policies
  The following features required the extended Entra ID attribute along with the Active Directory synchronization:
  - Exchange connectors that use the extended Entra ID attributes to filter the in-scope mailboxes.
  - SharePoint connectors that use the extended Entra ID attributes to filter the in-scope OneDrive for business site collections.

Limitations if Entra ID synchronization is not enabled

The following are the limitations if you have not enabled the Entra ID synchronization in Azure:

- The Custodian-scoped search gives a result of explicit user permissions only; the access rights of group memberships are not displayed in the result. Search for a group gives no result as Cohesity Alta SaaS Protection has no knowledge of group memberships.
- Policies that use the Custodian (inclusion or exclusion) clauses give a result of explicit user permissions only.
- Policies that use Custodian attribute (inclusion or exclusion) clauses give no result.

Chapter 10

Protect Microsoft 365 Multi-Geo tenant

This chapter includes the following topics:

- Considerations for adding SharePoint/Teams Sites/OneDrive connectors for Microsoft 365 Multi-Geo tenant

Considerations for adding SharePoint/Teams Sites/OneDrive connectors for Microsoft 365 Multi-Geo tenant

Cohesity Alta SaaS Protection supports the backup and restore of SharePoint sites, Teams sites, and OneDrive for Microsoft 365 tenants configured across multiple geographic locations by creating separate connectors for each location and backup requirement. During the connector configuration, ensure that the correct URL is specified.

Example scenario:

A Microsoft 365 tenant's default location is North America, with an additional location in Europe. This tenant has OneDrive, Teams sites, and SharePoint sites at both locations. To configure the connectors appropriately for the following backup requirements, create one connector per location that is one for North America (the default location) and another for Europe. Use the URLs specified in the following table.

Table 10-1

Backup requirements	Location	Admin Site URLs for SharePoint and Teams sites	URLs for OneDrive
■ To backup all OneDrive ■ To backup all Teams Sites ■ To backup all SharePoint sites	North America	https://company-admin.sharepoint.com	■ Admin Site URL: https://company-admin.sharepoint.com ■ My Site/OneDrive Site Collection base URL: https://company-my.sharepoint.com
	Europe	https://company-EUR-admin.sharepoint.com	■ Admin Site URL: https://company-EUR-admin.sharepoint.com ■ My Site/OneDrive Site Collection base URL: https://company-EUR-my.sharepoint.com

Chapter 11

Protect Exchange Online data

This chapter includes the following topics:

- Setting up Exchange Online data protection with Cohesity Alta SaaS Protection

Setting up Exchange Online data protection with Cohesity Alta SaaS Protection

To protect user's data in your Exchange Online environment using Cohesity Alta SaaS Protection, you need to **add and set up a Cohesity Alta SaaS Protection Exchange connector** based on your backup requirements.

Before you begin:

You must consider the following points before adding a connector.

- **Ensure that all prerequisites are completed.**
  See "Pre-requisites to setup protection for M365" on page 122.
- **The following items are supported for backup and restore:**
  - Mailboxes
    - User mailboxes
    - Group mailboxes
    - Teams mailboxes
  - Public Folders
  - Archive mailboxes
  - Shared mailboxes

  - Contacts and calendars
  - Tasks and notes
  - Mailbox Rules
  - Junk Email and Deleted Items: Junk email and deleted items folders to restore accidentally deleted or wrongly categorized emails.
  - Soft deleted mailboxes: This option can be configured using Connector service.
  - Recoverable items folder: An option to back up the Recoverable Items folder, which stores items recoverable after deletion.
  - Archived mailboxes: An option to back up archived mailboxes, ensuring that all user data, including archived content, is backed up.
  - Public folders: An option to back up Public folders.
  - Groups created using the Role assigned and Dynamic users options.
- **Other considerations**:
  The emails in the EWS environment are backed as `.eml` files. Cohesity Alta SaaS Protection receives these .eml files from Exchange, containing the original email as an encrypted attachment and a message body indicating that the email is encrypted. To view these .eml files, they must be downloaded/restored from Cohesity Alta SaaS Protection and opened in Outlook by a user with the necessary permissions.
- **Connector features**:
  - Flexible mailbox backup options
    Back up all user mailboxes or selectively back up specific mailboxes (granular backup) based on backup requirements.
  - Rolling Mailbox Scope to distribute the backup load across jobs.
  - Alphabetical Mailbox Scope to back up mailboxes based on alphabetical name ranges.
  - Back up mailboxes belonging to specific email domains.
  - Back up all or selected Microsoft 365 Group and Teams mailboxes.
  - Back up Public folders in the Exchange Online environment.

Note: The emails in the EWS environment are backed as `.eml` files. Cohesity Alta SaaS Protection receives these .eml files from Exchange, containing the original email as an encrypted attachment and a message body indicating that the email is encrypted. To view these .eml files, they must be downloaded/restored from Cohesity Alta SaaS Protection and opened in Outlook by a user with the necessary permissions.

Video tutorial to add an Exchange Online connector:

To add an Exchange connector, follow the procedure outlined on this page or watch the video tutorial below:

http://video.symantec.com/services/player/bcpid292374537001?bckey=AQ~~,AAAABuIiy9k~,I8Bhas-Vwr9zYL9V36WFi86fR_NoePscn&bctid=6362510350112

Step-by-step procedure to add an Exchange Online connector:

1. Access the Administration portal.

   The home page of the Administration portal is displayed.

2. Click **Connectors** on the **Backup** card.

3. Click **New backup connector**.

4. Click **Exchange**.

   To make the setup process easier and more intuitive, each tab in the connector creation workflow includes a help icon **(?)** at the left. You can click this icon to open the respective help topic for that tab, which can guide you through the setup step by step.

5. On the **General** tab, set up the basic configuration for the connector and click **Next**.

   See "Configure General settings" on page 83.

6. On the **Configure scope** tab, configure the capture scope to define which data to be protected and click **Next**.

   See "Configure capture scope for Exchange connectors" on page 130.

7. On the **Credentials** page, configure credentials to access the source workloads (the SharePoint data to be backed up) and click **Next**.

   See "Configure credentials" on page 88.

8 On the **Policy configuration** tab, configure the appropriate backup policy for more granular backup needs.

See "Configure Custom backup policy and guidelines" on page 93.

9 On the **Scheduling** tab, schedule when the backup job should run.

See "Schedule a backup" on page 115.

10 On the **Email notifications** tab, configure email addresses to receive notifications about backup activities.

See "Configure email addresses to get notifications" on page 116.

11 On the **Review** tab, save the settings and initiate the backup.

See "Review configuration and edit/save/initiate backup" on page 116.

Configure capture scope for Exchange connectors

Note: To know more about the maximum number of users data that can be backed up, contact Cohesity Support. You can also go to the **Licenses** page to view your subscription details.

You can use one of the following procedures as per your backup requirement:

To configure capture scope to back up mailboxes of all users

1 From the **Exchange settings** section, click **User mailboxes** and then click **All mailboxes**.

2 Configure folder filter to limit the backup scope to specific folders in the mailboxes of users:

See "Configure Folder filter" on page 87.

3 (Optional) Do the following:

- Select the **Recoverable items** check box to back up items in the **Recoverable Items** folder.

- Select the **Archive mailboxes** check box to back up items in the **Archive** folder.

4 Click **Next** to configure credentials.

See "Configure credentials" on page 88.

To configure the capture scope to back up the mailboxes of all users using the Rolling mailbox scope option

Important: With the 2.32.1 release, this option will not be available for new connectors. For existing connectors, this option will appear as read only.

If you have a large number of mailboxes in your Exchange Online environment, the backup scope can become extensive. You can configure the capture scope using the **Rolling mailbox scope** option to manage this scenario. By selecting this option, you can map a specific number of mailboxes to be included in the backup. It helps minimize the load on any one connector. You can configure multiple connectors to cover all the mailboxes in your environment.

Note: To know more about the maximum number of mailboxes that can be backed up, contact Cohesity Support. You can also go to the **Licenses** page to view your subscription details.

---

1 From the **Exchange settings** section, click **User mailboxes** and then click **All mailboxes**.

2 Click the **Rolling mailbox scope** option and do the following:

- Enter the number of mailboxes that you want to map to this connector in the **No. of mailboxes in scope** field.
  Only the specified number of mailboxes can be backed up using this connector.

3 (Optional) Configure filters to limit the backup scope to specific users based on their Entra ID attributes.

See "Configure User filter" on page 85.

See "Configure Group filter" on page 86.

4 (Optional) Configure folder filter to limit the backup scope to specific folders in the mailboxes of users.

See "Configure Folder filter" on page 87.

5 (Optional) Do the following:

- Select the **Recoverable items** check box to back up the **Recoverable Items folder**.

- Select the **Archive mailboxes** check box to back up the archived mailboxes.

6 Click **Next** to configure credentials.

See "Configure credentials" on page 88.

To configure the capture scope to back up the mailboxes of users using the Alphabetical mailbox scope option

Important: With the 2.32.1 release, this option will not be available for new connectors. For existing connectors, this option will appear as read only.

If you have a large number of mailboxes in your Exchange Online environment, the backup scope can become extensive. To manage this scenario, configure the capture scope using the **Alphabetical mailbox scope** option. You can map a range of mailboxes to be included in the backup. It helps minimize the load on any one connector. To cover all the mailboxes in your environment, you can configure multiple connectors.

Note: To know more about the maximum number of mailboxes that can be backed up, contact Cohesity Support. You can also go to the **Licenses** page to view your subscription details.

---

1 From the **Exchange settings** section, click **User mailboxes** and then click **All mailboxes**.

2 Click the **Alphabetical mailbox scope** option and do the following:

- Enter the range of email addresses that you want to back up using this connector.

  For example, if you specify the start letter as 'A' and the end letter as 'F', all email addresses within the range of 'A' to 'F' are included in the backup scope.

  The mailboxes are processed based on the first letter of the email address.

  If you are using the **Alphabetic mailbox scope,** you may need to enable the **Include mailbox not starting with the letter** option for one of the connectors. It backs up the mailboxes of the users whose email addresses do not begin with an alphabet.

3 (Optional) Configure filters to limit the backup scope to specific users based on their Entra ID attributes.

See "Configure User filter" on page 85.

See "Configure Group filter" on page 86.

4 (Optional) Configure folder filters to limit the backup scope to specific folders in the mailboxes of users.

See "Configure Folder filter" on page 87.

5 (Optional) Do the following:

- Select the **Recoverable items** check box to back up items in the **Recoverable Items** folder.
- Select the **Archive mailboxes** check box to back up items in the **Archive** folder.

6 Click **Next** to configure credentials.

See "Configure credentials" on page 88.

You can use the following procedure to limit the capture scope to specific domains only.

Note: To know more about the maximum number of users data that can be backed up, contact Cohesity Support. You can also go to the **Licenses** page to view your subscription details.

To configure the capture scope to back up the mailboxes of specific users only

1 From the **Exchange settings** section, click **User mailboxes** and then click **Specific mailboxes**.

2 Do the following:

- Click **+ Add SMTP addresses**.
- On the **Add SMTP Addresses** page, enter the email addresses of the users, groups, or Teams that are to be backed up using this connector. Use semicolons between addresses.
- Click **Add**.

3 (Optional) Configure the folder filters to limit the backup scope to specific folders in the mailboxes of users.

See "Configure Folder filter" on page 87.

4 (Optional) Do the following:

- Select the **Recoverable items** check box to back up items in the **Recoverable Items** folder.

- Select the **Archive mailboxes** check box to back up items in the **Archive** folder.

5 Click **Next** to configure credentials.

See "Configure credentials" on page 88.

To configure the capture scope to back up mailboxes from specific domains only

You can use the following procedure to limit the capture scope to specific domains only.

Note: To know more about the maximum number of users data that can be backed up, contact Cohesity Support. You can also go to the **Licenses** page to view your subscription details.

---

1 From the **Exchange settings** section, click **All mailboxes**.

2 Select the **Limit backup to specific domains** check box > enter domain SMTP addresses in the **Domain names** section.

3 Do the following:

- Click **+ Add SMTP addresses**.
- On the **Add SMTP Addresses** page, enter domain names.
  Use semicolons between addresses.
- Click **Add**.

4 (Optional) Configure folder filters to limit the backup scope to specific folders the mailboxes of users.

See "Configure Folder filter" on page 87.

5 (Optional) Do the following:

- Select the **Recoverable items** check box to back up items in the **Recoverable Items** folder.

- Select the **Archive mailboxes** check box to back up items in the **Archive** folder.

6 Click **Next** to configure credentials.

See "Configure credentials" on page 88.

To configure the capture scope to back up all Group/Teams mailboxes

To enable Dynamic group mailbox backup using PowerShell as the management API, provide an impersonation account representing a member or owner of the respective group. Adding an impersonation account is mandatory for Modern/OAuth authentication. In this case, the provided users are added as members or owners (in the case of Dynamic groups) to all groups and Teams that are in backup scope.

1 From the **Exchange settings** section, click **Group/Teams mailboxes** and then click **All mailboxes**.

2 (Optional) Configure the folder filter to limit the backup scope to specific folders in the mailboxes of users.

See "Configure Folder filter" on page 87.

3 (Optional) Do the following:

- Select the **Recoverable items** check box to back up items in the **Recoverable Items** folder.
- Select the **Archive mailboxes** check box to back up items in the **Archive** folder.

4 Click **Next** to configure credentials.

5 Click **+ Add impersonations**.

6 On the **EWS OAuth Impersonation User SMTP addresses** page, enter impersonation accounts, click **Add**.

Use semicolons between email addresses.

The added account is displayed page.

7 Click **Next** to configure credentials.

See "Configure credentials" on page 88.

To configure the capture scope to back up specific Group/Teams mailboxes

1 From the **Exchange settings** section, click **Group/Teams mailboxes** and then click **Specific mailboxes**.

2 Do the following:

- Click **+ Add SMTP addresses**.
- On the **Add SMTP Addresses** page, enter the email addresses of the users, groups, or Teams that are to be backed up using this connector. Use a semicolon between addresses.
- Click **Add**.

3. (Optional) Configure the user filter to limit the backup scope to specific users based on their Entra ID attribute.

   See "Configure Group filter" on page 86.

4. (Optional) Configure the folder filter to limit the backup scope to specific folders in the mailboxes of users.

   See "Configure Folder filter" on page 87.

5. (Optional) Do the following:
   - Select the **Recoverable items** check box to back up the **Recoverable Items folder**.
   - Select the **Archive mailboxes** check box to back up the archived mailboxes.
6. Click **Next** to configure credentials.
7. Click **+ Add impersonations**.
8. On the **EWS OAuth Impersonation User SMTP addresses** page, enter impersonation accounts, click **Add**.

   Use semicolons between email addresses.

   The added account is displayed page.
9. Click **Next** to configure credentials.

   See "Configure credentials" on page 88.

You can use the following procedure to back up Public folders in your Exchange Online environment.

To configure the capture scope to back up Public folders

1. From the **Exchange settings** section, click **Public Folders**.
2. (Optional) Configure folder filter to limit the backup scope to specific folders.

   See "Configure Folder filter" on page 87.
3. Click **Next** to configure credentials.
4. Click **+ Add impersonations**.

5 On the **EWS OAuth Impersonation User SMTP addresses** page, enter impersonation accounts, click **Add**.

The added account is displayed page. The impersonated user must have a mailbox and full access to the entire Public folder hierarchy.

6 Configure the credentials.

See "Configure credentials" on page 88.

7 Click **Next**.

Chapter 12

Protect SharePoint sites and data

This chapter includes the following topics:

- Setting up SharePoint Online protection with Cohesity Alta SaaS Protection
- Backup and restore support for SharePoint Online
- End-user SharePoint data access in Cohesity Alta SaaS Protection
- Run the Delete and Stubbing policies to the SharePoint Online environment
- Backup limitations for SharePoint Online

Setting up SharePoint Online protection with Cohesity Alta SaaS Protection

To protect user's data and sites in your SharePoint Online environment using Cohesity Alta SaaS Protection, **you need to add and set up a Cohesity Alta SaaS Protection SharePoint Online connector** based on your backup requirements.

Before you begin:

Consider the following points before adding a connector.

- **Ensure that all prerequisites are completed.**
  See "Pre-requisites to setup protection for M365" on page 122.
- **The items that are supported for backup and restore are listed in the following topics:**
  - See "Supported and unsupported SharePoint Objects, Properties, Settings, and Types for backup and restore" on page 144.

  - See "Supported Sites and List templates for backup and restore" on page 146.
  - See "Supported SharePoint permission objects for backup and restore" on page 148.
- **The items that are not supported for backup and restore are listed in the following topics:**
  - See "Backup limitations for SharePoint Online" on page 151.
  - See "Restore limitations for SharePoint Online" on page 283.
- **Other considerations:**
  - Using the SharePoint connector, you can back up all or specific SharePoint sites based on your backup requirements. You need to create separate connectors for these requirements.
  - The SharePoint connector can only back up the site collections that are not associated with Microsoft 365 Groups and Teams (except Communication sites). To back up Microsoft 365 Groups and Teams, use the Teams Site Collection connector with the **All group and team site collections** option.
  - For Microsoft 365 Multi-Geo tenants, See "Considerations for adding SharePoint/Teams Sites/OneDrive connectors for Microsoft 365 Multi-Geo tenant" on page 125.
- **Connector features:**
  - Custom backup policy: You can define specific data types, versions, permissions, columns, and content types to back up.
  - Delete policy: You can define a Delete policy to manage storage by removing unnecessary items from the source SharePoint Online environment while retaining backups in Cohesity Alta SaaS Protection.
    See "Configure Delete policy for SharePoint Online and guidelines" on page 95.
  - Stubbing policy: you can define a Stubbing policy to replace original items with stubs (shortcuts) in the SharePoint Online environment, which helps reduce storage usage while maintaining access to data.

Video tutorial to add a SharePoint connector:

To add a SharePoint Online connector, follow the step-by-step procedure outlined on this page or watch the following video tutorial:

http://video.symantec.com/services/player/bcpid292374537001?bckey=AQ~~,AAAABuIiy9k~,I8Bhas-Vwr9zYL9V36WFi86fR_NoePscn&bctid=6362511129112

Step-by-step procedure to add a SharePoint connector:

Each tab in the connector creation workflow includes a help icon (?) on the left. Click this icon to open the corresponding help topic for that tab, which guides you through the setup process step by step.

Procedure:

1. Access the Administration portal.
2. On the home page, click **Connectors** on the **Backup** card.
3. Click **New backup connector**.
4. **Configure the general settings.**

   Click **SharePoint**.
5. On the **General** tab, set up the general configuration for the connector and click **Next**.

   See "Configure General settings" on page 83.
6. **Configure the capture scope.**

   On the **Configure scope** tab, configure the capture scope to define which SharePoint sites or content should be protected and click **Next**.

   See "Configure capture scope for SharePoint connectors" on page 141.
7. **Configure credentials.**

   On the **Credentials** tab, configure credentials to access the source workloads (the SharePoint data to be backed up) and click **Next**.

   See "Configure credentials" on page 88.
8. **Configure policies.**

   On the **Policy configuration** tab, do the following as per your backup requirements:

   - Configure the appropriate backup policy for more granular backup needs.
     See "Configure Custom backup policy and guidelines" on page 93.
   - Configure the Delete and Stubbing policies to free up SharePoint storage by removing unwanted items after backup.
     See "Configure Delete policy for SharePoint Online and guidelines" on page 95.
     See "Configure Stubbing policy" on page 100.
     See "Guidelines to configure Stubbing policy for SharePoint Online" on page 102.

9 **Configure backup schedule.**

On the **Scheduling** tab, schedule when the backup job should run.

See "Schedule a backup" on page 115.

10 **Configure email address.**

On the **Email notifications** tab, configure email addresses to receive notifications about backup activities.

See "Configure email addresses to get notifications" on page 116.

11 **Save configuration.**

On the **Review** tab, save the settings and initiate the backup.

See "Review configuration and edit/save/initiate backup" on page 116.

Related topics:

- See "Connector status" on page 119.
- See "Perform on-demand/ad-hoc backup" on page 239.
- See "Video tutorial for connector troubleshooting" on page 241.
- See "Restore SharePoint/OneDrive/Teams Sites and data" on page 272.

Configure capture scope for SharePoint connectors

The capture scope for the connector is configured on the **Capture scope** tab of the connector creation workflow.

The following is an overview of how to configure the capture scope for a SharePoint connector:

- **Step 1:**
  Choose whether to back up all sites or specific sites and then enter its Admin center URL.
- **Step 2:**.
  Configure additional backup options such as permission and settings.
  See "Configure additional backup options for SharePoint/Teams site/ OneDrive connectors" on page 142.
- **Step 3:**.
  (Optional) Define filters to limit the backup scope to specific folders.
  See "Configure Folder filter" on page 87.

You can use one of the following procedures as per your backup requirement:

To backup all sites:

1. Click **All site collections**.
2. To enter the Admin center URL:
   - Click the **Use default** icon next to the **Admin site URL** option.
     The default URL is ***https://<company>-admin.sharepoint.com***.
   - Replace ***<company>*** with the name of your organization or tenant.
3. Perform step 2.
4. Perform step 3.

To backup specific sites only:

1. Click **Specific site collections**.
2. To enter the Admin center URL:
   - Click the **Use default** icon next to the **Admin site URL** option.
     The default URL is populated in the field as ***https://<company>-admin.sharepoint.com***.
   - Replace ***<company>*** with the name of your organization or tenant.
   - Click **+ Add specific site collection**, and do the following:
     - On the **+ Add specific site collection** page, click the **Use default** icon next to the **Admin site URL** option.
       The default URL is populated in the field as *https://<company>-admin.sharepoint.com*. Replace *<company>* with the name of the organization or tenant.
     - Click **Add**.
     - Repeat the procedure to add more sites as per your backup required.
       The added sites to are displayed on the screen. You can use the **Remove** option to remove the selected site from the list.
       If you have many specific sites to be added in the list, you can contact Cohesity Support, we can help you import the list.
3. Perform step 2.
4. Perform step 3.

Configure additional backup options for SharePoint/Teams site/ OneDrive connectors

Configure additional backup options:

- **Process document libraries only**
  You can select this option to exclude lists, blogs, and wikis from the backup.
- **Exclude system lists**
  When this checkbox is selected, Cohesity Alta SaaS Protection skips the backup of lists and libraries that are marked as hidden or catalog.
- **Capture max__versions**
  You can enter the number of versions to retain.
  If the check box is **not** selected, all versions of the items are backed up.
  If the check box is selected, only the set number of versions is backed up.
  Any versions beyond the specified number are marked as **Removed from source**.
- **Capture settings, columns, content types**
  You can select this option to back up the settings, columns, and content types.
  This check box is selected by default.
  If this check box is **not** selected, backups will not include these elements, and the corresponding structures will not be recreated during the restore.
  If the setting was enabled earlier and then disabled after a few backups, the permission information is removed from the backup. Subsequent backups capture the metadata again if there are any changes.
  See "Supported and unsupported SharePoint Objects, Properties, Settings, and Types for backup and restore" on page 144.
- **Capture permissions**
  You can select this option to back up the SharePoint permission objects.
  Subsequent backups recapture these settings if they have changed. Permission changes are only captured during full backups for items and their stub.
  If the setting was enabled earlier and then disabled after a few backups, the permission information is removed from the backup.
  See "Supported SharePoint permission objects for backup and restore" on page 148.

(Optional) Next step:

Configure folder filters to limit the backup scope to specific folders.

See "Configure Folder filter" on page 87.

Backup and restore support for SharePoint Online

You can backup and restore the following for SharePoint Online items:

- Documents

- List items
- Versions
- Site pages
- Site collections
- Sub-site settings
- Site and sub-site columns
- Site and sub-site content types
- List settings
- List columns
- List content types
- Permission objects such as groups
- Role definitions
- Role assignments
- See "Supported Sites and List templates for backup and restore" on page 146.
- See "Supported and unsupported SharePoint Objects, Properties, Settings, and Types for backup and restore" on page 144.
- See "Supported SharePoint permission objects for backup and restore" on page 148.

Supported and unsupported SharePoint Objects, Properties, Settings, and Types for backup and restore

Cohesity Alta SaaS Protection supports the following PrincipalTypes:

The following table lists the supported and unsupported settings and types at different levels in SharePoint.

Table 12-1

Levels in the SharePoint structure	Supported	Unsupported
Site collection level	Sharing	-

Table 12-1 *(continued)*

Levels in the SharePoint structure	Supported	Unsupported

Site and sub-site level	■ User interfaces
	  ■ Title, description, and logo
	  ■ Quick launch
	  ■ Top link bar
	  ■ Navigation elements
	■ Site columns and content types
	■ Site Administration
	  ■ Regional settings
	■ Site features
	■ Site collection administration
	  ■ SharePoint Designer Settings
		Managed metadata and lookup columns

List level	■ List name, description, and navigation ■ Versioning settings ■ Advanced settings ■ Validation settings ■ List columns and content types Calculated, Choice, Currency ($, ¥, €), Date and time, Hyperlink or picture, Image, Location, Multiple lines of text, Number (1, 1.0, 100), Person or Group, Single line of text, Task outcome, and Yes and No check box.	Managed metadata, Lookup columns, and external metadata
SharePoint Files in document libraries	File data and properties associated to the content type for the file.	Properties not associated to content type for the file like item property bag, comment.

Table 12-1 *(continued)*

Levels in the SharePoint structure	Supported	Unsupported
SharePoint Items in lists	Properties associated with the content type for the item, list item attachments.	Properties not associated to the content type for the file like item property bag, comments.

Supported Sites and List templates for backup and restore

The following sites and list templates are validated for backup and restore. Templates not listed here are supported as well. There may be some exceptional cases that are not supported.

Sites

- Community Portal
- Communication Site
- Community Site
- Content Center
- Document Center
- Enterprise Wiki
- Developer Site
- Project Site
- Project Web Acess (PWA)
  The Project Web Access site will be backed up as part of the regular backup process. However, site creation through restore and the restoration of site lists are not supported.
- Publishing Portal
- Records Center
- Team Site
- Team Site (Classic Experience)
- Team Site (No Microsoft 365 Group)

Lists

- Announcements

- Asset Library
- Asset Manager
- Blank/Custom List
- Calendar
- Contacts
- Content Scheduler
- Custom List in Datasheet View
- Discussion Board
- Document Library
- Employee Onboarding
- Event Itinerary
- Expense Tracker
- Explanation Templates
- Files
- Gift Ideas
- Import Spreadsheet
- Issue Tracker
- Issue Tracking
- Links
- Models
- Picture Library
- Playlist
- Promoted Links
- Recipe Tracker
- Report Library
- Survey
- Tasks
- Travel Request
- Wiki Page Library

Sensitivity labels

- Personal
- Public
- General \ Anyone
- General \ All Employees Only
- Confidential \ Anyone

Supported SharePoint permission objects for backup and restore

The following table lists the supported permission objects at different levels in the SharePoint Online structure for backup and restore.

Table 12-2

Levels in SharePoint Online structure	Permission objects
Site and sub-site level	▪ Site groups ▪ Admin users ▪ Associated group ▪ Role definitions ▪ Unique role assignments
List, folder, and file level	Unique role assignments

End-user SharePoint data access in Cohesity Alta SaaS Protection

End users can access Cohesity Alta SaaS Protection data either directly by the End-User portal or indirectly by stubs. End-users can only access data in Cohesity Alta SaaS Protection for which they have permissions at source. Cohesity Alta SaaS Protection captures this information while taking a backup. This section explains how access details at source are replicated in Cohesity Alta SaaS Protection for SharePoint/OneDrive and Teams Sites.

See “Guidelines to configure Stubbing policy for SharePoint Online” on page 102.

General

- By default, Cohesity Alta SaaS Protection captures only access information for site, list, and folder level permissions from the source.
  To capture access information at item level, contact support.

- Cohesity Alta SaaS Protection only captures access details for users who have SharePoint direct-access permissions.
- When permissions change at the source, changes in Cohesity Alta SaaS Protection are only reflected when the connector successfully backs up the source at its scheduled time.
- Cohesity Alta SaaS Protection only allows access to files for end-users or groups with the SharePoint permission levels that include the following list permissions:
  - Open items: Mapped to Cohesity Alta SaaS Protection Read, end user can preview, download, and restore files from the End-User portal or download and restore files from stub.
  - Edit items: Mapped to Cohesity Alta SaaS Protection Write, there are no Cohesity Alta SaaS Protection operations which use this for now.
  - Delete items: Mapped to Cohesity Alta SaaS Protection Delete, there are no Cohesity Alta SaaS Protection operations which use this for now.
- If a user or group has SharePoint permission level with any other permission, then access will not be permitted. For example:
  - For a SharePoint permission level with only the **View Items** or **View Application Pages** permissions, access will not be permitted. Default SharePoint permission levels that use only **View Items** permission include **Restricted View**, **View Only**, and **Download Only**.

    When files are stubbed, users with these permission levels will not be able to access the files from the stub.
  - SharePoint permission levels **Limited Access** also generally does not contain the **Open Items** permissions, so such access to users with such permissions in Cohesity Alta SaaS Protection will not be permitted.

Directory synchronization with Cohesity Alta SaaS Protection

- Directory synchronization should be configured as part of the Cohesity Alta SaaS Protection on-boarding process.
- Cohesity Alta SaaS Protection requires directory synchronization for resolving SharePoint permissions, which are assigned to Entra groups and teams, and permissions, which are given to users with only a UPN and no email address.
- Directory synchronization by Cohesity Alta SaaS Protection happens once a day. There can be intermittent access issues when changes have been made in Entra to a user or a group and a synchronization has not taken place.
- Some changes/configurations in Entra can cause issues when doing directory synchronization in Cohesity Alta SaaS Protection, which can cause the end-user

to not be able to access files either through the End-User portal or stubs. Contact support in such scenarios.

For example, frequent UPN changes - After User Principal Name change, end users are unable to download SharePoint items from End-User Portal. (veritas.com).

  - When a UPN is configured as a proxy email address for another user.

- It is required to synchronize the entire directory with Cohesity Alta SaaS Protection, rather than parts to avoid access issues for end users.
- If Cohesity Alta SaaS Protection backs up two different AD tenants with shared users (for example, a user in Tenant A is also an external user in Tenant B), permission issues can arise when accessing items assigned to shared users.

Permissions to SharePoint Administrators, SharePoint Groups, Entra Groups, and Teams

- Site Administrators have full access to items in Cohesity Alta SaaS Protection.
- For permission at the source with an AD group or Team members, a single permission for that AD Group or Team is created.
- For permission at the source with a SharePoint group or Team owners, one permission per group member/owner is created in Cohesity Alta SaaS Protection.

  Permissions for ‘Everyone’, ‘NT AUTHORITY\authenticated users’, ‘Everyone except external users’ are mapped to a built-in Cohesity Alta SaaS Protection system group called ‘All Internal’.

  - This will grant access to all end-users (including external users in Microsoft Entra) synchronized to Cohesity Alta SaaS Protection by the directory synchronization process to that item.
  - If multiple Microsoft 365 tenants are being backed up then end users in Cohesity Alta SaaS Protection across all tenants will get access to the item.
- Permissions for the ‘Company Administrators’ group are not synchronized to Cohesity Alta SaaS Protection as Cohesity Alta SaaS Protection does not support such a group.

OneDrive

For OneDrive content, Cohesity Alta SaaS Protection synchronizes permissions only for the user who owns the OneDrive. So, from the Cohesity Alta SaaS Protection End-User portal and stubs within OneDrive, only the user to whom the OneDrive belongs can access the content.

Sharing links

- Currently, permissions granted by sharing links are not supported for Teams, SharePoint, and OneDrive.

Run the Delete and Stubbing policies to the SharePoint Online environment

Before running policies, and See "Configure Delete policy for SharePoint Online and guidelines" on page 95.

Important: The connector should not be configured for incremental backup. You can contact Cohesity Support for confirmation.

To run Delete and Stubbing policies to the SharePoint Online environment

1. Access the Administration portal URL.
2. Click **Administration** > **Connectors**.
3. Click within the row of the connector and click **Backup**.
4. On the **Backup now** page, do the following:
   - Select the **All items** option to perform a full backup.
     You can use this option to run the Delete and Stubbing policies at the source location, after the first full backup is completed.
   - Click **Backup**.

   Note: The **New and changes items** options can be used to perform incremental backup.

Note: The time it takes to perform a backup can vary depending on the size of the data being backed up.

Backup limitations for SharePoint Online

The following are the limitations for SharePoint Online connector:

- When the **Require Check Out** option is enabled for a document library, the files in that library are not stubbed by default. To enable stubbing for these files, you need to select the **Stub Items in Lists that Require Checkout** check box in the Connector service.

- SharePoint connector with CDP (continuous data protection) does not work with App registration. Basic or Modern Authentication is required for SharePoint connector with CDP.
- The **Capture site collection, site, list settings, columns and content types** and **Capture permissions** options are not supported for SharePoint on-premises.
- Incremental backups are not supported with manual credentials.
- The site property `AllowExternalEmbeddingWrapper` is not backed up.
- During restore of the items under moderation enabled list Cohesity Alta SaaS Protection will not approved the items because Cohesity Alta SaaS Protection does not back up the moderation status property of the such items.

Chapter 13

Protect Teams sites

This chapter includes the following topics:

- Setting up Teams Site protection with Cohesity Alta SaaS Protection
- Backup limitations for Teams site collections

Setting up Teams Site protection with Cohesity Alta SaaS Protection

To protect your Teams Site environment using Cohesity Alta SaaS Protection using Cohesity Alta SaaS Protection, you need to **add and set up a Cohesity Alta SaaS Protection Teams Site connector** based on your backup requirements. You can backup and restore the Teams, its private channels, and Microsoft 365 groups.

Before you begin:

You must know the following points before adding a connector.

- **Ensure that all prerequisites are completed.**
  See "Pre-requisites to setup protection for M365" on page 122.
- **The following items not supported for backup:**
  - The files that are posted in Teams are stored in the user's OneDrive.
  - The file that is shared in a Teams channel is stored in a private channel or on the SharePoint site for the team.
  - If you back up OneDrive or SharePoint sites using SharePoint connectors and stubbing is enabled, the files are replaced by stubbed URLs in SharePoint sites. The references in these posts still point to the earlier URLs that are no longer available. To access such files, you can open the **Files** tab in the chat or channel.

- **The items/scenarios that are not supported for backup/restore are listed in the following topics:**
  - See "Restore limitations for SharePoint Online" on page 283.
- **Other considerations:**
  - To back up Microsoft 365 Groups and Teams, the Teams Site Collection connector with the **All group and team site collections** option is configured.

Video tutorial to add a Teams site collections connector:

To add a Teams site collections connector, follow the step-by-step procedure outlined on this page or watch the following video tutorial.

http://video.symantec.com/services/player/bcpid292374537001?bckey=AQ~~,AAAABuIiy9k~,I8Bhas-Vwr9zYL9V36WFi86fR_NoePscn&bctid=6362510537112

Step-by-step procedure to add a Teams site collections connector:

Each tab in the connector creation workflow includes a help icon **(?)** on the left. Click this icon to open the corresponding help topic for that tab, which guides you through the setup process step by step.

Procedure:

1. Access the Administration portal.

   The home page of the Administration portal is displayed.
2. Click **Connectors** on the **Backup** card.
3. Click **New backup connector**.
4. Click **Teams Site Collections**.
5. On the **General** tab, set up the basic configuration for the connector and click **Next**.

   See "Configure General settings" on page 83.
6. On the **Configure scope** tab, configure the capture scope to define which SharePoint sites or content should be protected and click **Next**.

   See "Configure capture scope for Team site collections connectors" on page 155.
7. On the **Credentials** tab, configure credentials to access the source workloads (the SharePoint data to be backed up) and click **Next**.

   See "Configure credentials" on page 88.

8 On the **Policy configuration** tab, do the following as per your backup requirements:

- Configure the appropriate backup policy for more granular backup needs.
  See "Configure Custom backup policy and guidelines" on page 93.
- Configure the Delete and Stubbing policies to free up SharePoint storage by removing unwanted items after backup.
  See "Configure Delete policy for SharePoint Online and guidelines" on page 95.
  See "Configure Stubbing policy" on page 100.
  See "Guidelines to configure Stubbing policy for SharePoint Online" on page 102.

9 On the **Scheduling** tab, schedule when the backup job should run.

See "Schedule a backup" on page 115.

10 On the **Email notifications** tab, configure email addresses to receive notifications about backup activities.

See "Configure email addresses to get notifications" on page 116.

11 On the **Review** tab, save the settings and initiate the backup.

See "Review configuration and edit/save/initiate backup" on page 116.

Related topics:

- See "Connector status" on page 119.
- See "Perform on-demand/ad-hoc backup" on page 239.
- See "Video tutorial for connector troubleshooting" on page 241.
- See "Restore SharePoint/OneDrive/Teams Sites and data" on page 272.

Configure capture scope for Team site collections connectors

The capture scope for the connector is configured on the **Capture scope** tab of the connector creation workflow.

Follow these steps to configure the capture scope for a Team site collections connector:

- **Step 1: Determine what to back up and enter the Admin Center URL**.
  Choose whether to back up all sites or specific sites and then provide the Admin center URL.
- **Step 2: Configure additional backup options**.
  Set preferences such as permission and settings backup.

See "Configure additional backup options for SharePoint/Teams site/ OneDrive connectors" on page 142.

- **Step 3: (Optional) Configure folder filters**.
  Define filters to limit the backup scope to specific folders.
  See "Configure Folder filter" on page 87.

To back up all Team site collections and enter the Admin Center URL:

- Click **All group and team site collections**.
- To enter a URL of the Admin center:
  - Click the **Use default** icon next to the **Admin site URL** option.
    The default URL is populated in the field as ***https://<company>-admin.sharepoint.com***.
  - Replace the ***<company>* field** with the name of the organization or tenant.

To back up specific Team site collections only and enter the Admin Center URL:

- Click **Specific site collections**.
- To enter a URL of the Admin center:
  - Click the **Use default** icon next to the **Admin site URL** option.
    The default URL is populated in the field as ***https://<company>-admin.sharepoint.com***.
  - Replace ***<company>*** with the name of the organization or tenant.
  - Click **+ Add specific site collection**, and do the following:
    - On the **+ Add specific site collection** page, click the **Use default** icon next to the **Admin site URL** option.
      The default URL is populated in the field as https://<company>-admin.sharepoint.com. Replace <company> with the name of the organization or tenant.
    - Click **Add**.
    - Repeat the procedure to add more sites as per your backup required.
      The sites that are added are displayed on the screen. You can use the **Remove** option to remove the selected site from the list.

Backup limitations for Teams site collections

Following are the limitations of the Teams site collection connector:

- The files that are posted in Teams are stored in the user's OneDrive.
- The file that is shared in a Teams channel is stored in a private channel or on the SharePoint site for the team.
- If you back up OneDrive or SharePoint sites using SharePoint connectors and stubbing is enabled, the files are replaced by stubbed URLs in SharePoint sites. The references in these posts still point to the earlier URLs that are no longer available. To access such files, you can open the **Files** tab in the chat or channel.

See "Backup limitations for SharePoint Online" on page 151.

Chapter 14

Protect OneDrive data

This chapter includes the following topics:

- Setting up OneDrive protection with Cohesity Alta SaaS Protection

Setting up OneDrive protection with Cohesity Alta SaaS Protection

To protect user's data in your OneDrive environment using Cohesity Alta SaaS Protection using Cohesity Alta SaaS Protection, **you need to add and set up a Cohesity Alta SaaS Protection OneDrive connector** based on your backup requirements..

Before you begin:

You must know the following before adding a connector:

- **Ensure that all prerequisites are completed**.
  See "Pre-requisites to setup protection for M365" on page 122.
- **The following items are supported for backup and restore:**
  - Files and Documents: All files and documents stored in the user's OneDrive account, including documents, spreadsheets, presentations, images, videos, and any other file types.
  - Folders and Folder Structures: Folder hierarchy and structure.
  - Shared Files and Folders: Shared files or folders.
  - Version History: Version history of files.
  - Metadata and File Properties: Metadata associated with files, such as file names, creation dates, modification dates, and other custom properties.

  - Permissions and Sharing Settings: Permissions and sharing settings applied to files and folders, including user access rights, and permissions inheritance.

- **The items/scenarios that are not supported for backup/restore are listed in the following topics:**
  - See "Restore limitations for SharePoint Online" on page 283.

Video tutorial to add a OneDrive connector:

To add a OneDrive connector, follow the procedure outlined on this page or watch the video tutorial below.

http://video.symantec.com/services/player/bcpid292374537001?bckey=AQ~~,AAAABuIiy9k~,I8Bhas-Vwr9zYL9V36WFi86fR_NoePscn&bctid=6362511520112

Step-by-step procedure to add a OneDrive connector:

Each tab in the connector creation workflow includes a help icon **(?)** on the left. Click this icon to open the corresponding help topic for that tab, which guides you through the setup process step by step.

Procedure:

1. Access the Administration portal.

   The home page of the Administration portal is displayed.

2. Click **Connectors** on the **Backup** card.
3. Click **New backup connector**.
4. Click **OneDrive**.
5. On the **General** tab, set up the basic configuration for the connector and click **Next**.

   See "Configure General settings" on page 83.

6. On the **Configure scope** tab, configure the capture scope to define which SharePoint sites or content should be protected and click **Next**.
7. On the **Credentials** tab, configure credentials to access the source workloads (the SharePoint data to be backed up) and click **Next**.

   See "Configure credentials" on page 88.

8. On the **Policy configuration** tab, do the following as per your backup requirements:
   - Configure the appropriate backup policy for more granular backup needs. See "Configure Custom backup policy and guidelines" on page 93.

- Configure the Delete and Stubbing policies to free up SharePoint storage by removing unwanted items after backup.
  See "Configure Delete policy for SharePoint Online and guidelines" on page 95.
  See "Configure Stubbing policy" on page 100.
  See "Guidelines to configure Stubbing policy for SharePoint Online" on page 102.

9 On the **Scheduling** tab, schedule when the backup job should run.

  See "Schedule a backup" on page 115.

10 On the **Email notifications** tab, configure email addresses to receive notifications about backup activities.

  See "Configure email addresses to get notifications" on page 116.

11 On the **Review** tab, save the settings and initiate the backup.

  See "Review configuration and edit/save/initiate backup" on page 116.

Related topics:

- See "Connector status" on page 119.
- See "Perform on-demand/ad-hoc backup" on page 239.
- See "Video tutorial for connector troubleshooting" on page 241.
- See "Restore SharePoint/OneDrive/Teams Sites and data" on page 272.
- See "Restore limitations for SharePoint Online" on page 283.

Configure capture scope for OneDrive connectors

The capture scope for the connector is configured on the **Capture scope** tab of the connector creation workflow.

Follow these steps to configure the capture scope for a Team site collections connector:

- **Step 1: Determine what to back up and enter the Admin Center URL**.
  Choose whether to back up all sites or specific sites and then provide the Admin center URL.
- **Step 2: Configure additional backup options**.
  Set preferences such as permission and settings backup.
  See "Configure additional backup options for SharePoint/Teams site/ OneDrive connectors" on page 142.
- **Step 3: (Optional) Configure folder filters**.

Define filters to limit the backup scope to specific folders.
See "Configure Folder filter" on page 87.
See "Configure Group filter" on page 86.

To back up the data from all OneDrive sites

- Click **OneDrive Site collections**.
- To enter **Admin Site URL** and **My Site / OneDrive collection base URL**:
  - Click the **Use default** icon next to the respective fields.
    The default URL is populated.
  - Replace the ***<company>*** field with the name of the organization or tenant.
- To restrict the backup scope to specific domains, select the **Restrict to users with specific mail domain** check box, and enter the domain names.
  Only the data of users from the added domains is included in the backup.

To back up the data from specific OneDrive sites only

- Click **Specific Site collections**.
- Click **+ Add specific site collection**.
- On the **+ Add specific site collection** page, click the **Use default** icon next. The default URL is populated. Replace ***<company>*** with the name of the organization or tenant. Click **Add**.
- Repeat the procedure to add more sites as per your backup required.
  The sites are displayed on the screen. You can use the **Remove** option to remove the selected site from the list.

Chapter 15

Protect Teams chats

This chapter includes the following topics:

- Setting up Teams chat protection with Cohesity Alta SaaS Protection
- Backup limitations for Teams chat

Setting up Teams chat protection with Cohesity Alta SaaS Protection

To protect users data in your Teams chat environment using Cohesity Alta SaaS Protection using Cohesity Alta SaaS Protection, you need to add and set up a Cohesity Alta SaaS Protection Teams chat connector based on your backup requirements. However, you must consider the following points before adding a connector.

- **Ensure that all prerequisites are complete.**
- You can set up an individual connector for each backup requirement, like one-on-one chats, group chats, and channel conversations. Alternatively, you can configure a single connector that covers all your backup requirements.
- **The following items are supported for backup and restore:**
  - Chat conversations: All and specific users' chat conversations that occur within the Teams chat environment, including one-on-one chats and group chats.
  - Media files: Media files that are shared within Teams chat, such as images, videos, and audio files.
  - Emojis, GIFs, and Stickers: Links, emojis, GIFs, stickers, or other visual element.
  - Chat history: Chat history for each user.

- **The following items are not supported for backup:**
  - Teams calendar
  - The images embedded in chat messages.
  - Praise and reactions (such as thumbs up, and so on).
  - The important tag for important messages is missing when backed up or restored.
  - Loop component.
- **The following items are not supported for the restore**:
  - Restore of reactions on the chats is not supported.
  - Restore of users' one-on-one chat is not supported.
    Downloading the one-on-one chats using the Administration portal or Export Utility lets you access the one-on-one chats. The chats are downloaded in HTML format.
  - The **Type** column in the **Export Jobs** tab of the Export Service is displayed as **Unknown** for the Teams chat when restore is done using the Export service.
  - Replies to the deleted, edited, or reacted messages do not show which message the reply is associated with.
    Example: A reply to an edited message does not specify which message it was in response to.
  - Scheduled meetings are not restored correctly.
- **Connector features:**
  - All user chat backup
    An option to back up one-on-one and group chat data for all users.
  - Selective user's chat backup
    An option to back up one-on-one and group chat data for specific users.
  - Backup of all chats in Teams channels
    An option to back up all chats in Teams channels.
  - Limit backup scope based on time range

An option to limit the backup to a specific number of days.

Step-by-step procedure to add a Teams chat connector:

1. Access the Administration portal.

   The home page of the Administration portal is displayed.

2. Click **Connectors** on the **Backup** card.

3. Click **New backup connector**.

4. Click **Teams chat**.

   To make the setup process easier and more intuitive, each tab in the connector creation workflow includes a help icon **(?)** at the left. You can click this icon to open the respective help topic for that tab, which can guide you through the setup step by step.

5. On the **General** tab, set up the basic configuration for the connector and click **Next**.

   See "Configure General settings" on page 83.

6. On the **Capture scope** tab, configure the capture scope and click **Next**.

   See "Configure capture scope for Teams chat connectors" on page 165.

7. On the **Credentials** tab, do any of the following to configure credentials:

   To use Microsoft Graph Modern/OAuth, do the following:

   - Click **Manual**.
   - Enter the Tenant ID, Client ID, and Client Secret.
     These details are generated while adding an application to your Cohesity Alta SaaS Protection tenant.
     These details are generated when you create an application registration in your M365 tenant.
     For more information on registering an app for the Teams chat connector using Export API, follow the link:
     Registering Azure Active Directory (AAD) Application for Teams Chat Connectors using Export API

   To use the 365 App registration mode, do the following:

   When using the **365 App registration mode**, refer to the following topics:

   - If no or less number of apps are displayed on the page when you use the **M365 App Registration mode**.
     See "Assign Microsoft 365 apps registration" on page 89.
   - If the status of the assigned app is displayed as **Inactive**.
     See "Approve Microsoft 365 apps using the App Consent Grant utility" on page 92.

8 On the **Scheduling** tab, schedule when the backup job should run.

See "Schedule a backup" on page 115.

9 On the **Email notifications** tab, configure email addresses to receive notifications about backup activities.

See "Configure email addresses to get notifications" on page 116.

10 On the **Review** tab, save the settings and initiate the backup.

See "Review configuration and edit/save/initiate backup" on page 116.

Related topics:

- See "Connector status" on page 119.
- See "Perform on-demand/ad-hoc backup" on page 239.
- See "Video tutorial for connector troubleshooting" on page 241.
- See "Restore Teams chat messages and Teams channel conversations" on page 288.
- See "Backup limitations for Teams chat" on page 166.
- See "Restore limitations for Teams chat" on page 290.

Configure capture scope for Teams chat connectors

You can use the procedure to configure the capture scope to back up for Teams chat data.

To configure the capture scope to back up for Teams chat data

1 To select which data to back up from the Teams chat environment, do one of the following:

- **Option 1**: To back up one-on-one and group chat of all users, do the following:
  - From the **Team capture mode** section, click **None**.
  - From the **User Chat capture mode** section, click **All Users**.
- **Option 2**: To back up one-on-one and group chat of specific users, do the following:
  Starting with release 3.10.1 release, this option will be available for new or existing connectors.
  - From the **Team capture mode** section, click **None**.
  - From the **User Chats capture mode** section, click **Specific Users**.

        - Click **+ Add Specific mailboxes**.
        - On the **Add specific mailbox** page, enter the SMTP addresses of the users whose chat messages need to be backed up using this connector.
        - Click **Add**.
    - **Option 3**: To back up all Teams, do the following:
        - From the **Team capture mode** section, click **All Teams**.
        - From the **User Chats capture mode** section, click **None**.
    - **Option 4**: To back up specific Teams, do the following:
        - From the **User Chats capture mode** section, click **None**.
        - From the **Team capture mode** section, click **Specific Teams**.
            - On the **Add specific team** page, enter the SMTP addresses of the teams whose channel conversations need to be backed up using this connector.
            - Click **Add**.

2. From the **Reference time zone** dropdown list, select the required reference zone in which you want to see the conversation timestamp.

   Once a Teams chat connector is created, the reference time zone of the connector cannot be changed.

3. Configure filters to restrict the backup scope to specific users and folders. Do the following:
    - To restrict the backup scope to specific users based on their attributes or group membership in Microsoft Entra ID.
      See "Configure Group filter" on page 86.
    - To restrict the backup scope to specific folders only.
      See "Configure Folder filter" on page 87.
4. Click **Next** to configure credentials.

Backup limitations for Teams chat

The following items in the Teams chat environment are not supported for backup:

- Teams calendar
- The images embedded in chat messages.

- Praise and reactions (such as thumbs up, and so on) are not backed up.
- The important tag for important messages is missing when backed up or restored.
- Loop components are not backed up.

For the restore limitations, refer to the following topic:

See "Restore limitations for Teams chat" on page 290.

Chapter 16

Protect Google Drive data

This chapter includes the following topics:

- Prerequisites to setup Google Drive protection with Cohesity Alta SaaS Protection
- Setting up Google Drive protection with Cohesity Alta SaaS Protection
- Backup limitations for Google Drive
- FAQs

Prerequisites to setup Google Drive protection with Cohesity Alta SaaS Protection

This topic covers the process of configuring the Google Workspace prerequisites to create the connector that will capture the data.

A few notes to consider:

- The process will require elevated access to the Google Workspace console.
- The connector only supports capturing data from users in Google Workspace; it does not support regular Gmail.

Authentication and Authorization

- A service account is required to access resources, including Google Drives of delegated access to users.

Create a Project

A project is a collection of settings, credentials, and metadata about the application or applications you're working that make use of Google APIs and Google Cloud Platform resources.

Create a project

1. Create a Project by logging into the console via the following URL.

   https://console.cloud.google.com/apis/credentials

2. Create a Credential of type service account.
3. To enable the APIs.
   - Click the **Enable APIS AND SERVICES**.
   - From the list, enable the required APIs listed below: Google Drive, Service Directory API, Admin SDK API
4. Create the service account, making it an owner of the project.
5. Create the service account key and download the JSON

   This JSON file will be used when configuring the connector.
6. To enable domain-wide delegation for the service account, do the following:
   - Browse to: https://admin.google.com/ac/owl/domainwidedelegation
   - Select **Security**, then API controls, then Domain-wide delegation.
   - Click **Add new**.
   - Enter the Client ID, which is the service account Unique ID.
   - Enter the URL's below for the scopes:
     - https://www.googleapis.com/auth/drive
     - https://www.googleapis.com/auth/admin.directory.user.readonly
     - https://www.googleapis.com/auth/admin.directory.group.member.readonly
   - Click **Authorize**.

This completes the process. Now you can create and configure the Connector.

Setting up Google Drive protection with Cohesity Alta SaaS Protection

To protect users' data on the Google Drive environment using Cohesity Alta SaaS Protection, you need to add and set up a Cohesity Alta SaaS Protection Google Drive connector based on your backup requirements.

Before you begin:

You must know the following before adding a connector:

- **Ensure that all prerequisites are completed.**
  See "Prerequisites to setup Google Drive protection with Cohesity Alta SaaS Protection" on page 168.
- **The following items are supported for backup and restore**:
  - Files and documents: All files and documents that are stored in Google Drive, including documents, spreadsheets, presentations, images, videos, and any other file types.
  - User drives and Shared drives: Drives dedicated to each user and common shared Drives.
  - Version history: Version history of files.
  - Deleted files: Deleted files.
  - Metadata and file properties: Metadata and properties, such as owner information, last modified date, and custom metadata fields associated with Google Drive.
- **The following items are not supported for backup and restore**.
  - You cannot backup of the following data in the Google Drive environment:
    - `Google Jamboard`
    - `Google Sites`
    - `Google Maps`
    - `Google Forms`
    - Local computer files under **Computers** node of Google Drive.
    - **Shared with me** folders or files.
    - Drive/Folder color preference.
    - Star status of folder or file.
    - Sharing permissions (whom a folder or file is shared with)
  - You can backup and restore the following Google Workspace applications, but not in the native format. The supported formats for backup and their format conversion after restore are as follows:

Item type	Cohesity Alta SaaS Protection backup and restore format
Google Docs	DOCX
Google Sheets	XISX

Item type	Cohesity Alta SaaS Protection backup and restore format
Google Presentation	PPTX
Google Drawing	PNG
Google Apps Script	JSON

- **Other considerations:**
  - You cannot restore the Google Drive data using the Cohesity Alta SaaS Protection End-User portal.

Step-by-step procedure to add a Google Drive connector:

Each tab in the connector creation workflow includes a help icon (?) on the left. Click this icon to open the corresponding help topic for that tab, which guides you through the setup process step by step.

Important: If group email addresses are added to the scope for specific users, the connector will retrieve the users in the group and back up their data. Similarly, group email addresses added to the Excluded Users scope will also be processed in the same manner.

Procedure:

1. **Access the Administration portal and select the connector type**.
   - Access the Administration portal.
   - Click **Connectors** on the **Backup** card.
   - Click **New backup connector**.
   - Click **GoogleDrive**.
2. On the **General** tab, set up the basic configuration for the connector.

   See “Configure General settings” on page 83.
3. On the **Capture scope** tab, configure the capture scope.

   See “Configure Capture scope Google Drive connectors ” on page 172.

4 On the **Credentials** tab, configure the credentials as follows:

Admin User SMTP	Enter the SMTP address of a user who has Admin API permissions.
Credentials JSON	Paste the content from a JSON file, which is generated as part of the prerequisites. For more information on the prerequisites to add Google Drive connectors, refer to the following link: https://www.veritas.com/content/support/en_US/article.100050288

5 On the **Policy configuration** tab, configure backup policy for granular backup requirements.

See "Configure Custom backup policy and guidelines" on page 93.

6 On the **Scheduling** tab, schedule when the backup job should run.

See "Schedule a backup" on page 115.

7 On the **Email notifications** tab, configure email addresses to receive notifications about backup activities.

See "Configure email addresses to get notifications" on page 116.

8 On the **Review** tab, save the settings and initiate the backup.

See "Review configuration and edit/save/initiate backup" on page 116.

Related topics:

- See "Connector status" on page 119.
- See "Perform on-demand/ad-hoc backup" on page 239.
- See "Video tutorial for connector troubleshooting" on page 241.
- See "Restore Google Drive data" on page 292.
- See "Backup limitations for Google Drive" on page 175.

Configure Capture scope Google Drive connectors

You can use one of the following procedures as per your backup requirement to backup users data in your Google Drive environment:

Configure the Google Drive connector to backup all users' data

1 Click **All users**.

2 ConfigureTable 16-1, and then click **Next**.

For more information,

Configure the Google Drive connector to backup all users' data but only exclude a few users' data from the backup scope

1 Click **All users**.

2 Click **Add users**.

3 On the **Add users address** page, enter the email addresses of the users who are to be excluded from the backup scope.

Use semicolon between email addresses.

4 Configure other settings, and then click **Next**.

For more information, See Table 16-1 on page 175.

Configure the Google Drive connector to backup specific users' data

1 Click **Specific users**.

2 On the **Add users address** page, enter the email addresses of the users who are to be added in the backup scope and click **Add**.

You can also add email addresses of the groups that are to be included in the backup.

Use semicolon between email addresses.

3 Configure other settings, and then click **Next**.

For more information, See Table 16-1 on page 175.

Configure the Google Drive connector to backup specific groups' data

1 Click **Specific users**.

2 Click **Add users**.

3 On the **Add users address** page, enter the group email addresses of the Google groups to be included in the backup scope, and then click **Add**.

   Use semicolon between email addresses.

4 Configure other settings, and then click **Next**.

   For more information, See Table 16-1 on page 175.

Configure the Google Drive connector to backup the Shared drives

1 Click **Shared drives**.

2 Configure other settings, and then click **Next**.

   For more information, See Table 16-1 on page 175.

Configure the capture scope to back up the Google Drive using the Alphabetical mailbox scope option

If you have a large number of drives in your environment, the backup scope can become extensive. To manage this scenario, configure the capture scope using the **Alphabetical user scope** option. You can map a range of drives to be included in the backup. It helps minimize the load on any one connector. To cover all the drives in your environment, you can configure multiple connectors.

1 Click **All users**.

2 Click the **Alphabetical user scope** option and do the following:

   - Enter the range of email addresses that you want to back up using this connector.
     For example, if you specify the start letter as 'A' and the end letter as 'F', all email addresses within the range of 'A' to 'F' are included in the backup scope.
     The mailboxes are processed based on the first letter of the email address.
     If you are using the **Alphabetic user scope**, you may need to enable the**Include users whose email addresses starts with non-alphabetical character** option for one of the connectors. It backs up the mailboxes of the users whose email addresses do not begin with an alphabet.

3 Configure other settings on the page, and click **Next**.

   For more information, See the section called “Other settings:” on page 175.

Other settings:

Table 16-1 Other settings

Settings	Description
Backup deleted items	Select this check box to include deleted items in the backup. By default, items are permanently deleted from the recycle bin after 30 days in Google Drive.
Capture permissions	Select this check box to capture the permissions on the items.
Folder filter	Configure it to limit the backup scope to specific folders only. See "Configure Folder filter" on page 87.

Next step:

Configure credentials.

Backup limitations for Google Drive

The following are the limitations of the Google Drive connector:

- You cannot backup of the following data in the Google Drive environment:
  - `Google Jamboard`
  - `Google Sites`
  - `Google Maps`
  - `Google Forms`
- You cannot backup and restore for the following:
  - Local computer files under **Computers** node of Google Drive.
  - **Shared with me** folders or files.
  - Drive/Folder color preference.
  - Star status of folder or file.
  - Sharing permissions (whom a folder or file is shared with)
- You cannot restore the Google Drive data using the End-User portal.

FAQs

- Can I add both users and groups under Specific users?

  Yes. You can add individual email addresses and group addresses. The connector resolves the groups to the users they contain.

- Can I change the capture scope later?

  Yes, edit the connector configuration to update the capture scope. Previous backups remain unaffected.

- Are deleted items backed up?

  Yes, if the Backup deleted items checkbox is selected. Otherwise, permanently deleted items (after 30 days) are not retained.

Chapter 17

Protect Gmail data

This chapter includes the following topics:

- Prerequisites to setup Gmail protection with Cohesity Alta SaaS Protection
- Setting up Gmail protection with Cohesity Alta SaaS Protection

Prerequisites to setup Gmail protection with Cohesity Alta SaaS Protection

This topic covers the process of configuring the Google Workspace prerequisites to create the connector that will capture the data.

A few notes to consider:

- The process will require elevated access to the Google Workspace console.
- The connector only supports capturing data from users in Google Workspace; it does not support regular Gmail.

Authentication and Authorization

- A service account is required to access resources, including Google Drives of delegated access to users.

Create a Project

A project is a collection of settings, credentials, and metadata about the application or applications you're working that make use of Google APIs and Google Cloud Platform resources.

Create a project

1. Create a Ppoject by logging into the console via the following URL.

   https://console.cloud.google.com/apis/credentials

2. Create a Credential of type service account.
3. To enable the APIs.
   - Click the **Enable APIS AND SERVICES**.
   - From the list, enable the required APIs listed below: Google Drive, Service Directory API, Admin SDK API
4. Create the service account, making it an owner of the project.
5. Create the service account key and download the JSON

   This JSON file will be used when configuring the connector.
6. To enable domain-wide delegation for the service account, do the following:
   - Browse to: https://admin.google.com/ac/owl/domainwidedelegation
   - Select **Security**, then API controls, then Domain-wide delegation.
   - Click **Add new**.
   - Enter the Client ID, which is the service account Unique ID.
   - Enter the URL's below for the scopes:
     - https://www.googleapis.com/auth/admin.directory.user.readonly
     - https://www.googleapis.com/auth/gmail.modify
     - https://www.googleapis.com/auth/gmail.readonly
     - https://www.googleapis.com/auth/admin.directory.group.member.readonly
   - Click **Authorize**.

This completes the process. Now you can create and configure the Connector.

Setting up Gmail protection with Cohesity Alta SaaS Protection

To protect user's data in your Gmail environment using Cohesity Alta SaaS Protection, you need to add and set up a Cohesity Alta SaaS Protection Gmail connector based on your backup requirements.

Before you begin:

You must know the following before adding a connector:

- **Ensure that all prerequisites are completed**..
  See "Prerequisites to setup Gmail protection with Cohesity Alta SaaS Protection" on page 177.
- **The following items are supported for backup and restore**:
  - Emails: All emails in the Gmail account, including inbox messages, sent items, drafts, and archived emails.
  - Attachments: Attachments associated with emails.
  - Labels and Folders: Labels and folders.
  - Deleted Emails: Deleted emails.
- **Connector features**:
  - Backup all or specific user's data
    An option to back up all or specific users' data.
  - Exclude specific users
    An option to exclude certain users from the backup by adding their email addresses to the excluded users list.
  - Backup of Deleted and Spam folder
    An option to include or exclude deleted items and the items in the Spam folder.

Step-by-step procedure to add a Gmail connector:

Each tab in the connector creation workflow includes a help icon (?) on the left. Click this icon to open the corresponding help topic for that tab, which guides you through the setup process step by step.

Important: If group email addresses are added to the scope for specific users, the connector will retrieve the users in the group and back up their data. Similarly, group email addresses added to the Excluded Users scope will also be processed in the same manner.

Procedure:

1. **Access the Administration portal and select the connector type**.
   - Access the Administration portal.
   - Click **Connectors** on the **Backup** card.
   - Click **New backup connector**.

- Click **Gmail**.

2. On the **General** tab, set up the basic configuration for the connector.

   See "Configure General settings" on page 83.

3. On the **Capture scope** tab, configure backup scope.

   See "Configure capture scope for Gmail connectors" on page 180.

4. On the **Credentials** tab, do the following:

Admin User SMTP	Enter the SMTP address of an administrator user that is used for obtaining lists of drives, and so on.
Credentials JSON	Copy the content from a JSON file, which is generated as part of the prerequisites.

5. Click **Next**.
6. On the **Policy configuration** tab, configure backup policy.

   See "Configure Custom backup policy and guidelines" on page 93.

7. On the **Scheduling** tab, schedule when the backup job should run.

   See "Schedule a backup" on page 115.

8. On the **Email notifications** tab, configure email addresses to receive notifications about backup activities.

   See "Configure email addresses to get notifications" on page 116.

9. On the **Review** tab, save the settings and initiate the backup.

   See "Review configuration and edit/save/initiate backup" on page 116.

Related topics:

- See "Connector status" on page 119.
- See "Perform on-demand/ad-hoc backup" on page 239.
- See "Video tutorial for connector troubleshooting" on page 241.
- See "Restore Gmail data" on page 294.

Configure capture scope for Gmail connectors

You can use one of the following procedures as per your backup requirement:

Configure the capture scope for Gmail connectors to backup data of all users

1 Click **All users**.

2 Configure other settings on the page, and click **Next**.

For more information, See Table 17-1 on page 182.

Configure the capture scope for Gmail connectors to backup all users but exclude backup for a few users

1 Click **All users**.

2 Click **+ Add users**.

3 On the **Add users address** page, enter users' email addresses to be excluded from the backup scope.

Use semicolon between email addresses.

Click **Add**.

4 Configure other settings on the page, and click **Next**.

For more information, See Table 17-1 on page 182.

Configure the capture scope for Gmail connectors to back up the data of specific users only

1 Click **Specific users**.

2 Click **+ Add users**.

3 On the **Add users address** page, enter users' email addresses for whom you want to take backup and click **Add**.

Use semicolon between email addresses.

4 Configure other settings on the page, and click **Next**.

For more information, See Table 17-1 on page 182.

Configure the capture scope for Gmail connectors to backup specific groups only

1 Click **Specific users**.

2 Click **Add users**.

3 On the **Add users address** page, enter the group email addresses of the Google groups to be included in the backup scope, and then click **Add**.

   Use semicolon between email addresses.

4 Configure other settings on the page, and click **Next**.

   For more information, See Table 17-1 on page 182.

Configure the capture scope to back up the mailboxes of users using the Alphabetical mailbox scope option

If you have a large number of mailboxes in your environment, the backup scope can become extensive. To manage this scenario, configure the capture scope using the **Alphabetical user scope** option. You can map a range of mailboxes to be included in the backup. It helps minimize the load on any one connector. To cover all the mailboxes in your environment, you can configure multiple connectors.

1 Click **All users**.

2 Click the **Alphabetical user scope** option and do the following:

   - Enter the range of email addresses that you want to back up using this connector.
     For example, if you specify the start letter as 'A' and the end letter as 'F', all email addresses within the range of 'A' to 'F' are included in the backup scope.
     The mailboxes are processed based on the first letter of the email address.
     If you are using the **Alphabetic user scope**, you may need to enable the**Include users whose email addresses starts with non-alphabetical character** option for one of the connectors. It backs up the mailboxes of the users whose email addresses do not begin with an alphabet.

3 Configure other settings on the page, and click **Next**.

   For more information, See Table 17-1 on page 182.

Other settings:

Table 17-1 Other settings

Settings	Description
Capture Trash	Select this check box to back up the deleted items in the Trash folder.
Capture Spam	Select this check box to back up the items in the Spam folder.

Table 17-1 Other settings *(continued)*

Settings	Description
Folder filters	Configure folder filters to limit the backup scope to a few folders. See "Configure Folder filter" on page 87.

Next step:

Configure credentials.

Chapter 18

Protect Audit logs

This chapter includes the following topics:

- Add Audit log connectors
- Audit log connector limitations

Add Audit log connectors

With the Cohesity Alta SaaS Protection 2.36.1 release, the Audit Log Connector is supported for existing customers only. New customers will not have access to this feature.

Use the following procedure to add an Audit log connector.

To add an Audit log connector

1. Access the Administration portal.

   The home page of the Administration portal is displayed.

2. Click **Connectors** on the **Backup** card.

3. Click **New backup connector**.

4. Click **Audit Log**.

   To make the setup process easier and more intuitive, each tab in the connector creation workflow includes a help icon **(?)** at the left. You can click this icon to open the respective help topic for that tab, which can guide you through the setup step by step.

5. On the **General** tab, set up the basic configuration for the connector.

   See “Configure General settings” on page 83.

6. On the **Capture scope** tab, do the following:

- In the **Process last __days** field, enter the number of days for which you want to backup the data.

  By default, it is 14 days.

  By default, the connector backs up data from the previous 14 days. It is recommended that you configure this option to 180 days for the first backup to ensure that all data for the last 180 days is backed up.

  Once the initial backup is completed, Cohesity recommends changing this value to 7 days for efficient data processing during the subsequent backups.

- If required, configure folder filters to include or exclude any specific folders from being backed up.

  See "Configure Folder filter" on page 87.

- Click **Next**.

7 On the **Credentials** tab, configure credentials to access the source workloads (the SharePoint data to be backed up) and click **Next**.

  See "Configure credentials" on page 88.

8 Click **Next**.

9 On the **Scheduling** tab, schedule when the backup job should run.

  See "Schedule a backup" on page 115.

10 On the **Email notifications** tab, configure email addresses to receive notifications about backup activities.

  See "Configure email addresses to get notifications" on page 116.

11 On the **Review** tab, save the settings and initiate the backup.

  See "Review configuration and edit/save/initiate backup" on page 116.

Audit log connector limitations

The limitations of the Audit log connector are:

- Cohesity Alta SaaS Protection uses the `Search-UnifiedAuditLog PowerShell` command to retrieve audit logs. The duration of this process may vary, ranging from a few minutes to several hours, depending on factors such as the volume of logs within the specified time interval. This may result in delays in the backup process.

- The `Search-UnifiedAuditLog` command enforces a minimum query window of one second and imposes a maximum limit of 5,000 records per query. If the number of audit log records exceeds 5,000 within a single second, Cohesity

Alta SaaS Protection will be unable to back up the audit log data for that specific second.

- The user interface does not display progress information until audit logs for the specified hour have been fully collected and processed.
- The `Search-UnifiedAuditLog` command has internal time-out limitations. To address this, Cohesity Alta SaaS Protection performs up to three retry attempts. If all retries return zero results, it is assumed that no data is available for the specified time range. It is important to note that this retry mechanism may contribute to increased backup duration.
- Restoration of audit log records directly to a Microsoft server is not supported. Therefore, Cohesity Alta SaaS Protection allows restoration of audit log backup data only to a File server.
- If, for any reason, the connector fails to process certain timeslots, those timeslots cannot be revisited for data collection. Several factors may contribute to timeslots being missed, including:
  - Failures in retrieving audit entries from Microsoft or errors encountered while uploading data to Cohesity Alta SaaS Protection.
  - The connector being unable to keep pace with the volume of data generated by the customer's Microsoft tenant.
  - The connector being inactive or in an erroneous condition, and hence not running as expected.

Chapter 19

Protect Salesforce data and metadata

This chapter includes the following topics:

- About Salesforce protection
- Key considerations and prerequisites for adding Salesforce connectors
- Add Salesforce connectors
- Limitations of Salesforce connectors
- Salesforce Objects not supported for backup

About Salesforce protection

Cohesity Alta SaaS Protection supports protecting the following data in the Salesforce organization using the Cohesity Alta SaaS Protection Salesforce connector. It supports the backup and restore of the following:

- Data
- File/attachments/Salesforce CRM
- Metadata

Salesforce data includes objects, records, files, attachments, documents, and Salesforce CRM Content. Salesforce metadata includes layouts, profiles, object schemas, permission sets, Apex classes, workflows, reports, dashboards, and more.

By default, the connector backs up all objects except Feed, History, and Share objects. The connector supports the backup and restore of shared libraries. Cohesity

Alta SaaS Protection supports the backup and restore of encrypted data in Salesforce using SecureShield or any other third-party encryption product.

What is supported?

The Salesforce connector supports various Salesforce clouds, editions, organizations, and environment types, ensuring seamless integration and functionality across multiple use cases. It also supports SecureShield and commonly used AppExchange Apps. Cohesity Alta SaaS Protection also supports backup and restore for Salesforce's Summer 2024 release.

- Salesforce clouds:
  - Sales
  - Service
  - Field Services
  - Salesforce Industries - Manufacturing (formerly known as Vlocity)
- Salesforce editions:
  - Enterprise
  - Unlimited
  - Performance
- Salesforce organizations:
  - Enterprise
  - Partner Enterprise (Structured data and Metadata only)
- Salesforce environment types:
  - Production
  - Sandbox
- Support for commonly used AppExchange Apps

Feature of the Salesforce connector

The Salesforce connector includes features such as incremental backups for most standard and all custom objects, and sandbox seeding for testing and development scenarios. With support for granular data backup and restore, point-in-time restores, and content browsing, the Salesforce connector ensures efficient and precise data recovery.

Additionally, it supports SecureShield, commonly used AppExchange apps, parallelism for faster backups, and provides robust data validation options and permission management.

- **Incremental backup**
  After the first full backup, all subsequent backups are incremental for the majority of the standard and all the custom objects.

  Note: Metadata backup is always a full backup.

- **Restore to different organizations (Sandbox seeding)**
  The creation of sandbox environments by seeding them with backed-up data allows for realistic testing and development scenarios. Cohesity Alta SaaS Protection supports restore of common use cases, such as:
  - Production to sandbox
  - Sandbox to sandbox
- **Parallelism support**
  Parallelism during backup operations to minimize the time required to complete the job.
- **SecureShield and other apps support**
  There is full support for additional features such as SecureShield and commonly used AppExchange apps within the Salesforce environment.
- **Recovery point-based backups**
  There is support for point-in-time restore letting you restore records and objects for the selected recovery points along with nested child and parent object records. This ensures integrity between records after the restore.
- **Storage summary**
  The **Analytics** page enables you to view recovery points and the space occupied by the recovery points within the Stors of Cohesity Alta SaaS Protection.
- **Granular data restore**
  There is supports for selectively restoring specific elements of Salesforce, such as individual records or objects. You can also use advanced filters to select the required data.
- **Metadata validation options before restore**
  The following metadata validations are supported before deployment:
  - Validate and Restore (Deploy): Validate the selected metadata-compressed components for dependencies and perform the restore.
  - Validate Only: Validate only the selected metadata-compressed components for dependencies.
- **Content browsing and restore**

The support for content browsing and restore includes:

- Point-in-time views for accessing historical data.
- Ability to view backed-up objects, each having its own schema.
- Ability to view and download metadata.
- **Complex Query filters for restore**
  - Ability to view and restore specific objects or records.
  - Ability to select records for the restore using filter criteria. You can preview child object data records before running the actual restore.
  - Wizard-based data and metadata restores.

Key considerations and prerequisites for adding Salesforce connectors

::Key considerations for adding Salesforce connectors

Consider the following points before adding Salesforce connectors to ensure a seamless setup:

- **Implement all the prerequisites**
- **Ensure you have the following information ready:**
  - **User name**: The name of the Backup Admin user you have created within the targeted Salesforce organization.
  - **Instance URL**: The instance URL of the targeted Salesforce organization.
  - **Consumer Key**: The Consumer Key is generated when you add a Connected App to the targeted Salesforce organization.
    See "Configure User, Profile, and Connected App for Salesforce" on page 196.
- **Consider the default connector configuration**
  By default, Salesforce connectors back up all objects except for **Feed**, **History**, and **Share**, as these objects are not typically critical for business continuity. However, you can enable backups for these objects based on your specific needs, considering the following:
  - **History** objects:
    These objects cannot be restored. Select them for backup only if retaining historical information on record or field-level changes is necessary for auditing purposes.
  - **Share** objects:

Only manual Share objects can be restored. Other types of Share objects cannot be restored due to Salesforce API limitations.

Note: During the Salesforce restore, Share tables are automatically created unless they contain manual Share rules.

- **Feed** objects:
  Feed objects are views into the **FeedItem** object. Cohesity Alta SaaS Protection backs up only the **FeedItem** object to avoid duplication. Due to Salesforce API limitations, only specific types of FeedItem records can be restored.

Skipping these objects accelerates the backup process and reduces the storage required for Cohesity Alta SaaS Protection recovery points.

::Prerequisites for adding Salesforce connectors

Following are the prerequisites to add Salesforce connectors:

Table 19-1

Prerequisite	Description
Connector per organization	You need to create a separate connector for each Salesforce organization you want to back up.

Table 19-1 *(continued)*

Prerequisite	Description
Structured Stor, SalesforceFiles Stor, Connector service, and Export service	Cohesity handles this prerequisite for your tenant as part of the provisioning process. Cohesity provides structured Stors, SalesforceFiles Stor, and one or more VMs (with preinstalled Connector and Export services) within your Cohesity Alta SaaS Protection tenant. Depending on the Salesforce organization, one or more Connector VMs and SalesforceFiles Stors may be provisioned. Cohesity provisions one structured Stor per targeted Salesforce organization; the SalesforceFiles Stor is shared across Salesforce connectors. If a connector using a structured Stor is deleted, you can create a new connector using the same structured Stor. Ensure that the URL and type (Production or Sandbox) of the Salesforce organization match those of the original structured Stor. . **Note:** The Connector and Export service are hosted on a single VM, which can support multiple connectors depending on the size of the Salesforce organization and its data. The Connector/Export service VM may host multiple connectors based on the size of the Salesforce organization we need to protect. For larger Salesforce organizations (with more data), the connector may be hosted independently on a separate Connector/Export service VM. **Note:** When these Stors are configured together for a connector, retain versions of backup data and metadata to protect the Salesforce organization.

Table 19-1 *(continued)*

Prerequisite	Description
Profile (Backup Admin), user (Backup Admin), and Connected App setup within the Salesforce organization	You are required to create a user, a profile, and a Connected app in each Salesforce organization that is to be backed up. See "Configure User, Profile, and Connected App for Salesforce" on page 196. For backing up unstructured data objects, the Backup Admin must have the **Query All Files** permission. **Note:** A Connected App is a mechanism that securely links external applications to Salesforce, enabling controlled access to Salesforce data and metadata through OAuth authentication, with customizable permissions and settings.
Sharing of public library	To protect the public libraries in the target organization, they must be shared with **Backup Admin** with **Library Administrator** access permission.

Table 19-1 *(continued)*

Prerequisite	Description
Auto-number field	

Table 19-1 *(continued)*

Prerequisite	Description

	If you want to restore Auto-number field with the same value as it was backed up.
	
	Salesforce's standard Auto-number fields (for example, Case Number) come with an additional restriction — their field type cannot be modified. Uploading data to a standard Auto-number field requires that the standard field be replaced with a copy used in place of the standard field.
	
	To set up a copy of the standard/custom field:
	
	■ Create a new custom field to hold the Auto-number data.
	■ Use the following trigger to populate the new custom field:
	`trigger PopulateCustomAutonumberForCase on Case (after insert, after update) {`
	`List<Case> casesToUpdate = new List<Case>();`
	`for (Case c : Trigger.new) {`
	`// Handle after insert and after update`
	`// Check if the custom autonumber field is null`
	`if (String.isBlank(c.CustomAutonumber__c)) {`
	`// Collect the IDs of cases that need updating`
	`casesToUpdate.add(c);`
	`}`
	`}`
	`if (!casesToUpdate.isEmpty()) {`
	`List<Case> casesToEdit = [SELECT Id, CustomAutoNumber__c, CaseNumber FROM Case WHERE Id IN :casesToUpdate]; for (Case c :`

Table 19-1 *(continued)*

Prerequisite	Description

	`casesToEdit) {`
	`// Populate the custom field with the standard case number field c.CustomAutonumber__c = c.CaseNumber; }`
	`update casesToEdit;`
	`}`
	`}`
	For objects that already have an auto-number field in your Salesforce organization, you must first add the custom field manually.

Marketing User permission	If you want to restore the Campaign object, the **Backup Admin** user must have the **Marketing User** permission.

Configure User, Profile, and Connected App for Salesforce

This topic describes the procedure to create a user, profile, and a Connected App in Salesforce (Lightning Experience) for use by Cohesity Alta SaaS Protection.

Before you configure a Connected App, create a dedicated Salesforce user for Cohesity Alta SaaS Protection and grant the permissions it needs to perform backup and restore operations using Salesforce APIs.

- Create a dedicated integration user: Create a Salesforce user (for example, Cohesity Backup Admin) that is used exclusively for backup and restore operations.
- Assign a supported Salesforce license: The Cohesity Backup Admin user must be assigned a Salesforce license. Cohesity Alta SaaS Protection does not currently support the Salesforce API Integration License, as it provides limited access to Salesforce objects and features.
- There are two options to create a profile:
  - Option A (recommended): Create a custom profile by cloning System Administrator: Create a new custom profile by cloning the System Administrator profile (for example, Cohesity Backup Admin profile).
  - Option B (alternative): Standard User + Permission Set. Use this approach if your organization's security policies do not allow cloning the System Administrator profile.

Option B (alternative): Standard User + Permission Set. Use this approach if your organization's security policies do not allow cloning the System Administrator profile. It is strongly recommended to assign all permissions listed in the Required Permissions table below. These permissions determine what the integration user can read and write through Salesforce APIs during backup and restore. If any permissions are excluded, Cohesity assumes that the customer understands the associated risks and may not provide support for related issues.

For Option B (Permission Set approach):

- Create the permission set and assign all required permissions to the Cohesity Backup Admin user before you authorize that user for the Connected App.
- Create the Cohesity Backup Admin user with a Standard User profile (not System Administrator).
- Assign the permission set to the Cohesity Backup Admin user (instead of granting permissions via a cloned admin profile).

Required Permissions (Permission Set Checklist)

Use the checklist below to build the permission set. At a minimum, ensure coverage for object permissions, field-level security, and record types across both standard and custom objects.

- Object permissions: Modify All and Create permissions for all objects in the Salesforce organization (standard and custom).
- Field permissions: Read Access and Edit Access for all fields across all objects (standard and custom).
- Record type permissions: Read and Edit access for all record types across all objects (standard and custom).
- Additional requirements
  - Ensure all relevant feature permission sets are assigned.
  - Ensure the user has all required feature licenses for any installed AppExchange products.

A few permissions (for example, Modify All Data) can automatically enable other permissions. In addition, Salesforce may auto-enable permissions that are not explicitly listed in the table based on what you select. Do not remove any auto-enabled permissions if they are required for Cohesity Alta SaaS Protection features to work as expected.

Table 19-2

Permissions	Data / Metadata / Both	Salesforce Description	Used by Cohesity Alta SaaS Protection for
Access Activities	Data	Access tasks, events, calendar, and email.	Protection (backup and restore) of Tasks, Events, Calendar and Email
Access Libraries	Data	Access libraries.	Protection of Libraries
Apex REST Services	Data	Allow access to Apex REST services	Access to Salesforce APIs
API Enabled	Both	Access any Salesforce.com API.	To access Salesforce APIs for backup and restore of Data and Metadata
Assign Topics	Data	Assign existing topics to feed items. Remove topics from feed items.	Restore of FeedItem (while assigning a topic to FeedItem)
Author Apex	Metadata	Create Apex classes and triggers.	Restore of Apex classes and Triggers
Change Dashboard Colors	Metadata	Choose dashboard color theme and palette.	Restore of Dashboards
Chatter Internal User	Data	Use all Chatter features.	Protection of Chatter Objects
Create and Own New Chatter Groups	Data	Use all Chatter features.	Protection of Chatter Objects
Create Content Deliveries	Data	Create content delivery links to share files that aren't managed by a library. To let a user create content deliveries for files in a library, enable Deliver Content for that user in the library.	Protection of Salesforce Orgs where Content Delivery feature is enabled. Restore of public link Field for the Document/Attachment requires this.

Table 19-2 *(continued)*

Permissions	Data / Metadata / Both	Salesforce Description	Used by Cohesity Alta SaaS Protection for
Create Folders for Lightning Email Templates	Metadata	Create Folders for Lightning Email Templates.	Restore of Email Template (in Folder)
Create Libraries	Data	Create libraries.	Restore of Library
Create Public Links	Data	Let users create links to share files externally. Unlike content deliveries, public links can't be password protected. To let a user create links to files in a library, enable Deliver Content for that user in the library.	Restore of Public Links of Documents / Attachments / Files
Create Topics	Data	Create new topics by assigning them to feed items.	Restore of FeedItem (while assigning a topic to FeedItem)
Customize Application	Metadata	Customize the organization using App Setup menu options.	Required for 'Connected App' backup. Restore of various Metadata types, for example, Custom Fields, Page Layout and so on.
Edit HTML Templates	Metadata	Edit Classic HTML Email Templates.	Restore of Email Templates
Edit Read Only Fields	Data	Edit fields that are read only due to page layouts or field-level security.	Restore values back into some fields that are read-only due to page layout or field level security
Edit Tasks	Data	Create, edit, and delete tasks.	Restore of Tasks

Table 19-2 *(continued)*

Permissions	Data / Metadata / Both	Salesforce Description	Used by Cohesity Alta SaaS Protection for
Edit Topics	Data	Edit topic names and descriptions.	Restore of Topics
Manage All Private Reports and Dashboards	Metadata	Allows full access to reports and dashboards in all other users' private folders (API only).	Restore to reports and dashboards in all other users' private folders (API only).
Manage Auth. Providers	Metadata	Create and edit Auth. Providers	Restore of Auth Providers
Manage Certificates	Metadat	Ability to manage certificates	Protection of Certificates
Manage Chatter Messages and Direct Messages	Data	Access all users' messages sent in Chatter.	Protection of Chatter data
Manage Connected Apps	Metadata	Manage, create, edit, and delete connected applications.	Restore of Connected Apps
Manage Custom Permissions	Metadata	Create, edit, and delete custom permissions.	Restore of Permission Sets and Profiles
Manage Custom Report Types	Metadata	Create, edit, and delete custom report types.	Restore of Custom Reports
Manage Dashboards in Public Folders	Metadata	Create, edit, delete dashboards, and manage their sharing in all public folders.	Restore of Custom Dashboards
Manage Data Categories	Metadata	Create, edit, and delete data categories.	Protection of 'DataCategoryGroup' backup
Manage Data Integrations	Data	Monitor or abort Bulk API jobs.	Bulk API management (during backup and restore)

Table 19-2 *(continued)*

Permissions	Data / Metadata / Both	Salesforce Description	Used by Cohesity Alta SaaS Protection for
Manage Letterhead	Both	Create, edit, and delete letterheads for HTML emails.	Protection of Email Letterheads.
Manage Multi-Factor Authentication in API	Metadata	Use the API to manage user identity verification methods for multi-factor authentication.	Required for Metadata Backup
Manage Public Classic Email Templates	Metadata	Create, edit, and delete text emails, mail merge templates, and folders for public email templates.	Restore of Email Template in Folder
Manage Public Documents	Data	Create, edit, and delete folders for public documents.	Restore of Folders for Documents
Manage Public List Views	Metadata	Create, edit, and delete public list views	Restore of List Views
Manage Reports in Public Folders	Data	Create, edit, delete reports, and manage their sharing in all public folders.	Restore of Reports in Public Folder
Manage Unlisted Groups	Metadata	View and moderate unlisted Chatter groups.	Protection of Unlisted Groups
Manage Users	Metadata	Create, edit, and deactivate users, and manage security settings, including profiles and roles.	Restore of Users

Table 19-2 *(continued)*

Permissions	Data / Metadata / Both	Salesforce Description	Used by Cohesity Alta SaaS Protection for
Modify All Data	Data	Create, edit, and delete all organization data, regardless of sharing settings	Needed for auto-inclusion of new objects and related objects. Third party product objects, custom objects as and when they get added to the Org, they will get picked up by Alta SaaS Protection only if this permission is given. Also, some objects (TopicAssignment, FeedRevision, FeedAttachment, Announcement, FeedComment, EntitySubscription) require this permission for query. A few other objects require this permission for Metadata restore.

Table 19-2 *(continued)*

Permissions	Data / Metadata / Both	Salesforce Description	Used by Cohesity Alta SaaS Protection for
Modify Metadata through Metadata API Functions	Metadata	Create, read, edit, and delete org metadata. Users must have appropriate access rights to the metadata they're trying to modify. Be careful if delegating this permission. Some metadata executes in system context, when object permissions, field-level security, and sharing rules that apply to the user are ignored. For example, Apex executes in system context.	Metadata restores
Update Email Messages	Data	Modify certain email message related records.	Restore of Email Messages
View All Custom Settings	Metadata	Let users view all custom setting data directly and via the API.	Protection of Custom Settings
View All Lookup Record Names	Data	View the record names in lookup fields regardless of sharing settings. Lookup fields include system fields, such as Created By and Last Modified By.	Backup of System Fields
View All Profiles	Metadata	View all user profiles, regardless of profile filtering setting.	Backup of Profiles

Table 19-2 *(continued)*

Permissions	Data / Metadata / Both	Salesforce Description	Used by Cohesity Alta SaaS Protection for
View And Edit Converted Leads	Data	View and edit converted lead records.	Restore of Converted Leads
View Developer Name		View the DeveloperName field via the API.	Backup of Developer Name field
View Encrypted Data	Data	View the value of encrypted fields in plain text.	Protection of Encrypted Fields
Edit Case Comments	Data	Edit their own case comments but not other user's comments.	Restore of CaseComment
Import Solutions	Data	Import solutions for the organization.	Protection of Solutions
Manage Cases	Data	Administer case settings, including Email-to-Case and mass transfer of cases.	Protection of Cases
Manage Categories	Data	Define and modify solution categories settings.	Define and modify solution categories settings.
Manage Entitlements	Data	Enable, create, and update entitlement management items.	Enable, create, and update entitlement management items.
Manage Content Permissions	Data	Create, edit, and delete library permissions in Salesforce CRM Content.	Create, edit, and delete library permissions in Salesforce CRM Content

Table 19-2 *(continued)*

Permissions	Data / Metadata / Both	Salesforce Description	Used by Cohesity Alta SaaS Protection for
Manage Content Properties	Data	Create, edit, and delete custom fields in Salesforce CRM Content.	Create, edit, and delete custom fields in Salesforce CRM Content
Manage Flow	Data	Allow users to view, create, edit, delete, and activate all flows and flow types in Lightning Experience apps and Setup.	Protection of Workflows
Manage record types and layouts for Files	Both	Create, edit, and delete content types in Salesforce CRM Content..	Create, edit, and delete content types in Salesforce CRM Content.
Manage Salesforce CRM Content	Data	Create, edit, and delete libraries and library memberships.	Create, edit, and delete libraries and library memberships.
Query All Files	Data	Allows View All Data users to SOQL query all files in the org.	Protection of Documents / Attachments / Files / Salesforce CRM Content

Create user and profile

You may be using Salesforce Lightning Experience or Classic Experience. Use this procedure to create a user and profile in Salesforce Lightning Experience.

To create user and profile

1. Log in to your Salesforce org using a user with the System Administrator profile.
2. Click **Setup**.
3. Locate the profile setup by typing **profile** in the search box on the left.
4. Click **New Profile**.
5. Select System Administrator from the list to create a clone of the profile.
6. Enter a name for the profile (for example, Cohesity Backup Admin Profile).

7 Click **Save**.

8 Go to the profile you have just created and click **Edit**.

9 Assign the following permissions to the profile:

- Modify All Data
- API enabled
- View Encrypted Data
  If encrypted fields are used for standard/custom objects.
- Query all files
  To back up private library files for all users.
- View and Edit Converted Leads
  If the lead has been converted and needs to be restored.

10 Click **Save**.

11 Click **View Users** > **New User** to create a new user.

12 Enter user details like First Name, Last Name, Username, Email and then select the profile created earlier.

13 Click **Save**.

14 Log off, then log on using the newly created user.

Configure Connected App

To Configure Connected App

1 Log on using the newly created user.

2 Click **Setup**.

3 Locate the App Manager setup by typing it in the search box on the left.

4 On the top right, click **New Connected App**.

5 Select **Create a Connected App** option and click **Continue**.

6 Provide the basic information for the new app, such as the name.

7 Click the checkbox to enable OAuth settings. Set the callback URL to **http://localhost:1717/OauthRedirect**.

8 Select **Full Access** and **Perform requests at any time (refresh_token, offline_access)** from the list of the available OAuth scopes. This is required by the app for permissions to back up and restore various objects and records.

9 Click **Save**.

10. Go to the app created above and look for the consumer key. Copy the consumer key to a text file for use later. This is required when creating a connector on the Cohesity Alta SaaS Protection Web UI.
11. Go to the Cohesity Alta SaaS Protection Web UI to create a Salesforce connector.
12. Enter the Salesforce username, instance URL, and consumer key.
13. To find the instance URL, log in to the Salesforce org, click **Setup**, type **My Domain**, click **My Domain**, copy the **Current My Domain URL**, and add **https://** to the beginning.
14. Click **Generate certificate** and download the certificate.
15. When entering the username, ensure that the user is part of the profile (for example, Cohesity Backup Admin Profile) associated with the connected app so that access is limited to the user.
16. Go back to the Salesforce app created earlier and click Edit to associate the certificate created by Cohesity Alta SaaS Protection and to relax IP restrictions.
17. Click the **Use Digital Signature** checkbox and upload the certificate created by Cohesity Alta SaaS Protection using the **Choose File** button.
18. Keep all other settings as default and click **Save**.
19. From the **App Manager**, locate this app and click **Manage**.
20. Click **Edit Policies**.
21. Under **OAuth Policies**, set Permitted Users to Admin approved users are pre-authorized and set IP Relaxation to Relax IP restrictions. Keep default values for all other settings.
22. Click **Save**.
23. Scroll down and click M**anage Profiles**.
24. Select the profile associated with the user who can use this connected app for backup and restore. For example, select the Cohesity Backup Admin Profile.
25. Click **Save**.
26. This completes the setup of the Connected App in Salesforce for users using Lightning Experience.

Add Salesforce connectors

You need to create a separate connector for each Salesforce organization you want to back up. Each connector backs up data, files, attachments, CRMs, and metadata. Cohesity Alta SaaS Protection uses two different storages: one for unstructured

content like files, attachments, and metadata, and another for structured content like objects and records.

Before adding a connector, refer to the following topic for prerequisites and to understand the key considerations:

See "Key considerations and prerequisites for adding Salesforce connectors" on page 190.

To add a Salesforce connector to back up data and metadata

1. Access the Cohesity Alta SaaS Protection Administration portal.

   The home page of the Administration portal is displayed.

2. On the **Backup** card, click **Connectors**.
3. Click **New backup connector**.
4. Click **Salesforce**.
5. On the **General** tab, do the following:
   - In the **Name** field, enter a name for the connector.

     Note: The **Type** field displays the connector type.

   - From the **Stor for unstructured data (files, attachments and metadata)** dropdown list, select the SalesforceFiles Stor provided by Cohesity as a prerequisite for connector creation.

     Note: The same Stor can be used for multiple connectors. If unavailable, contact Cohesity Support.

   - From the **Stor for structured data (objects and records)** dropdown list, select the SalesforceFiles Stor provided by Cohesity as a prerequisite for connector creation.
     If the Stor is not available, contact Cohesity Support.
   - The **Machine** field displays the Connector service to host this connector. You can change the selected one from the list if required.
   - (Optional) Enable the **Enable email notification** option to receive backup job status email notifications.
   - Click **Next**.
6. On the **Capture scope** tab, configure your backup scope.

By default, Salesforce connectors back up all Standard objects, Custom objects, files, attachments, CRMs, and metadata from the targeted Salesforce organization except for **Feed**, **History**, and **Share** objects, as these objects are not typically critical for business continuity.

However, you can enable backups for these objects based on your specific needs, considering the following:

- **History** objects:
  These objects cannot be restored. Select them for backup only if retaining historical information on record or field-level changes is necessary for auditing purposes.
- **Share** objects:
  Only manual Share objects can be restored. Other types of Share objects cannot be restored due to Salesforce API limitations.

  Note: During the Salesforce restore, Share tables are automatically created unless they contain manual Share rules.

- **Feed** objects:
  Feed objects are views into the **FeedItem** object. Cohesity Alta SaaS Protection backs up only the **FeedItem** object to avoid duplication. Due to Salesforce API limitations, only specific types of FeedItem records can be restored.
  Skipping these objects accelerates the backup process and reduces the storage required for Cohesity Alta SaaS Protection recovery points.

Refer to the following topic to know the backup limitations of Salesforce connectors.

See "Limitations of Salesforce connectors" on page 211.

While backing up a Salesforce organization, a field length mismatch may sometimes occur, resulting in a backup failure. Check the error logs to identify the fields that have returned more data than current field length. It is recommended to widen the field length of these fields in your Salesforce organization to prevent backup failures and ensure that all data is backed up. If widening the field length of these fields is not possible, enable the **Allow backup of fewer characters if data returned by API is more than Field length** checkbox to back up only the initial characters that fit within the current field length. Note that the remaining characters will not be backed up.

7 On the **Credentials** page, do the following:.

- From the **Salesforce organization type** dropdown list, select the required type: **Production** or **Sandbox**.
- In the **Salesforce organization user name** field, enter the name of the Backup Admin user you have created within the targeted Salesforce organization as pre-requisites.
- In the **Salesforce organization instance URL** field, enter the URL of the targeted Salesforce organization.
- In the **Consumer key** field, enter the key, which is generated while adding the Cohesity Alta SaaS Protection Connected app to the targeted Salesforce organization.
- Click **Generate certificate**.
  A success message is displayed.

Note: Certificate is used for OAuth-based authentication.

- On the pop-up, click **Keep** to download the certificate.
- Save the certificate to the local computer.
- Click **Next**.

8 On the **Scheduling** tab, schedule backup jobs.

See "Schedule a backup" on page 115.

9 On the **Email notifications** tab, configure email addresses to receive notifications about backup activities.

See "Configure email addresses to get notifications" on page 116.

10 On the **Review** tab, save the settings and initiate the backup.

See "Review configuration and edit/save/initiate backup" on page 116.

11 Go to the targeted Salesforce organization, upload the generated certificate.

See "Configure User, Profile, and Connected App for Salesforce" on page 196.

Uploading a certificate to the Salesforce organization establishes secure communication and authenticates the connection between the targeted Salesforce organization and Cohesity Alta SaaS Protection. The process uses certificate-based OAuth authentication, linking the certificate to the Connected App in Salesforce organization to securely access Salesforce data and metadata with user consent.

Key points to remember:

- Always upload the certificate after completing the connector creation process.
- A new certificate is created if you accidentally click the **Generate Certificate** option on the **Credentials** tab. In such cases, replace the existing certificate with the new one.
- If you edit the connector configuration, generate a new certificate and re-upload it.

Related topics:

- See "Perform on-demand/ad-hoc backup" on page 239.
- See "Edit connector configuration" on page 121.
- See "Delete connectors" on page 121.
-
- See "Browse backed-up data" on page 245.c
- See "View backup events" on page 241.

Limitations of Salesforce connectors

The following are the Salesforce connector limitations for the current release:

- **Unsupported functionalities**:
  - Deletion, Tagging, and Retention policies.
    Backed-up data is retained indefinitely with Cohesity Alta SaaS Protection.
  - Scopes and Custodian Groups.
  - Auto-scaling, auto-sharding, and splitting of connectors.
- **Refer to the following links for other limitations**:
  See "Salesforce Objects not supported for backup" on page 211.
  See "Salesforce Objects not supported for restore" on page 315.
  See "Limitations of Salesforce Data restore" on page 313.
  See "Limitations of Salesforce Metadata backup and restore" on page 325.

Salesforce Objects not supported for backup

Cohesity Alta SaaS Protection does not support the backup of the following:

- **Event objects**:

These objects store transient information and are not designed to hold long-term data like classic Salesforce objects.

- **External objects**:
  Cohesity Alta SaaS Protection backs up data primarily stored within the Salesforce organization. These objects are not stored within the Salesforce organization, hence, not supported for the backup.
- **Objects not supporting the Salesforce API Query():**
  The objects that do not support the Salesforce API query() function cannot be backed up.
- **Big objects**:
  The backup of Big objects is not supported.
- **Unsupported Salesforce objects**:
  Some objects are inherently unsupported by Salesforce for backup.
- **Certain fields in the User object**:
  The following fields in the **User** object are not supported for the backup:
  - Load Lightning Pages While Scrolling
  - Send Apex Warning Emails
  - Quick Access Menu
    For more information, refer to the **User** topic in Standard Objects / User
- **Limitations due to API limitations**:
  - Private Dashboards and Reports cannot be backed up.
    Only Public Dashboards and Reports are supported for backup.
  - The image in the ContentNote cannot be backed up.
    Salesforce does not provide any API for retrieving images from a ContentNote. Therefore, if a ContentNote contains an image, it will not be backed up or restored.
    ContentNote is a non-restorable object because it is automatically restored during the restoration of the associated ContentDocument. To restore a ContentNote, restore the corresponding ContentDocument record(s).
  - When using the Salesforce Bulk API to upload data, the API does not preserve CRLF (\r\n) line endings in uploaded files—particularly in text-based formats such as CSV. Instead, it normalizes line endings to LF (\n).
- **Following is the complete list of objects not supported for backup**:
  - *ChangeEvent
  - ApexPageInfo

- ApexTypeImplementor
- AppDefinition
- AppTabMember
- AttachedContentDocument
- AuraDefinitionBundleInfo
- AnlytDataAssetEventStore
- CaseMilestone
- CollaborationInvitation
- ColorDefinition
- CombinedAttachment
- DataStatistics
- *dlm
- DataType
- DcsnTblSourceObjectRecord
- DelegatedAccount
- EmbeddedServiceDetail
- EmbeddedServiceLabel
- EntityDefinition
- EntityMilestone
- EntityParticle
- ExpressionFilterCriteria
- ExternalDataSource
- ExternalDataUserAuth
- FeedLike
- FeedSignal
- FeedTrackedChange
- FieldDefinition
- FlexQueueItem
- FlowDefinitionView
- FlowOrchestrationInstance

- FlowOrchestrationWorkItem
- FlowRecordRelation
- FlowTestView
- FlowVariableView
- FlowVersionView
- FormulaFunction
- FormulaFunctionAllowedType
- FormulaFunctionCategory
- IconDefinition
- IdeaComment
- IIdpEventLog
- Image
- ListViewChartInstance
- LogoutEventStream
- LookedUpFromActivity
- MobileApplicationDetail
- MyDomainDiscoverableLogin
- Name
- NetworkActivityAudit
- NetworkDiscoverableLogin
- NetworkModeration
- NetworkSelfRegistration
- NoteAndAttachment
- MobileDeviceAppRegistration
- OpenActivity
- OauthToken
- OrgLifecycleNotification
- OutgoingEmail
- OutgoingEmailRelation
- OwnedContentDocument

- OwnerChangeOptionInfo
- PermissionSetGroupComponent
- PicklistValueInfo
- PlatformAction
- PlatformEventUsageMetric
- PromptVersion
- Publisher
- UserSharedFeature
- UserAppMenuItem
- RecentlyViewed
- Recommendation
- RecommendationResponse
- RelatedListColumnDefinition
- RelatedListDefinition
- RelationshipDomain
- RelationshipInfo
- Scontrol
- ScorecardAssociation
- SearchLayout
- SecurityCustomBaseline
- Site
- SiteDetail
- SiteIframeWhiteListUrl
- SPSamlAttributes
- StaticResource
- TwoFactorMethodsInfo
- UserEntityAccess
- UserFieldAccess
- UserRecordAccess
- UserSetupEntityAccess

- Vote

Chapter 20

Protect Entra ID objects

This chapter includes the following topics:

- Setting up Entra ID protection with Cohesity Alta SaaS Protection
- Backup and restore limitations for Entra ID

Setting up Entra ID protection with Cohesity Alta SaaS Protection

To protect your Entra ID environment using Cohesity Alta SaaS Protection, you need to add and set up a Cohesity Alta SaaS Protection Entra ID connector based on your backup requirements.

Before you begin:

You must know the following before adding a connector:

- **The following items are supported for backup and restore**:
  - Users: It includes backing up the user-related data such as profiles, settings, permissions, and other user-specific information.
  - Groups: It includes backing up the structure, memberships, and settings associated with the groups.
  - Application Registrations: It includes backing up the configurations, settings, and information associated with applications registered within the Entra ID environment.
  - Enterprises Applications: It includes backing up the configurations, settings, and data associated with enterprise-level applications registered and used within the Entra ID environment.
- **The following items/scenarios are not supported for backup and restore:**

- Backup and restore of passwords and multifactor authentication are not supported due to Graph API limitations.
- Restore of multifactor authentication for the permanently deleted users is not supported.
- Backup and restore of Application Registrations and Enterprise Applications' secrets are not supported.
- Restore of Distribution Lists or Mail-enabled security groups is not supported.
- Restore of eligible assignments and assignments with expired dates is not supported due to Graph API limits.
- Backup and restore of photos or logos are not supported.
- Only cloud-native attributes are restored for on-premises synchronized objects.
- To perform restore of an Enterprise Application, its corresponding Application Registration should be restored first.
- Restore of Enterprise Application for which the corresponding Application Registration is permanently deleted is not supported.

Step-by-step procedure to add a Microsoft Entra ID connector:

Each tab in the connector creation workflow includes a help icon (?) on the left. Click this icon to open the corresponding help topic for that tab, which guides you through the setup process step by step.

Procedure:

1 **Access the Administration portal and select the connector type**.
   - Access the Administration portal.
   - Click **Connectors** on the **Backup** card.
   - Click **New backup connector**.
   - Click **Microsoft Entra ID**.
     Do any of the following:
     - Play the video that guides you through the Entra ID connector creation process. After the video ends, close the page. This action directs you to the **New Connector** page where you can proceed to create a connector.
     - Click **Skip** if you prefer not to watch the video. This action directs you to the **New Connector** page where you can proceed to create a connector.

- Select the **Don't show this again** check box to avoid seeing this page when you create subsequent Entra ID connectors.

2. On the **General** tab, set up the basic configuration for the connector.

   See "Configure General settings" on page 83.

3. On the **Capture scope** tab, click **Next**.
4. On the **Credentials** tab, configure credentials to access the source workloads (the SharePoint data to be backed up) and click **Next**.

   See "Configure credentials" on page 88.

5. On the **Scheduling** tab, schedule when the backup job should run.

   See "Schedule a backup" on page 115.

6. On the **Email notifications** tab, configure email addresses to receive notifications about backup activities.

   See "Configure email addresses to get notifications" on page 116.

7. On the **Review** tab, save the settings and initiate the backup.

   See "Review configuration and edit/save/initiate backup" on page 116.

Related topics:

- See "Connector status" on page 119.
- See "Perform on-demand/ad-hoc backup" on page 239.
- See "Video tutorial for connector troubleshooting" on page 241.
- See "About Entra ID (Azure AD) objects and records restore " on page 327.

Backup and restore limitations for Entra ID

The backup and restore limitations of the Microsoft ID connector are:

- Backup and restore of passwords and multifactor authentication are not supported due to Graph API limitations.
- Restore of multifactor authentication for the permanently deleted users is not supported.
- Backup and restore of Application Registrations and Enterprise Applications' secrets are not supported.
- Restore of Distribution Lists or Mail-enabled security groups is not supported.
- Restore of eligible assignments and assignments with expired dates is not supported due to Graph API limits.

- Backup and restore of photos or logos are not supported.
- Only cloud-native attributes are restored for on-premises synchronized objects.
- To perform restore of an Enterprise Application, its corresponding Application Registration should be restored first.
- Restore of Enterprise Application for which the corresponding Application Registration is permanently deleted is not supported.

Chapter 21

Protect Box data

This chapter includes the following topics:

- Prerequisites for Box connectors configuration
- Setting up Box protection with Cohesity Alta SaaS Protection
- Backup limitations for Box data

Prerequisites for Box connectors configuration

For the Prerequisites for Box connectors configurations, refer to the following knowledge base article:

How to create a Box.com Application For Authentication to Cohesity Alta SaaS Protection

Setting up Box protection with Cohesity Alta SaaS Protection

To protect user's data in your Box environment using Cohesity Alta SaaS Protection, you need to **add and set up a Cohesity Alta SaaS Protection Box connector** based on your backup requirements.

Before you begin:

You must know the following before adding a connector.

- **Ensure all prerequisites are completed**.
  See "Prerequisites for Box connectors configuration" on page 221.
- **The following items are supported for the backup and restore:**
  - Files and folders:

    - All files and folders for all users, or a set of specified users, including documents, spreadsheets, presentations, images, videos, and other file types.
    - All folders and files shared with the user being processed. For instance, all data accessible to a user is backed up in the context of that user. If the same folder is shared with ten users, it is backed up ten times (once per user). Deduplication ensures that only one physical copy is stored.
  - Version history: The version history of files, including all previous revisions and versions that have been trashed.
  - Access control: Set the Access Control List (ACL) for backed-up content to the user whose account the content belongs to. Similar to O365 mailboxes and OneDrive for Business, existing ACLs are ignored, and a specific user's ACL is applied.
  - Metadata: All tags applied to files.
  - Notes: Notes for collaborative note-taking. The raw Boxnote file is backed up and can be restored properly.
  - Deletion policy: Delete file versions and files that match the deletion policy. If the last version of a file is deleted, the file is removed. An option to purge deleted content (bypassing the Box trash) is available.
  - Restore of folders and files back to Box:
    - Missing files can be restored with their entire version history.
    - Existing files will have only the latest version restored from the backup and made the current version.
- **The following items/scenarios are not supported for backup**:
  - Deleted files (in Trash)

    Note: If a file and all its versions are in the trash, its content will not be backed up. However, if only some versions are in the trash while the file remains active, those versions will still be backed up.

  - Sharing permissions.
  - Comments on files.
  - Custom metadata for files, beyond basic information such as last modified date, size, and data owner.
  - Tasks.

  - Folder's and file's retention information.
  - Folder's and file's legal hold information.
- **The following items/scenarios are not supported for restore:**
  - Multiple versions of the files.
  - Any content that was not backed up.
  - Recreation of the permissions on restore.
  - Recreation of the shares on restore.
  - Custom metadata on folders and files.

Step-by-step procedure to add a Box connector:

Each tab in the connector creation workflow includes a help icon (?) on the left. Click this icon to open the corresponding help topic for that tab, which guides you through the setup process step by step.

Procedure:

1. **Access the Administration portal and select the connector type**.
   - Access the Administration portal.
   - Click **Connectors** on the **Backup** card.
   - Click **New backup connector**.
   - Click **Box**.
2. On the **General** tab, set up the basic configuration for the connector and click **Next**.

   See “Configure General settings” on page 83.
3. On the **Capture scope** tab, configure the capture scope.

   See “Configure capture scope for Box connector” on page 224.
4. On the **Credentials** tab, do the following:

Credentials JSON	Copy the content from a JSON file, which is generated as part of the prerequisites.

5. On the **Configure policy** tab, configure backup policy.

   See “Configure Custom backup policy and guidelines” on page 93.
6. On the **Scheduling** tab, schedule when the backup job should run.

   See “Schedule a backup” on page 115.

7 On the **Email notifications** tab, configure email addresses to receive notifications about backup activities.

See "Configure email addresses to get notifications" on page 116.

8 On the **Review** tab, save the settings and initiate the backup.

See "Review configuration and edit/save/initiate backup" on page 116.

Related topics:

- See "Connector status" on page 119.
- See "Perform on-demand/ad-hoc backup" on page 239.
- See "Video tutorial for connector troubleshooting" on page 241.
- See "Restore Box data" on page 290.

Configure capture scope for Box connector

To configure backup scopes for Box data

1 Do one of the following:

- Option 1: Click **All users** to back up the data of all users in the Box environment.
- Option 2: Do the following to back up the data of specific users:
  - Click **Specific users**.
  - Expand **Specific users** and click **+ Add users**.
  - On the **Add users address** page, enter users' email addresses. Use semicolon between email addresses.
  - Click **Add**.

2 To back up all versions of the items, select the **Capture Old Versions** check box.

Clear the check box to backup the most recent version of data.

3 To back up the data, which is deleted but not yet purged from Box, do the following:

- Select the **Capture Old Versions** check box.
- Select the **Capture Deleted Versions** check box.
  Clear the check box to skip backup of the data in the trash.

4. To restrict the backup scope to few folders.

   See “Configure Folder filter” on page 87.

5. After configuration of the backup scope, click **Next** to configure credentials. For more information, (see Step 9)

Backup limitations for Box data

The following items in the Box environment are not supported for backup:

- Deleted files (in Trash)

  Note: If a file and all its versions are in the trash, its content will not be backed up. However, if only some versions are in the trash while the file remains active, those versions will still be backed up.

- Sharing permissions.
- Comments on files.
- Custom metadata for files, beyond basic information such as last modified date, size, and data owner.
- Tasks.
- Folder's and file's retention information.
- Folder's and file's legal hold information.

Chapter 22

Protect Email/Message data

This chapter includes the following topics:

- Prerequisite for Email/message connector
- Add Email/Messages file

Prerequisite for Email/message connector

Outlook 64-bit must be installed on the server running the Cohesity Alta SaaS Protection Connector service where the EML files connector is running.

After the prerequisites' procedures are completed, you can add a connector.

Add Email/Messages file

The Email/Message file connector is used to archive .EML or .MSG files available on a file share.

To add an EML/Messages file connector

1. Access the Administration portal.

   The home page of the Administration portal is displayed.
2. Click **Backup**.
3. On the left, click **Connectors**.
4. Click **New backup connector**.

5 Click **Email/Message file** and then click **Next**.

To make the setup process easier and more intuitive, each tab in the connector creation workflow includes a help icon **(?)** at the left. You can click this icon to open the respective help topic for that tab, which can guide you through the setup step by step.

6 Configure the general settings such as the name, the storage to store the backed-up data, and so on.

See "Configure General settings" on page 83.

7 On the **Capture scope** page, do the following and click **Next**.

- Click **Eml** or **Msg**.
  - **Eml**: Click this option to back up the .EML files from the source.
  - **Msg**: Click this option to back up the .Msg files from the source.
- Select the following options as required.

Use sender and recipients for ACL	Select this check box to override the parent folder ACL with SMTP permission of the sender and recipient.
Use Subject as Item name	Select this check box to back up the emails using the subject of the email. If this check box is not enabled, the email gets ingested based on the actual file name. It is recommended to enable this option.

- Restrict the backup scope to specific required folders only.
  See "Configure Folder filter" on page 87.

8 Click **Next**.

9 On the **Scheduling** tab, schedule when the backup job should run.

See "Schedule a backup" on page 115.

10 On the **Email notifications** tab, configure email addresses to receive notifications about backup activities.

See "Configure email addresses to get notifications" on page 116.

11 On the **Review** tab, save the settings and initiate the backup.

See "Review configuration and edit/save/initiate backup" on page 116.

Chapter 23

Configure Retention policies

This chapter includes the following topics:

- About WORM policies
- Ingestion WORM policies page
- Add/edit Ingestion WORM retention policies and guidelines
- Add/edit At-Rest WORM retention policies
- Add/edit Deletion policies
- View deletion history
- How to edit the policy evaluation interval?
- How to add a Location filter?
- How to add a filter?

About WORM policies

All data in Cohesity Alta SaaS Protection is retained indefinitely by default. Cohesity Alta SaaS Protection has a Write Once Read Many (WORM) retention policy for its storage (Stor). This policy ensures that the backed-up data cannot be modified or deleted for a specified duration. Once an item is stored in the WORM, it can be read multiple times but cannot be overwritten, modified, or deleted. You can set a retention period to specify how long a particular item must be kept in the storage (Stor). After the retention period, the item can be deleted if needed. The WORM policies make sure that items are only purged once they are eligible for deletion.

You can define and apply policies to the items at the time of ingestion or after ingestion when the data is stored on the storage (Stor).

Table 23-1

WORM policy types	Description
Ingestion WORM retention policy	Applies the specified retention period to items while they are ingested into Cohesity Alta SaaS Protection.See "Add/edit Ingestion WORM retention policies and guidelines" on page 230.
At-Rest WORM policy	Applies the specified retention period to items after they are ingested into Cohesity Alta SaaS Protection. See "Add/edit At-Rest WORM retention policies" on page 232.

Ingestion WORM policies page

This page lists the ingestion policies configured for your tenant, which you can filter by the type of the Stor and its name.

You can see details such as:

- The name of the policy
- The progress on progress bar
- The next schedule
- The scope, which can be either **Full** (when the policy is applied for the first time) or **Incremental** (when the policy is applied consecutively after the first time).
- The status, which can be **In-Progress**, **Completed**, or **N/A**.
  N/A indicates that the policy is yet to be run.

For a selected policy, you can perform the following tasks using the options provided on the action menu:

Table 23-2

Actions	Description
New policy	Create a new policy. See "Add/edit Ingestion WORM retention policies and guidelines" on page 230.
Enable	Activate the policy to apply it during the ingestion process.

Table 23-2 *(continued)*

Actions	Description
Disable	Deactivate the policy to prevent it from being applied.
Copy	Create a duplicate of the existing policy.
Delete	Remove the policy from the configuration.
Analytics	Go to the **Analytics** page to view statistics related to the policy.
Content	Go to the **Content** page to browse the items on which the policy is applied.

Add/edit Ingestion WORM retention policies and guidelines

Before you begin:

Before you implement retention policies on Cohesity Alta SaaS Protection, consider the following points:

- Items that have a retention period assigned to them cannot be deleted.
- Retention periods can only be extended, not shortened.
- If an item has multiple retention periods, the longest one takes priority, except for when it is in WORM Pending status.
- If an item falls under multiple retention policies, the policy that has WORM pending status plus the one based on the last modified or archival data takes priority.
- Retention periods for existing item versions are applied by event-based retention, and new versions are verified periodically.
- Item-level WORM policies apply retention periods to new items and versions during the writing process without affecting existing versions in storage (Stor).
- Deleting a policy does not affect existing items under the retention period.

Step-by-step procedure to add/edit an ingestion WORM retention policy:

1. Access the Administration portal.

   The home page of the Administration portal is displayed.

2. Click **Retention**.

3. On the left, click **Ingestion WORM retention policies**.

4. Do any of the following:

   - To add a new policy, click **New policy**.
   - To update an existing policy, click the name of the policy.

5. On the **Create policy** page, do the following:

   - Enter an appropriate name for the policy.
   - From the **Stor** dropdown list, select the Stor for which the policy has to be added.
   - By default, the status of the policy is disabled; it is saved but will not run. Toggle the **Status** option to enable the policy.
   - Select any of the following options:
     - **Last modified date**: Select this option to create a policy based on the item's last modified date.
       If a policy is set for a retention period of one month, the item cannot be deleted or modified in the Stor for one month from the last modified date.

       Note: Last modified date: The date on which a user has performed a modification to the item.

     - **Archived date**: Select this option to create a policy based on the item's archived date.
       If a policy is set for a retention period of one month, the item cannot be deleted or modified in the Stor for one month from the archived date.

       Note: Archive date: The date on which the item was previously backed up to Cohesity Alta SaaS Protection.

   - Select the required retention period from the **Retention period** section. (In days, months, or years).

- (Optional) Configure filters to include or exclude specific locations or data from having the policy applied.
  See "How to add a Location filter?" on page 237.
  See "How to add a filter?" on page 238.
- Click **Create** to add a policy or click **Update** to save the changes.

The policy is displayed on the **Ingestion WORM retention policies** page under the storage (Stor) for which you have added the policy.

When a policy is configured and enabled it enforces retention periods during which items cannot be deleted or modified.

Add/edit At-Rest WORM retention policies

Important: Before adding an Ingestion WORM retention policy, you must read the guidelines to understand its implications.

To add/edit an At-Rest WORM retention policy

1. Access the Administration portal.

   The home page of the Administration portal is displayed.
2. Click **Retention**.
3. On the left, click **At-Rest WORM retention policies**.
4. Do any of the following:
   - To add a new policy, click **New policy**.
   - To update an existing policy, click the name of the policy.
5. On the **Create policy** page, perform the following steps:
   - Enter an appropriate name for the policy.
   - From the **Stor** dropdown list, select the Stor for which the policy has to be added.
   - Select one of the following schedules to run the policy:
     - **One time**: This option runs the policy once, and after it has run, the schedule changes to **Never**.
     - **Continuous**: This option runs the policy every time the policy evaluation runs.
     - **Date range**: To schedule the policy, specify a **From** and **To** date range to run.

  - **Never**: Use this option if you are not ready to run the policy or want to stop the policy from running. The time-scheduled policies are converted to Never after they have run.

- Select any of the following action modes as required:
  - **Preview**: Lists the items for retention. To ensure that you understand fully the scope of data that will be retained, run the policy in Preview mode initially.
  - **Production**: Retains the items as per policy.

- By default, the status of the policy is disabled; it is saved but will not run. Toggle the **Status** option to enable the policy.

  As soon as the policy is enabled, it runs as per the schedule that is set in the **Schedule** section.

- Configure the policy based on any of the following criteria:
  - **Last modified date**: Select the option to create a policy based on the item's last modified date.

    If a policy is set for a retention period of one month, the item cannot be deleted or modified in the Stor for one month from the last modified date.

    Note: Last modified date: The date on which a user has performed a modification to the item.

  - **Archived date**: Select the option to create a policy based on the item's archived date.

    If a policy is set for a retention period of one month, the item cannot be deleted or modified in the Stor for one month from the archived date.

    Note: Archive date: The date on which the item was previously backed up to Cohesity Alta SaaS Protection.

  - **Date item**: Select this option to retain the item for a certain period from when it starts meeting the policy.
  - **Exact date**: Select this option to set a specific date for the retention period. For times when you do not want the retention calculated, and you want items to expire on a specific date.
  - **Metadata**: Select the required metadata.

    When this option is selected, the available **datetime** or **smalldatetime** fields in the Stors metadata are displayed in the **Metadata** dropdown.

To retain the item version, you can then specify the period beyond that given date.

- From the **Retention period** dropdown list, set the required retention period (in days, months, or years).
- Select the required retention period from the **Retention period** section. (In days, months, or years).
- (Optional) Configure filters to include or exclude specific locations or data from having the policy applied.
  See "How to add a Location filter?" on page 237.
  See "How to add a filter?" on page 238.
- Click **Create** to add a policy or click **Update** to save the changes.

The policy is displayed on the **At-Rest WORM policies** page under the storage (Stor) for which you have added the policy.

When a policy is configured and enabled it enforces retention periods during which items cannot be deleted or modified.

Add/edit Deletion policies

Before you begin:

Before you implement the Deletion policy, consider the following points:

- **Overview**
  Deletion policy is used to permanently and irreversibly delete specific content from the Stors. However, this policy does not affect:
  - Items under legal hold.
  - Items within the WORM retention period.
  - Items tagged with **Prevent Deletion** behavior.
- **Preview mode (mandatory)**
  You should always run the policy in **Preview** mode to review which all items will be deleted.
  It is recommended that you consult with Cohesity Support before adding any policy.
- **Policy evaluation**
  The policies operate based on the configured policy evaluation interval within your Cohesity Alta SaaS Protection environment, which is typically set to every 15 minutes by default.

- **Two-step deletion process**
  The deletion process within Cohesity Alta SaaS Protection occurs in two steps. Firstly, references to records are removed, followed by sending delete instructions to the underlying Stors. The periodic maintenance tasks clean up empty folders without any descendants.
- **Post-deletion behavior**
  - Empty folders are cleaned by background maintenance.
  - Data becomes inaccessible immediately after deletion begins.
  - Garbage collection processes clean all copies of the deleted content.
  - Overwriting: Deleted storage blocks are eventually overwritten.

Step-by-step procedure to add/edit a Deletion policy:

1. Access the Administration portal.

   The home page of the Administration portal is displayed.
2. Click **Retention**.
3. On the left, click **Deletion policies**.
4. Do one of the following:
   - To add a new policy, click **New policy**.
   - To update existing policy, click the name of the policy.
5. On the **Create policy** page, do the following:
   - Enter an appropriate name for the policy.
   - From the **Stor** list, select the Stor for which the policy has to be added.
   - Configure the schedule to run the Deletion policy based-on one of the following criteria:
     - **One time**: Runs once as per the policy interval settings, and then its schedule changes to **Never**.
     - **Continuous**: Runs as per the policy interval settings.
     - **Date range**: Lets you specify a **From** and **To** date range to run the policy.
     - **Never**: If you are not ready to run the policy or want to stop the policy from running. The **one time-scheduled policies** is converted to **Never** after its runs.
   - Select any of the required action modes:

  - **Preview**: Lists the items, which can be deleted with this policy.
  - **Production**: Deletes the items in the scope of the policy unless it is protected by legal hold or WORM policy.
- By default, the status of the policy is disabled; it is saved but cannot run. Toggle the **Status** option to enable the policy. As soon as the policy is enabled, it runs as per the schedule that is set in the **Schedule** section.
- (Optional) Configure filters to include or exclude specific locations or data from having the policy applied.
  See "How to add a Location filter?" on page 237.
  See "How to add a filter?" on page 238.
- Click **Create** to add a policy.
  While you editing the policy, the **Update** option is displayed, click it to save the changes.
  The policies are displayed on the **Deletion policies** page, under the storage (Stor) for which you have added the policy.

Related topics:

- See "How to edit the policy evaluation interval?" on page 237.
- See "View deletion history" on page 236.

View deletion history

You can view the data that has been successfully deleted using the Deletion policy. All deletion activity is always audited. Use the following link to view any retention policy action that failed due to an error:

item actions auditing page

To view deletion history

1. Access the Administration portal URL.

   The home page of the Administration portal is displayed.
2. Click **Retention**.
3. On the left, click **Deletion history**.

   You can perform the following actions:

   - View the deleted files with its corresponding deletion date, policy, name of the Stor, and size of the file.
   - Sort the list by clicking the **Sort all items by** icon.

- Export the list to Excel, by clicking the **Export** option.
- Search for the specific data using the **Refined search** option.

To search for the specific data

1. Click **Refine search**.
2. On the **Refine search** page, select the search criteria and click Search.

   The files are displayed on the **Deletion history** page.

How to edit the policy evaluation interval?

The policy evaluation interval is used to define the frequency or schedule at which a policy is enforced on specific items in the storage (Stors).

To edit the policy evaluation interval

1. Open a web browser and access the Administration portal URL. The home page of the Administration portal is displayed.
2. Click **Administration**.
3. On the left, click **Storage**.
4. Click the name of the storage (Stor) for which the policy evaluation interval has to be edited.
5. On the **General** tab, edit the value that is entered in the **Policy evaluation interval in minutes** field.
6. On the top, click **Save**.

   The policy interval is updated.

How to add a Location filter?

The Location filter can be used to include or exclude locations from the defined policy being applied.

- Click **Add a filter**.
- From the **Location** dropdown list, select one of the following options:
  - **includes**: If you select this option and add locations, the policy will be applied to the added locations.
  - **excludes**: If you select this option and add locations, the policy will not be applied to the added locations.
- Click the **Select location** icon.

- On the **Select locations** page, do the following:
  - Expand the required Stor and select the location, select the required CSV file > click **Open** > click **Select**.
  - Click **Export** option to export the list of locations to CSV.
  - Save the exported .csv file to the local computer.
  - Make the required changes, such as if you want to delete any location from the list.
  - Click **Import** to import the locations using CSV file, select the required CSV file > click **Open** > click **Select**.

How to add a filter?

An example to add a filter is described as follows:

- Click **Add a filter**.
- Select the **Last modified** option.
- Set the required value on the calendar that is displayed on the screen.
- Set the required operator, like equal, after, and so on.
- Click **Create**.
- A few operators for the Last modified filter are described as follows:
  - **Before**: The policy is applied to the data which is accessed before the specified date and time.
  - **After**: The policy is applied to the data which is accessed after the specified date and time.
  - **Between**: The policy is applied to the data which is accesses within a specified date and time range.
  - Then select the required retention period from the **Retention period** section as ***1 month***.

    This example retains the data last accessed with the specified date and time. No policy can delete or modify the specified data.

Chapter 24

Perform backups

This chapter includes the following topics:

- Perform on-demand/ad-hoc backup
- Video tutorial for connector troubleshooting
- View backup events
- Viewing backup tasks details

Perform on-demand/ad-hoc backup

An on-demand (ad hoc) backup is performed outside the regular backup schedule.

Before you begin

- Ensure the Microsoft 365 app registrations provisioned for the for Microsoft 365 connectors are in an **Active** state.
- If the assigned apps are not active, the status will display as **Pending app activation**, and backups cannot proceed. Admin consent must be granted for the provisioned apps before running backups.

Perform an on-demand/ad-hoc backup

1. Access the Administration portal.
2. Click **Administration** > **Connectors**.
3. Click the required connector's row.

   To search for the required connector, enter its name in the **Filter by name** field.

   Ensure the connector's status is not **Pending app activation**.

4 Click **Backup now** at the upper left of the page.

5 On the **Backup now** page, do the following:

For the first backup of any connector	For the second backup of the connectors without Deletion/Stubbing policies	For the second backup of the connectors with Deletion/Stubbing policies
The **Backup** option is available on the page. Click this option to initiate the backup. This will initiate a full backup on the source workload.	The **Backup** option is displayed. Click **Backup** to initiate the backup. This will initiate an incremental backup on the source workload.	The following two options are displayed: ■ **New and Changed Items**: Select this for an incremental backup. ■ **All Items**: Selecting this option will run the Deletion/Stubbing policy and perform a full backup. For any subsequent backups you can choose the **New and Changed Items** option for incremental backup.

The backup is initiated. The duration may vary depending on the data size. If necessary, you can cancel the backup using the **Stop Backup** option on the Connector service.

View backup status and data

1 On the **Connectors** page, the connector's status changes to **Initial Running (backup)** for the first backup and **Running** for subsequent backups.

2 The **Last backup count column** reflects the number of items backed up (not applicable for Salesforce connectors).

3 Navigate to the **Content** page and select the Stor linked to the connector. The backed-up data will appear in the left pane. See "Browse backed-up data" on page 245.

For analytics, See "Gain insights into storage utilization " on page 253.

Upon backup completion

- On successful backup completion, the status changes to **Completed**.

- On partial success/failure backup, the status changes to **Completed with Errors**, and registered email addresses receive error or success details.

Related topics:

- See "Connector status" on page 119.
- See "Configure email addresses to get notifications" on page 116.
- See "Manually approve Microsoft 365 apps registration" on page 91.
- See "Approve Microsoft 365 apps using the App Consent Grant utility" on page 92.

Video tutorial for connector troubleshooting

Here is the video tutorial for connector troubleshooting.

http://video.symantec.com/services/player/bcpid292374537001?bckey=AQ~~,AAAABuIiy9k~,I8Bhas-Vwr9zYL9V36WFi86fR_NoePscn&bctid=6362511138112

View backup events

You can use the **Last Backup** filter to view events related to specific backup instances. By default, this filter is applied automatically

Procedure to navigate to backup events:

1. Open a web browser and access the Administration portal URL.

   The home page appears.
2. Click **Administration** > **Connectors**.
3. In the list of connectors, locate the required connector and click anywhere in its row and click **Events**.

Actions you can perform on the Events page:

- **View event details**:
  Click any event. The **Event details** page opens at the left of the screen.
- **Export events to CSV**:
  Click **Export** to download the list of events in CSV format.
- **Filter events**:
  Click the filter icon and select either **Persistent errors** or **All**. You can also filter the list of events based on warning, error, information, and so on.

- **Stop getting specific events (Suppress specific events)**:
  - See "About Event suppression" on page 242.
  - See "Create event suppression rules" on page 242.

About Event suppression

Event suppression is the process of ignoring events that are generated due to a higher-level event or known events. A good example is the mailboxes of the users who have left the organization. The corresponding connector displays events for these mailboxes, as the statuses of the mailboxes are inactive.

Reducing the volume of events is possible by defining event suppression rules. It reduces the number of events that help identify critical events and take action to rectify them.

Create event suppression rules

To create an event suppression rule - method 1

1. Access the Administration portal.

   The home page of the Administration portal is displayed.
2. Click **Administration**.
3. On the left, click **Connectors**.
4. Click the row of the connector, for which you want to create a suppression rule.
5. Click **Events**.
6. Click the row of the event that needs to be suppressed.
7. Hover on that event and click **Suppression events like these** icon.
8. On the **New Connector event suppression rule** page, do the following:

   The connector is displayed in the **Connector** drop-down list.
9. Click **Create**.

   A rule is added. It is displayed on the **Event Suppression rule** page with details such as the connector, the path, and the name of the rule.

To create an event suppression rule - method 2

1. Access the Administration portal.

   The home page of the Administration portal is displayed.
2. Click **Administration**.
3. On the left, click **Connectors**.

4 On the left, click **Event suppression rules**.

5 Click **New suppression rule**.

6 On the **New Connector event suppression rule** page, do the following:

- Select the required connector from the **Connector** drop-down list.
- Enter messages, which you want to suppress.
  You can use wild card.
- Enter exemption in the field.
  You can use wild card.

7 Click **Create**.

A rule is added. It is displayed on the **Event Suppression rule** page with details such as the connector, the path, and the name of the rule.

To update location for the event

1 Access the Administration portal URL.

The home page of the Administration portal is displayed.

2 Click **Administration**.

3 On the left, click **Connectors**.

4 On the left, click **Event suppression rules**.

5 Click the rule that is to be updated for the location.

6 Select the **Location Path** check box.

7 Click **Update**.

A rule is added. It is displayed on the **Event Suppression rule** page with details such as the connector, the path, and the name of the rule.

With this rule the specified messages for the selected location is suppressed from the events.

Viewing backup tasks details

To view backup tasks details

1 Access the Administration portal URL.

2 Click **Administration** > **Connectors**.

3. Click within the row of the connector, click the **Tasks** icon.

   The **Tasks** page displays all the tasks that are performed on the selected connector with details such as the time that is taken for backup, size of the data, and number of errors.

4. On the **Tasks** page, you can perform the following actions as required:

To view details of the task:	Click within the row of the task. The **Tasks details** page opens at the left of the screen.
To view error details of the tasks:	Either click within the row of the tasks, click **Error logs**. The **Error logs** page opens at the left of the screen. On the **Error logs** page you can click the filter icon to view either **Persistent Errors** or **All Error** as required.
To filter the tasks:	Click the filter option. By default the **Connector Backup** option is selected. Select the required option.

Chapter 25

View and share backed-up data

This chapter includes the following topics:

- Browse backed-up data
- Share data
- Remove data sharing

Browse backed-up data

To browse the backed-up data

1. Access the Administration portal.
2. Click **Content**.
3. On the **Content** page, select the required Stor.

   The backed-up data is displayed on the page.

Share data

You can share data with other users using the following procedure.

To share data with other users

1. Access the Cohesity Alta SaaS Protection Administration portal.
2. Click **Content**.
3. All Stors are available in the top-left list. Select the required Stor from the list. For example, ***M365 Mailboxes*.**

4. On the right pane, select the items to be shared.
5. From the **Actions** menu, click **Restore** > **Add admin share**.
6. On the **Share with others** page, do the following:
   - Enter the email addresses or names of the users with whom you want to share the data.
   - Select the **Send invitation email** check box.
     A notification email is sent to the added users with the URL of the End-User portal.
   - From the **Access expires** drop-down list, set the expiration date for the shared content.
     It is an optional step.
   - Click **Share**.

Remove data sharing

1. Access the Cohesity Alta SaaS Protection Administration portal.
2. Click **Content**.
3. All Stors are available in the top-left list. Select the required Stor from the list. For example, ***M365 Mailboxes*.**
4. On the **Folder** pane, browse for the required folder.
5. On the right pane, select the items of which admin share you want to remove. Click **...** (That is **More actions** icon) and then click **Manage admin shares**.
6. On the left, click **SaaS**.
7. Click the corresponding action menu and click **Restore**.
8. Browse and select the folder that you want to share.
9. From the **Action** menu, click the **Manage admin shares** option.
10. Click the **Admin shares** tab.

    All the shares are displayed on the page.
11. Select checkboxes of the items that you want to remove and click **Remove**.
12. On the **Remove share** dialog box, click **Remove**.

    The selected shares are removed from the list.

Chapter 26

Analytics

This chapter includes the following topics:

- About analytics
- Analytics page and refresh behavior
- Aggregation buckets
- Gain insights into storage utilization
- Gain insights into storage utilization for Entra ID and Salesforce connectors
- Gain insights into blocked activities, most active users, and more
- Gain insights into data volume (size and item count) on legal hold
- Gain insights into data volume (size and item count) saved in different Enhanced cases
- Gain insights into data volume (size and count) under different policies
- Gain insights into data volume (size and item count) under different Tags
- Gain insights into data volume (size and item count) under different Tags behaviors
- Gain insights into storage savings after deduplication and compression
- Gain insights into data ingestion trends

About analytics

The Analytics feature in Cohesity Alta SaaS Protection provides visibility into the size and item count of backed-up data. Cohesity Alta SaaS Protection enables you

to view this information at each stage of the data lifecycle—from ingestion to optimization—helping you understand how data evolves through processing.

- **Reported by source workload**
  It is the size and item count reported by the source workload (for example, Exchange, SharePoint, and so on).
- **Post-backup (Stors)**
  Cohesity Alta SaaS Protection adds additional metadata and also modifies the data format when storing the backed-up data to its Stors as follows:

Workload	Format changes
Exchange Online	■ Converts emails to MIME format. ■ MIME formatting may increase size by ~30% for emails with attachments due to Base64 encoding. ■ For mostly text emails, the size may decrease, but no email content is lost. ■ Reports are based on the MIME-calculated size.
SharePoint Online	■ Generates an additional blob per item version to store metadata. ■ Blob size: 1–4 KiB per item version. ■ List items (for example, Employee Onboarding, Surveys) show only list item size as reported by SharePoint. ■ The size on **Analytics** > **Storage** includes list **item size** + **attachments**.
Teams chat	Includes additional metadata for teams, channels, and chats in the Analytics size report.

- **After deduplication and compression**
  It is the optimized size and item count after deduplication and compression are applied to the stored data to minimize storage usage.

Procedure to view the size and item count reported by the source workload for an individual connector:

1. On the home page, click **Backup**.
2. Click **Connectors**.
3. Click within the row of the required connector.
4. Click **Tasks**.
5. The **Task details** page is opened. The size is displayed under the **Total uploaded** field.

Procedure to view the size and item count post-backup:

These details are displayed on the **Analytics** page as well as on the **System** page.

>> For Analytics page:

1. Open a web browser and access the Administration portal URL.

   The home page of the Administration portal is displayed.

2. On the home page, click **Analytics**.
3. On the left, click **Storage**.

   The size is displayed on the **Total size** section.

OR

1. On the home page, click **Administration**.
2. On the left, click **Storage**.
3. On the **General** tab, click the Stor for which you want to view the details.
4. Click the **Analytics** tab.

>> For System page:

1. On the home page, click **System**.
2. On the left, click **Storage**.
3. The size is displayed in the **Original size** section.

Procedure to view the size and item count after deduplication and compression:

1. On the home page, click **System**.
2. On the left, click **Storage**.

   The compressed size and storage savings are displayed in the **Storage savings** section.

Related topics:

- See "Analytics page and refresh behavior" on page 249.

Analytics page and refresh behavior

The Analytics page in Cohesity Alta SaaS Protection provides key insights into the size and item count of your backed-up data. You can use this page to view:

- Size and item count of backed-up data
- Blocked activities

- User role assignments
- Legal hold data
- User trends (for example, number of users added over time)

These insights are organized into tabs on the left side of the **Analytics** page. Additional tabs may appear based on your license—for example, Salesforce and Entra ID tabs for applicable SKUs.

Policy evaluation types:

The statistics shown on the **Analytics** page are updated based on policy evaluations. This includes both system-defined policies and custom policies created by administrator.

Table 26-1

Policy evaluation type	When it happens
Full evaluation	Occurs in the following scenarios: ■ The first week of each month. ■ Tenant upgrade (if applicable). ■ Policy configuration change that requires reevaluation. To known when the full evaluation is occurred, navigate to **Administration** > **Storage** > *Stor* > **General** > **Policy evaluation** section. View the timestamp of the **Policy full evaluation last ran** field.
Incremental evaluation	Occurs at a configurable interval. Set the **Policy evaluation interval (in minutes)** under **Administration** > **Storage** > ***Stor Name*** > **General**. This interval determines how frequently incremental policy execution occurs.

Refresh behavior:

If data is deleted by a Deletion policy, the size shown for that Stor may not reflect the change until the next full evaluation occurs. Always check the refresh time displayed in each section or chart. When multiple Stors or scopes are selected, the most recent update time is displayed.

Aggregation buckets

By default, Cohesity Alta SaaS Protection organizes data into aggregation buckets for efficient data management. The buckets are created based on the item's size, last accessed timestamp, and last modified timestamp.

Aggregation bucket for size:

A size bucket is created to categorize data into size ranges, such as:

- Less than 1 KiB
- 1 KiB – 10 KiB
- 10 KiB – 100 KiB
- Up to greater than 100 GiB

This categorization helps monitor storage consumption by bucket. For example, you can view how much storage is occupied by items within the 1 KiB – 10-KiB range compared to those smaller than 1 KiB.

To analyze data by size, click the **Size** option and you can switch between the **Item size** and **Item count** option based on your requirement.

Aggregation bucket for last accessed and last modified:

Data is grouped by the year it was last accessed or modified. This allows tracking of storage consumption per year based on last accessed or modified timestamp.

Manage aggregation buckets templates:

Use the following procedures to view, edit, add, and load Aggregation Buckets.

To view these Aggregation Buckets Templates, do the following:

1. Open the Administration portal.
2. Navigate to **Administration**. On the left, click **General**.
3. Select the **Aggregation Buckets Template** tab.
4. Click **View Aggregation Buckets Templates**.

   Click a template to see its predefined values.

To edit Aggregation Buckets Templates, do the following:

1. Open the Administration portal.
2. Navigate to **Administration**. On the left, click **Storage**.
3. Click the Stor of which Aggregation Buckets Templates you want to edit.
4. Click the **Metadata** tab.

5 Click the edit icon of the field of which values you want to edit.

For example, **Size**.

6 Click the bucket name that you want to change. Modify the values and click **Update**.

To add a new bucket, do the following:

1 Open the Administration portal.

2 Navigate to **Administration**. On the left, click **Storage**.

3 Click the Stor for which you want to add a new Aggregation Bucket Template.

4 Click the **Metadata** tab.

5 Click **+ Add Buckets**.

6 On the **Aggregation buckets page,** enter a label for the bucket, specify the values/range, and click **Add**.

The added bucket is now listed.

7 Click **Save**.

8 Click **More** > **Save as template**.

9 On the **Save as template** page, enter details and click **Save**.

The new bucket is saved in the template. You can navigate to the **General settings** and view the templates.

The buckets you create and customize are replaced with the standard default templates upon a tenant upgrade. After the upgrade, only the default templates are visible. To restore your custom templates, you need to manually load them.

To add load a custom template after tenant upgrade, do the following:

1 Open the Administration portal.

2 Navigate to **Administration**. On the left, click **Storage**.

3 Click the Stor.

4 Click the **Metadata** tab.

5 Click **More** > **Load template**.

6 From the **Load template** page, select the template and click **Load template**.

7 Click **Save**.

You can navigate to the **General settings** and view the templates.

Gain insights into storage utilization

The **Storage** tab on the **Analytics** page, provides detailed insights into the size and item count of the backup-up data. These insights help administrators monitor storage consumption.

The size displayed on this tab may differ from the size reported by the source workloads. This discrepancy occurs because Cohesity Alta SaaS Protection adds additional metadata and also modifies the data format when storing data. For more information,

See "About analytics " on page 247.

See "Analytics page and refresh behavior" on page 249.

Common features across charts:

The following features are common across most of the charts on this tab:

- **Item size** and **Item count** toggle option: Each chart includes an option to switch views between size-based and item count-based details.
- **Zoom in and out**: You can interact with line and bar charts by clicking within the chart and using the mouse scroll wheel to zoom in and out.
- **Details on hover**: You can hover over any pie chart to view statistics as percentages and verify the timestamp for the last update.
- **Scope/Stor selection**: To get the details, select the required option from the **Scope** dropdown list. You can either select the **All content** option to view details for all Stors or select specific Stors to view details related only to those Stors.

Statistics on the backed-up data:

The following details are displayed for the selected Stors:

Table 26-2

Sections/charts	Description
Total size	The size and item count of data stored to Cohesity Alta SaaS Protection Stors, including the size from source workloads, added metadata, and format changes. This reflects the size and item count before deduplication and compression.
Full text indexed	Displays the size and item count of the data that has been fully text-indexed.

Table 26-2 *(continued)*

Sections/charts	Description
On legal hold	Displays the size and item count of the data on legal hold.
Tagged	Displays the size and item count of the data tagged with the Tags created by you. See "About the Tagging policy" on page 359.
Data volume by size chart	A bar chart represents the size of the data.
Data volume by item version chart	A bar chart represents the item count of the data. It includes all version of each item.
Breakdown by content type chart	A pie chart that represents the storage consumption based on content type category such as images, documents, email, and so on.
Storage tiering chart	A pie chart that represents the data distribution across Hot, Cold, Cool, and Archive tiers.
History chart	A line chart that represents the trend of data ingestion over time.
Distribution chart	A bar chart that represents a summary of how stored data is distributed across configurable buckets for size, last accessed, and last modified statistics. See "Aggregation buckets" on page 251.

Gain insights into storage utilization for Entra ID and Salesforce connectors

Access the Administration portal. On the home page, click **Analytics**.

On the **Analytics** page, on the left, the following tabs are displayed:

Table 26-3

Tabs	Description
Entra ID	This page displays the data utilization statistics that includes object counts, data types, and data size within the Stor. You can select the required Stor from the respective dropdown lists and view its details as follows: ■ **Objects and records** section: The total size of the data and the count of restore points and objects of the selected structured Stor. You can also view the total number of records and how they are categorized among users, groups, Application Registrations, Enterprise Applications, and relations. ■ **Files** section: The total size and the number of files (profile photos) stored on the selected unstructured Stor.
Salesforce	This page provides information on the data utilization statistics that includes object counts, data types, and data size within the Stor. You can choose the required Stor from the respective dropdown lists and view its details as follows: ■ **Objects and records** section: This section displays the total size of the data and the count of restore points, objects, and records for the selected structured Stor. ■ **Files, attachments, and metadata** section: This section displays the total size of the data and the count of metadata, files, and attachments for the selected unstructured Stor. ■ **Metadata** section: You can select the required connector from the dropdown list and view the count of metadata restore points, metadata types, and metadata components for the selected connector.

Gain insights into blocked activities, most active users, and more

The following features are common across the charts on this tab:

- **Item size** and **Item count** options: Each chart includes an option to switch views between size-based and item count-based details.
- **Zoom in and out**: You can interact with line and bar charts by clicking within the chart and using the mouse scroll wheel to zoom in and out.
- **Details on hover**: You can hover over any pie chart to view statistics as percentages and verify the timestamp for the last update.

To get the details, select the required option from the **Scope** dropdown list. You can either select the **All content** option to view details for all Stors or select specific Stor(s) to view details related only to those Stor(s).

The following details are displayed for the selected Stor(s):

Table 26-4

Sections/Charts	Description
Recent blocked activities	Displays the count of the activities blocked for the selected Stors. These statistics are presented for the previous day, the last 7 days, and the last 30 days.
Top 5 blocked activity users (Last 30 days)	Lists the names of users whose activities were blocked that provides insights into security incidents and helps identify patterns in user actions.
Most shared items (weekly) and **Most retrieved items** charts	Display the most frequently shared and retrieved (restored and downloaded) items, respectively, offering insights into data usage patterns.
Role assignment chart	A bar chart that represents the count of users assigned to different roles that help in assisting in role management and ensuring proper access control across the organization.
Activity history chart	A bar chart represents the count of items shared and retrieved (restored or downloaded) on a monthly basis. It includes an option to switch between views to display details on the count of retrieved items and the count of shared items. You can interact with the chart by clicking on it and using the scrolled wheel to zoom in or out. The data can also be exported to Excel using the **Export** option.
Breakdown by tag chart	A pie chart that represents the spread of data among the Tags configured for the selected Stor.

Table 26-4 *(continued)*

Sections/Charts	Description
Previous year history chart	A line chart that plots the trend that represents the count of users, groups, disabled users, and shadowed users on the timeline.

Gain insights into data volume (size and item count) on legal hold

The **Discovery** tab provides statistics on the size and item count of the data on legal hold.

The data is derived from the Legal hold tag behavior policy.

See "About the Tagging policy" on page 359.

See "Add Discovery cases" on page 355.

Common features across charts:

The following features are common across most of the charts on this tab:

- **Item size** and **Item count** toggle option: Each chart includes an option to switch views between size-based and item count-based details.
- **Zoom in and out**: You can interact with line and bar charts by clicking within the chart and using the mouse scroll wheel to zoom in and out.
- **Details on hover**: You can hover over any pie chart to view statistics as percentages and verify the timestamp for the last update.
- **Scope/Stor selection**: To get the details, select the required option from the **Scope** dropdown list. You can either select the **All content** option to view details for all Stors or select specific Stors to view details related only to those Stors.

Statistics on the legal hold:

The following details are displayed for the selected Stors:

Table 26-5

Charts	Description
Amount of data on legal hold by Stor chart	A bar chart represents the volume of the data (size and item count).

Table 26-5 *(continued)*

Charts	Description
Amount of data on legal hold by Case chart	A pie chart represents the volume of the data (size and item count) on legal hold in different Cases.
Amount of data on legal hold by content type chart	A pie chart represents the volume of the data (size and item count) on legal hold, categorized by content type, such as images, documents, and so on.
Legal hold history chart	A line chart represents the trend of data being placed on legal hold over time.
Distribution chart	A bar chart that represents a summary of how stored data is distributed across configurable buckets for size, last accessed, and last modified statistics. See "Aggregation buckets" on page 251.

Gain insights into data volume (size and item count) saved in different Enhanced cases

When an Enhanced Discovery case is created and executed for a search, it collects data based on its search criteria, and the search results are saved in that Enhanced case. The **Cases** tab provides statistics on the size and item count of the data saved in different Enhanced cases.

See "Add Discovery cases" on page 355.

Common features across charts:

The following features are common across most of the charts on this tab:

- **Item size** and **Item count** toggle option: Each chart includes an option to switch views between size-based and item count-based details.
- **Zoom in and out**: You can interact with line and bar charts by clicking within the chart and using the mouse scroll wheel to zoom in and out.
- **Details on hover**: You can hover over any pie chart to view statistics as percentages and verify the timestamp for the last update.
- **Scope/Stor selection**: To get the details, select the required option from the **Scope** dropdown list. You can either select the **All content** option to view details for all Stors or select specific Stors to view details related only to those Stors.

Statistics on the data under different cases:

The following details are displayed for the legal hold data in the selected Case:

Table 26-6

Charts	Description
Data volume by size chart	A bar that represents the total size of the data saved in the selected Case.
Data volume by item version chart	A bar that represents the item count of the data saved in the selected Case.
Tag coverage by content type chart	A pie chart represents storage consumption by content type (such as images, documents, and emails) saved in the selected Case.
History chart	A line chart that represents data volume saved in the selected Case over time.
Distribution chart	A bar chart that represents a summary of how stored data is distributed across configurable buckets for size, last accessed, and last modified statistics. See "Aggregation buckets" on page 251.

Gain insights into data volume (size and count) under different policies

The **Policies** tab provides statistics on the volume of the data under different policies.

Common features across charts:

The following features are common across most of the charts on this tab:

- **Item size** and **Item count** toggle option: Each chart includes an option to switch views between size-based and item count-based details.
- **Zoom in and out**: You can interact with line and bar charts by clicking within the chart and using the mouse scroll wheel to zoom in and out.
- **Details on hover**: You can hover over any pie chart to view statistics as percentages and verify the timestamp for the last update.
- **Scope/Stor selection**: To get the details, select the required option from the **Scope** dropdown list. You can either select the **All content** option to view details for all Stors or select specific Stors to view details related only to those Stors.

Statistics on the data under different policies:

The following details are displayed for the selected policy:

Table 26-7

Sections/charts	Description
Policy name	Displays the name of the policy selected policy.
Item versions	Displays the count of items under the selected policy.
Total size	Displays the total size of the data under the selected policy.
Storage tiering chart	A pie chart that represents the breakdown of data volume across storage tiers (Cool, Cold, Archive, and Hot) for the data under the selected policy.
Policy coverage by tags chart	A pie chart represents the data volume for each Tag under the selected policy.
Policy coverage by content type chart	A pie chart represents storage consumption by content type (such as images, documents, and emails) for the data under the selected policy.
Distribution chart	A bar chart that represents a summary of how stored data is distributed across configurable buckets for size, last accessed, and last modified statistics. See "Aggregation buckets" on page 251.

Gain insights into data volume (size and item count) under different Tags

The **Tags** tab provides statistics on the volume of the data under different Tags.

See "About the Tagging policy" on page 359.

Common features across charts:

The following features are common across most of the charts on this tab:

- **Item size** and **Item count** toggle option: Each chart includes an option to switch views between size-based and item count-based details.

- **Zoom in and out**: You can interact with line and bar charts by clicking within the chart and using the mouse scroll wheel to zoom in and out.
- **Details on hover**: You can hover over any pie chart to view statistics as percentages and verify the timestamp for the last update.
- **Scope/Stor selection**: To get the details, select the required option from the **Scope** dropdown list. You can either select the **All content** option to view details for all Stors or select specific Stors to view details related only to those Stors.

Statistics on the data under different tags:

The following details are displayed for the selected Tag:

Table 26-8

Charts	Description
Data volume by size chart	A bar that represents the total size of the data under the selected Tag.
Data volume by item version chart	A bar that represents the item count of the data under the selected Tag.
Tag coverage by content type chart	A pie chart represents storage consumption by content type (such as images, documents, and emails) under the selected Tag.
History chart	A line chart that represents data volume under the selected Tag over time.
Distribution chart	A bar chart that represents a summary of how stored data is distributed across configurable buckets for size, last accessed, and last modified statistics. See "Aggregation buckets" on page 251.

Gain insights into data volume (size and item count) under different Tags behaviors

The **Tags behaviors** tab provides statistics on the volume of the data under different Tag behaviors such as Legal hold, Prevent discovery export, Prevent user retrieval, and Prevent deletion.

See "About the Tagging policy" on page 359.

Common features across charts:

The following features are common across most of the charts on this tab:

- **Item size** and **Item count** toggle option: Each chart includes an option to switch views between size-based and item count-based details.
- **Zoom in and out**: You can interact with line and bar charts by clicking within the chart and using the mouse scroll wheel to zoom in and out.
- **Details on hover**: You can hover over any pie chart to view statistics as percentages and verify the timestamp for the last update.
- **Scope/Stor selection**: To get the details, select the required option from the **Scope** dropdown list. You can either select the **All content** option to view details for all Stors or select specific Stors to view details related only to those Stors.

Statistics on data under different Tag behaviors:

The following details are displayed for the data tagged for the selected Tag behavior:

Table 26-9

Charts	Description
Data volume by size chart	A bar that represents the total size of the data under the selected Tag behavior.
Data volume by item version chart	A bar that represents the item count of the data under the selected Tag behaviors.
Tag coverage by content type chart	A pie chart represents storage consumption by content type (such as images, documents, and emails) under the selected Tag behaviors.
History chart	A line chart that represents data volume under the selected Tag behaviors over time.
Distribution chart	A bar chart that represents a summary of how stored data is distributed across configurable buckets for size, last accessed, and last modified statistics. See "Aggregation buckets" on page 251.

Gain insights into storage savings after deduplication and compression

The **Storage** tab on the **System** page provides details on the size of data after compressions and deduplication.

Navigate to the System page:

1. Access Administration portal.
2. On the home page, click **System**.
3. On the left, click **Storage**.

Use the following procedure to navigate:

Common features across charts:

The following features are common across most of the charts on this tab:

- **Item size** and **Item count** toggle option: Each chart includes an option to switch views between size-based and item count-based details.
- **Zoom in and out**: You can interact with line and bar charts by clicking within the chart and using the mouse scroll wheel to zoom in and out.
- **Details on hover**: You can hover over any pie chart to view statistics as percentages and verify the timestamp for the last update.
- **Scope/Stor selection**: To get the details, select the required option from the **Scope** dropdown list. You can either select the **All content** option to view details for all Stors or select specific Stors to view details related only to those Stors.

Statistics on the compressed data:

The following details are displayed for the selected Stors:

Always see the last updated timestamp. If multiple Stors are displayed, the most recent update time is displayed.

Table 26-10

Options/Sections	Description
Original size	Displays the total size of the data, reflecting the raw data stored in blobs without deduplication and compression.
Storage savings	Displays the details about the data size after deduplication and compression, as well as the amount of storage saved. These statistics are updated hourly during storage maintenance jobs.

Table 26-10 *(continued)*

Options/Sections	Description
Stor Usage chart	A bar chart represents the original, post-deduplication, and post-deduplication & compression sizes for each Stor. These statistics are updated hourly during Stor maintenance jobs.
Storage history chart	A line chart that represents the storage usage over time, providing insights into storage utilization. It highlights trends such as growth, stability, or reduction in usage. To analyze storage efficiency and optimization, you can toggle between views like Original size, After deduplication, and After deduplication & compression.

Gain insights into data ingestion trends

The **Ingress flow** tab on the **System** page provides the trends on the amount of data (size and item count) ingested to Cohesity Alta SaaS Protection.

To get the details, select the required option from the **Scope** dropdown list. You can either select the **All content** option to view details for all Stors or select specific Stor(s) to view details related only to those Stor(s).

Navigate to the Ingress flow tab:

1. Access Administration portal.
2. On the home page, click **System**.
3. On the left, click **Ingress flow**.

Always check for the last updated timestamp. If multiple Stors are displayed, the most recent update time is displayed.

Chapter 27

Perform restores using Administration portal

This chapter includes the following topics:

- About restore
- Prerequisites for restore
- Restore Exchange Online mailboxes
- Restore SharePoint/OneDrive/Teams Sites and data
- Restore Teams chat messages and Teams channel conversations
- Restore O365 audit logs
- Restore Box data
- Restore Google Drive data
- Restore Gmail data
- About Salesforce Data, Metadata, and CRM Content restore and Sandbox seeding
- About Entra ID (Azure AD) objects and records restore
- Restore Slack data
- Restore data to File server
- Set default restore point
- Configure Restore all, Restore all versions, Point-in-time, and Specific range restore options

- Configure email addresses for notifications
- Downloading an item

About restore

The backed-up data can be restored to the original or an alternative location in case of loss or damage. You can restore data using the Administration portal, End-User portal, or Export Utility to the following locations:

- Exchange Online
  See "Restore Exchange Online mailboxes" on page 267.
- SharePoint/OneDrive Online
  See "Restore SharePoint/OneDrive/Teams Sites and data" on page 272.
- Teams Chat
  See "Restore Teams chat messages and Teams channel conversations" on page 288.
- Box
  See "Restore Box data" on page 290.
- Google Drive
  See "Restore Google Drive data" on page 292.
- Gmail
  See "Restore Gmail data" on page 294.
- Salesforce organization
  See "About Entra ID (Azure AD) objects and records restore " on page 327.

Prerequisites for restore

Following are the prerequisites to restore the data:

- To initiate the restore using the Administration portal:
  - You must be an authorized user to initiate the restore.
  - The Export service must be installed and configured for your tenant. Also, the Export location for each of the restore types must be configured on the Export service. Impersonation account must me configured from Team chat restore.
  - The logged-in user must have the following authorizations:
    - Access all items

    - API
- To initiate the restore using the End-User portal:
    - You must be an authorized user to initiate the restore.
    - The Export service must be installed and configured for your tenant. Also, the Export location for each of the restore types must be configured on the Export service. Impersonation account must me configured from Team chat restore.
    - The logged-in user must have the following authorizations:
        - Access all items
        - API
        - End-User portal → Export
- To initiate the restore using the Export Utility, the Export Utility must be installed and configured for your tenant.
- Before initiating restores, you should go to the **Analytics** page > **Storage** on the Administration portal to know the volume of data that is to be restored.An accurate representation of the data is available after the All Items Policy is run. For the following workloads, the content size displayed on the **Data volume by size** chart and **System** → **Ingress flow** pages differs from those displayed on **Administration** → **Connectors** (under **Connector Backup Task** Details).
    - Exchange:
      This mismatch is due to difference in sizes as reported by Exchange versus how the data is backed up and stored in Cohesity Alta SaaS Protection. Cohesity Alta SaaS Protection backs up data from Exchange in MIME format. This format can increase the size of emails with attachments by approximately 30% due to Base64 encoding. For text-only emails, sizes may decrease slightly.

Restore Exchange Online mailboxes

With Cohesity Alta SaaS Protection, you can restore the user's entire mailbox, a specific folder within the mailbox, or an individual mailbox item.

Key features:

- Flexible restore
  Restore data back to the original user's mailbox or to another user's mailbox. Restore data to Group or Teams mailboxes.
- Download capability:

You can also download an item to the required location. See "Downloading an item" on page 338.

- Duplicate suppression
  Suppress duplicate items during restore to avoid multiple instances of the same content.

Note: When you export large amounts of data directly into a mailbox, ensure that the amount of data does not exceed any mailbox quotas.

To restore Exchange Online data using the Export utility, refer to the following knowledge base article:

How to use the Export Utility (For Admins) to Restore a Mailbox, Folder, or Messages to Exchange

Procedure to perform the restore of Exchange Online data to the Exchange Online environment:

1. Access the Administration portal.
2. Click **Content**.
3. On the **Content** page, do the following:
   - From the upper-left dropdown list, select the Stor that hold the data that you want to restore.
   - From the dropdown list next to the selected Stor, do any of the following:
     - To display all data in the selected Stor, select **All content**.
     - To view specific data within the Discovery cases, select the required Discovery case.

     The connectors are displayed on the left pane. You can enter the name of the specific connector in the **Filter by name** field to search for a specific connector.
   - On the left pane, select the connector name.
   - On the right pane, do any of the following:
     - To restore the user's entire mailbox, select the check box of the folder displayed.
     - To restore any specific mailbox item, click the folder, click **Active Mailbox** > browse for the required folders. For example, **Inbox** > select the check box of the required folders.
   - Click **Restore**.

4 On the **Restore** page, do the following:

- From the **Restore type** dropdown list, select **Email**.
- From the **Destination** dropdown list, select the restore (export) service that is configured for your tenant.
- Do any of the following applicable to your scenarios:
  - To restore data to the same user's mailbox, do the following:
    - Click **User mailbox**.
      The email address of the user is populated in the **Mailbox email address** field.
  - To restore data to another user's mailbox, do the following:
    - Click **User mailbox**.
    - In the **Mailbox email address** field, enter the user's email address where you want to restore this mailbox data.
  - To restore data to the group or Teams mailbox, do the following:
    - Click **Groups/Teams mailbox**.
    - In the **Mailbox email address** field, enter the email address of the group where you want to restore this item.
- Do any of the following applicable to your scenario:
  - To merge the data into the user's mailbox, enable the **Merge active mailbox** option.
  - To restore data to another location, disable the **Merge active mailbox** option and click **Browse**. On the **Restore** page, select the required target location for restore.
- Configure the following settings as required:
  - **Suppress duplicates (best effort)** check box:
    - If selected: The duplicate items are suppressed from the restore. That is no duplicate items will be restored.
    - If cleared: The duplicate items are restored at the destination.
  - **Only restore regular sent messages** check box:
    - If selected: The supported ItemClasses for restore, if the **Only restore regular sent messages** check box is selected:
      - ipm.note
      - ipm.post

- If cleared: The supported ItemClasses for restore, if the **Only restore regular sent messages** check box is cleared:
  - ipm.distlist
  - (Only the contact groups that were captured as JSON (post 2.9.387) can be restored.)
  - ipm.post
  - ipm.contact
  - ipm.stickynote
  - ipm.task
  - ipm.appointment
  - ipm.skypeteams.message
  - ipm.appointment.microsoft.onlinebooking
    (Limited support. Items get restored as Appointments and not as Bookings.)
  - ipm.schedule.meeting.resp.pos
  - ipm.schedule.meeting.resp.neg
  - ipm.schedule.meeting.resp.tent
  - ipm.schedule.meeting.request
  - ipm.schedule.meeting.canceled
  - ipm.schedule.meeting.notification.forward
  - ipm.note.groupmailbox.welcomeemail
  - ipm.note.enterprisevault.shortcut
  - IPM.Note.SMIME.MultipartSigned

  Unsupported Item Classes

  The restore is not supported for the following ItemClasses in regular folders, even if the **Restore regular sent messages** check box is selected:
  - ipm.appointment
  - ipm.contact
  - ipm.distlist
  - ipm.task

However, if you want to restore the ItemClasses not listed in the supported list, you can initiate the restore using Export utility and clear the **Suppress Unsupported Item Classes** check box.

Important: Clearing **Suppress Unsupported Item Classes** check box option may result in an unexpected behavior for restoring a few unsupported ItemClasses.

- **Overwrite items** checkbox:
  - If selected: The items already at the destination are replaced with the copy in the backup.
  - If cleared: The items already at the destination are **not** replaced with the copy in the backup. Only the changes are merged.

    The following restore behavior is observed for the Exchange contacts (with or without Name) and tasks (with or without Name):

Overwrite item check box	Same item available at destination	Result
Selected	Yes	A duplicate item is created at the destination with a different unique ID.
Selected	No	The item from the backup is restored on the destination with a unique ID.
Not selected	Yes	No duplicate entry is created.
Not selected	No	The item from the backup is restored on the destination with a unique ID.

- Do any of the following:
  - To restore all items in the selected backup location, click **Restore all**.
  - To restore the items from a specific point in time within the selected backup location, click **Point-in-time** and then set the date, time, and time zone.
  - To restore the items that are backed up within a specific range, click **Specific Range** and specify criteria such as the **last 7 days**, **last 7 hours**, and so on.
- Enter the email addresses of the users to send a notification on restore completion. Use a semicolon to add multiple email addresses. After all the configurations are completed, click **Restore**.

- Click **Restore**.

5 Navigate to the destination to confirm that the restore is completed successfully.

You can go to the See "About Restore dashboard" on page 340. to see the status of the restore.

Restore SharePoint/OneDrive/Teams Sites and data

With Cohesity Alta SaaS Protection, you can restore various components, including site collections, sub-sites, lists, folders, items, and different versions of items. These components can be restored to either the original location or an alternative location.

See "Supported and unsupported SharePoint Objects, Properties, Settings, and Types for backup and restore" on page 144.

Key features:

- Customizations restore:
  Cohesity Alta SaaS Protection restores customizations made within site collections, sub-sites, list settings, columns, and content types, ensuring that your unique configurations are preserved.
- Permissions restore:
  Permissions associated with the restored components are also reinstated, maintaining access controls and security settings.
- Auto-creation of structure:
  If a sub-site or list is missing at the destination for the restore, the structure of the missing sub-site or list will be created automatically, allowing data to be restored within it.
- Site collection restore:
  You can restore an entire site collection to a new URL if needed, which is particularly useful for migrating or recovering data to a different location.
- Download option:
  Additionally, you can download the items to the required location for easy access and management. See "Downloading an item" on page 338.

Recovery process:

When you start the recovery process for a specific backup, the item you selected and the associated child objects, including their configurations and metadata, are restored.

- If the objects being restored, such as sites, sub-sites, lists, and files, are not currently available, Cohesity Alta SaaS Protection generates them again during restore.
- If sites, sub-sites, lists, and files, are not available, they are generated during restore.
- To determine the existence of these objects, their names are verified. For example, the names of sites, sub-sites, lists, and files are matched to see if they exist. Site collections are verified for their existence using the site collection URL.

Restore behavior based on the component selected for restore and the restore location:

The following table outlines the restore behavior for each restore location and its corresponding backup component.

Handling errors during the restore of Site Collection, Sites, and List

The restore process for Site Collections, Sites, and Lists is designed to proceed even if an error occurs. Therefore, you should continue with the restore process even if an error is occurred while restore.

Table 27-1 Supported restore locations

Backup component	Supported restore locations
Folders/Items	■ It can be the same or a different site collection. ■ If an existing parent list at the destination is selected, the columns are merged into the destination list, and the selected items are restored. ■ If a parent list is absent at the destination, the parent site/sub-site must be selected for the restore to recreate the parent list. Then the selected items are restored. ■ If a folder is selected, the item gets restored under that folder.
List	■ It can be the same or a different site collection. ■ If an existing list at the destination is selected, the export merges the columns into the destination list. ■ If a list is not available at the destination, the parent site/sub-site needs to be selected, and the list is recreated.

Table 27-1 Supported restore locations *(continued)*

Backup component	Supported restore locations
Sub-site	■ It can be the same or a different site collection. ■ The parent site/sub-site needs to be selected at the destination. The restore process creates a new sub-site if there is no child sub-site with the same name; otherwise, it merges with the existing sub-site. ■ A sub-site from a source can only be restored as a sub-site of the destination selection.
Site Collection	Site Collection availability: ■ The site collection can be restored to the same or a different site collection. ■ If the site collection is not available at the specified URL, it will be recreated from scratch. Restore limitations: ■ Site collections cannot be restored as sub-sites of other destination sites. ■ A site with the same URL should not be present in the recycle bin before initiating the restore. Restore failures: ■ If the restore process fails, you can recover the site collection from the recycle bin, delete it, and then attempt the restore again. Administration portal restores: ■ Site creation and updates to certain site-level properties are only supported through the Administration portal. End-User portal restores: ■ Restores performed through the End-User portal can create sub-sites and lists within a site.

Restrictions for SharePoint Online restore:

The restrictions of restore the SharePoint Online data and sites are described in the following table.

Table 27-2

Restrictions of restore	Description
The parent site availability requirement.	If you select an individual item, folder, list, or sub-site for restore from a backup, the destination parent site collection and sub-site must be available. To restore an individual item, folder, list, or sub-site from a backup, you must ensure that the destination parent site collection and sub-site are already available.
The template type matching requirement.	To initiate the restore process for an object and its child objects, the source and the destination template types for lists, sub-sites, or site collections must match. For sites or sub-sites, you have the option to selectively choose individual child objects for restore.
The System lists restoration.	To recreate system lists from scratch, SharePoint restores site collections or sub-sites. If you need to restore a missing system list individually, it should already exist at the destination.
The column matching requirement.	To restore a list or site, the destination list or site must not have a column with the same ID or name but a different column type.
The Teams Wiki lists creation requirements.	To automatically recreate missing Teams Wiki lists, you must manually create a blank Teams Wiki list within Teams, and then restore the data to it.
The Role assignment behavior.	To assign permissions to existing roles for existing Microsoft Infra ID users and groups or SharePoint groups, when restoring role assignments at a destination other than the site level.
The existing list or site title.	To prevent a change in the title of a list or site that already exists at the destination.

Procedure to restore SharePoint/OneDrive/Teams Sites and data:

1. Access the Administration portal.
2. On the left, click **Content**.
3. On the **Content** page, do the following:
   - From the upper-left dropdown list, select the Stor that hold the data that you want to restore.

- From the dropdown list next to the selected Stor, do any of the following:
  - To display all data in the selected Stor, select **All content**.
  - To view specific data within the Discovery cases, select the required Discovery case.

  The names of the connectors are displayed on the left pane. You can enter the name of a connector in the **Filter by name** field to search for a specific connector.
- On the left pane, click the connector.
- On the right pane, do any of the following:

If you select...	Restore behavior
Site collection	A site collection along with any customizations and its child items is restored. ■ **Destination options** The site collection can be restored to the same or a different site collection. ■ **Auto-creation** If the site collection is not available at the specified URL, it will be recreated from scratch. ■ **Restore limitations** Site collections cannot be restored as sub-sites of other destination sites. A site collection with the same URL should not be present in the Recycle bin before initiating the restore. ■ **Restore failures** If the restore process fails, recover the site collection from the Recycle bin, delete it, and then attempt the restore again. ■ **Restores through the Administration portal:** Site creation and updates to a few site-level properties are only supported through the Administration portal. ■ **Restores through the End-User portal** Restores performed through the End-User portal can create sub-sites and lists within a site.

If you select...	Restore behavior
Sub-site	A sub-site, along with all customizations and nested objects, can be fully restored. ■ **Destination options** The sub-site can be restored to the same or a different site collection. The parent site or sub-site needs to be selected at the destination. ■ **Auto-creation** If there is no existing sub-site with the same name at the destination, the restore process will create a new sub-site. If a sub-site with the same name already exists, the restored sub-site will merge with the existing one. ■ **Restore limitations** A sub-site from the source can only be restored as a sub-site of the destination selection. Sub-sites cannot be restored as independent site collections.
List	A List along with its customizations and child objects is restored. ■ **Destination options** A list, along with its customizations and child objects, can be restored to the same or a different site collection. If an existing list at the destination is selected, the restore process merges the columns into the destination list. ■ **Auto-creation** If a list is not available at the destination, the parent site or sub-site needs to be selected, and the list will be recreated.
Folder or item	A specific folder or item, including its versions and associated metadata, can be restored to the same or a different site collection. ■ **Destination option** If an existing parent list is selected at the destination, the columns are merged into the destination list, and the selected items are restored. ■ **Auto-creation** If the parent list is absent at the destination, the parent site or sub-site must be selected to recreate the parent list. After the list is recreated, the selected items are restored. If a folder is selected at the destination, the item is restored under that folder.

- Click **Restore**.

4 On the **Restore** page, do the following:

- From the **Restore type** dropdown list, select **SharePoint/OneDrive**.
- From the **Destination** dropdown list, select the Export service that is configured for your tenant.

  For more details, contact Cohesity Support.

  The destination site is populated in the **Site collection URL** field based on the item you selected for restore. Alternatively, you can enter the required URL if you want to restore it to an alternate location.

  Important: To perform a restore using the End-User portal, the end user must be the Primary Admin of the site selected as the destination site for the restore.

  For a successful restore of SharePoint/OneDrive items to their original source location, the web templates for both the source and destination must be the same.
- Click **Browse** and then select the location for restore.
- Configure the following SharePoint settings:

Settings	Description
Restore all versions	This option determines which versions of items are restored from the backup. ■ If selected: All versions of items are restored. ■ If cleared: Only the latest version of items is restored. For example, if you have a library in SharePoint Online that contains a file called *example.docx*. Over time, the user has made several changes to the file, and each change has created a new version. The version history of the file will look like this: Version *1: Initial upload, version 2: Edited by John, version 3: Edited by Jane, and version 4.* You performed a backup of the document library. When you restore the document library from the backup and select this check box, all four versions of *example.docx* will be restored: *version 1, version 2, version 3, and version 4*. If you clear this check box, only the latest version that is version 4 will be restored.

Settings	Description
Reset the 'last modified time' of restored files to the time of restore.	Selecting this check box will reset the 'last modified time' of the last restored version of files to the time of restore. Note that this option is only supported for Document and Page libraries. This change will affect policies based on the 'last modified time' configured in the connector. For example, if this check box is selected and a policy is in place to stub files based on the 'last modified date', the 'last modified time' of restored files will be updated to the restore time. This may result in delays in stubbing these files. If you choose not to select this check box, the 'last modified date' will remain unchanged and reflect the backed-up content, preventing delays in stubbing the files.
Overwrite settings, columns, content types for site collections, sites, and lists	This option determines how settings, columns, and content types are restored. ■ If selected: The restore operation overwrites the existing settings, columns, and content types for an existing site or list with those from the backup. ■ If cleared: The restore operation only restores missing settings, columns, and content types without affecting the existing ones. Example: Suppose you have a SharePoint Online site collection with a custom list named *Project Tasks*. Over time, you have added custom columns like *Priority* and *Status*, and you have also created a custom content type called *Project Milestone*. You performed a backup of the site collection. If you restore the site collection and select this check box, the existing custom columns (*Priority* and *Status*) and content types (*Project Milestone*) in the *Project Tasks* list will be overwritten with the versions from the backup. If you clear this check box, only any missing columns or content types will be restored. The existing *Priority* and *Status* columns, as well as the *Project Milestone* content type, will remain unchanged. By default, this check box is not selected.

Settings	Description

Restore permissions	This option determines whether permissions should be restored during the restoration process.
	■ If selected:
	  ■ Permissions are restored only on SharePoint/OneDrive sites, lists, folders, and the items that are newly created during the restore process.
	  ■ Role definitions and site administrators are restored for the root site if it is created during the restore.
	  ■ SharePoint Groups are restored on any sites and sub-sites that are created during the restore process.
	  ■ Role assignments are restored for sites, sub-sites, lists, folders, and items, except for stubs.
	■ If cleared:
	  ■ Permissions are not restored.
	  ■ All objects inherit permissions from their parent.
	  ■ Site administrators are not restored.
	  ■ The site is created with default permission objects.
	By default, this check box is not selected.

Suppress 'Removed from source' content	This option determines whether to restore the content that is removed from the source. ■ If selected: Content that was deleted from the source will not be restored. This setting is enabled by default. If you need to change this configuration, contact the Cohesity Support team. If any data gets deleted from the source SharePoint, after backup, it gets marked as 'Removed from the source' at the next backup. However, during the restore, the marked data can cause some issues. Hence, you can select this check box to skip the restore of such data.

Settings	Description
Exclude Destination System Lists	This option determines whether system lists should be excluded from the restore process. When restoring system lists, like the Master page, theme gallery, and taxonomy hidden lists, and so on, an Access denied error can occur if the destination site requires the Add and Customize Pages permission. ■ If selected: Items from hidden lists or catalogs (except the Teams wiki list) are excluded from the restore operation. Any skipped items are recorded in the diagnostic logs. If a system list or a folder within a system list is chosen as the destination and this check box is selected, the restore operation will fail with an error, indicating that restoration to the selected system list is not allowed. ■ If cleared: The system lists, such as the Master page gallery and theme gallery, will be included in the restore operation.
Restore only stubbed items	This option determines whether only stubbed items should be restored during the restore process. ■ If selected: Only the items that are stubbed are restored. No site/list/folder, settings or metadata will be restored. **Note:** Stubbed items are placeholders for the original content that has been offloaded or archived. The stubbed item must be available at the original location during the restore. **Stub restore behavior** When a stub is rehydrated to restore, the name and permission of the original file are preserved. It differs from cases where a missing document is restored or replaced with permission restoration, where sharing links are neither retained nor restored.

Settings	Description
Overwrite items	If you choose the **Overwrite items** check box, you need to select one of the following restore behaviors: ■ **Recycle existing items before restoring**: This option removes the existing items and replaces them with a file from the backup. ■ **Restore to existing item (recycle existing versions)**: This option retains the existing items. File versions restored from the backup copy are maintained. ■ **Restore to existing item (keep existing versions)**: This option retains the existing items. Both file versions at the destination and those restored from the backup copy are maintained.
Restore all, Point-in-time, Specific range	See "Configure Restore all, Restore all versions, Point-in-time, and Specific range restore options" on page 337.
Send notification to	Enter the email addresses of the users to send a notification on restore completion. Use a semicolon to add multiple email addresses. After all the configurations are completed, click **Restore**.

5 Navigate to the destination location to confirm that the restore has happened successfully.

You can go to the **Restore dashboard** to see the status of the restore.

See "About Restore dashboard" on page 340.

Important: If an error occurs while restoring the settings of a Site, SubSite, or List, the restore job does not fail; it will log the error and continue to restore the remaining items.

Restore of OneDrive, Microsoft 365 Group, and Microsoft Teams sites

Recovery for OneDrive, Microsoft 365 Group, and Microsoft Teams sites is a two-step process as follows:

- User/Group/Team Creation: The first step requires manual creation by the user of the OneDrive account, Microsoft 365 Group, or Microsoft Teams. This step involves setting up the user, group, or Team.
- Data restore using SharePoint: Data can be restored to the respective sites using SharePoint restores.

To recover data for Microsoft Teams Sites:

- Create a New Destination Team: Create a new Team at the targeted location.
- Create Channels for the Team: Set up channels within the Team as needed.
- Add Users to the Team: Populate the Team with users who should have access to the data.
- Add Additional Resources: Include other necessary resources such as wikis, planners, customizations, and more to the Team.
- SharePoint Restore Process: Use the SharePoint restore process to recover SharePoint data and restore it to the top-level site that was created for the Team from the backup.
- Repeat for Teams Private Channel Sites: If there are private channel sites within the Team, repeat the process to restore data.

Permission objects are created by the restore process only on sites it creates. SharePoint Groups and Role definitions are not restored at the top-level site for OneDrive and Teams sites. Any unique Role Assignments using those Groups and Role definitions are also not restored.

If a list or site already exists at the destination, its title does not change during the restore process.

Restore limitations for SharePoint Online

The limitations for the restore of SharePoint sites and data restore are described in the following table:

Table 27-3

Limitations	Description
Point-in-time restore of metadata.	The point-in-time restore of metadata for site collections, sub-sites, and lists is not supported because it maintains a single copy of their metadata. Exception: This limitation does not apply to individual items.
Point-in-time restore of permissions.	Point-in-time restores of permissions are not supported as it maintains a single copy of permissions.

Table 27-3 *(continued)*

Limitations	Description
Restore of site and site collection settings.	Backup and restore of the following site and site collection settings are not supported: ■ Site collection and Site search settings. ■ Sort order within Regional settings. ■ Workflow settings under Site Administration. The language settings are restored only for the following scenarios: ■ If the Site collection is created during the restore. ■ If the Site collection already exists, at least one language is selected under the **Language settings** > **Available languages** section in the Site settings.
Restore of the order in Quick Launch links.	When a site or sub-site is restored to a new location, the order of links in the **Look and Feel** > **Quick Launch** settings is not retained.
Recreation of Visio sites.	Recreating Visio sites from scratch is not supported.
Restore of missing SharePoint Group descriptions.	SharePoint Group descriptions are not restored when a site collection is restored to a new location.
Restore of the Managed metadata and Lookup Columns.	When a list is recreated, **Managed Metadata and Lookup** column types are skipped, and the data for these columns is not restored. If the original column exists in the destination list with identical customization and the same name as in the backup, the data for these columns can be restored to the list.
Backup and restore of the List view.	List views are not included in the backup and restore process. When lists are recreated, the columns that are displayed in the default view at the time of backup are retained.
Restore of the Column in List.	The order of columns is not maintained when a list is restored from scratch, especially for calculated columns.

Table 27-3 *(continued)*

Limitations	Description
Restore of User References in List items.	When restoring list items with fields containing user references, the SharePoint app is displayed instead of the original user. It occurs with fields like a document or item's **Author/Editor** field, the **Reply By** field of a discussion item, and so on. The following scenarios may occur: ■ If the original user is not available in the directory. ■ If the user is external, sharing is disabled at the restore destination site.
Backup and restore of the advanced settings of the Lists.	Backup and restore of the following advanced settings of Lists are not supported: ■ Opening Documents in the Browser ■ Dialogs ■ Order of Survey questions
Restore of Location-Related Columns.	All location-related columns (for example, state, city) are created during restore.
Restore of the Access permissions.	In the case of SharePoint and OneDrive, you can restore the direct-access permissions that are assigned to users but not the link-based access permissions. The restore of link-based access is not supported.
Restore of Wiki and Web Part pages.	Wiki and Web Part pages are not supported for backup and restore. If they do not exist at the destination, they are restored as empty pages. Also, restoring the Web Parts of the Pages is not supported.
Restore of Home.aspx.	Restore of Home.aspx is not supported.
Restore of comment's versions.	Backup and restore of the versions of comments and approval comments in the document is not supported.
Restore of Workflow activation.	The restore process does not turn off workflows during restore, which means the restore can initiate unintended workflows.
Restore of the redirected Lists, Folders, or items.	For the redirected lists, folders, or items being restored to another site, SharePoint default group roles are not applied to any SharePoint object.
Restore of the Discussion Board Reply.	On the Discussion board, when a response to a message or reply is restored, it appears as a reply to the original discussion thread.

Table 27-3 *(continued)*

Limitations	Description
Restore of the unchanged OneNote files.	Any new OneNote file that is not backed up earlier remains unchanged and is not removed, even if the **Overwrite items** option is selected.
Tenant-to-Tenant Restoration.	An Access denied message is displayed when restoring a site collection to a different tenant's location. To resolve this error, disable the **DenyAddAndCustomizePages** permission on SharePoint Online for the site collections. This allows the necessary customization and configuration of the restored site collection in the new tenant's environment.
Restore of the Web Part page access.	When restoring a Web Part Page to a destination location, an **Access denied** message can be displayed. To resolve this error, disable the **DenyAddAndCustomizePages** permission on SharePoint Online for the site collection.
Restore of the duplicate items in site collection.	When restoring a site collection to another site collection, duplicate items are created at the destination due to metadata mismatches with default items in the **Reusable Content** list.
Duplicate Values error.	When restoring a list item, the error can be displayed due to the Enforce unique values setting from one of the list columns. To restore the item manually download the item to your local computer.
Sub-site and list creation errors.	Sub-site and list creation can fail with errors. It may refer to a non-existent file or folder. It may also refer to a valid file or folder that is not on the current web. When it happens, the location in which the error has occurred needs to be restored again.
Identically Named Lists and sub-sites conflicts.	Restoring the sites that have more than one list or sub-site with the same title is not supported. During the restore operation, all the identically named lists and sub-sites are placed onto a single list and sub-site at the destination.
Restore of the reserved Column Names.	SharePoint Online reserves specific column names for its internal use. The restore process may fail if the reserved names are used as custom column names in a list.
Restore of the Default Site page.	When restoring a default site page over an existing site, the first published version is created.

Table 27-3 *(continued)*

Limitations	Description
Restore of the Image Column.	The list is restored when you restore an individual list with an image column to an alternate location. The images within the list are not restored because they have a dependency on the Site Assets document library. When you perform a complete site restore to an alternate location, the image columns within the sites are restored as expected.
SharePoint index.	The backup and restore of the SharePoint index is not supported. When restoring items the SharePoint indexer will index the restored items in the background.
Information Protection Management setting enabled items	The files with the Information Rights Management (IRM) setting enabled should be restored to the same library or list at the time of the backup. The IRM setting of the library should be unchanged, otherwise the file cannot be opened after its restore. **Note:** The SharePoint files for which the IRM setting is enabled at the time of backup cannot be opened after their download.
Restore of Sensitivity labeled items.	For the items with Sensitivity labels configured for encryption, only restores from scratch for a single version can be performed. Restoring multiple versions and overwrite restores are not supported, as SharePoint does not allow the creation of a new version on top of such items.

Table 27-3 *(continued)*

Limitations	Description

Restore of the list items to lists which have publishing and approval requirements	■ Items are not published or approved if **Restore all versions** is not selected.
	■ Items will be published and/or approved based on the following conditions:
	  ■ The destination list must have either of these options enabled in SharePoint Online; the **Create major and minor (draft) versions** option for publishing, or the **Content approval** option for approval.
	  ■ The version number of the item restored must be a major version.
	  ■ NetBackup cannot retain the original author and date when restoring items to lists that require approval. The **Modified By** field will display the **SharePoint App**. To address this, NetBackup adds a comment indicating the original author and date.

Restore Teams chat messages and Teams channel conversations

You can use the following procedure to restore data to the Teams chat location.

Before you begin:

Before you begin, consider the following points:

- **Export Service Configuration**:
  Verify that the Export service is already configured for your tenant. Contact Cohesity Support if it is not configured.
- **Restore limitations**:
  Understand the restore limitations.
  See "Restore limitations for Teams chat" on page 290.

Procedure to restore Teams chats and Teams channel conversations:

1. Access the Administration portal.
2. On the left, click **Content**.
3. On the **Content** page, do the following:

- From the upper-left dropdown list, select the Stor that hold the data that you want to restore.
- From the dropdown list next to the selected Stor, do any of the following:
  - To display all data in the selected Stor, select **All content**.
  - To view specific data within the Discovery cases, select the required Discovery case.

  The users' names are displayed on the left pane. You can enter the name of a specific user in the **Filter by name** field to search for a specific user.
- On the left pane, select the username.
- On the right pane, do any of the following:
  - To restore the user's entire mailbox, select the check box of the folder.
  - From the right pane, expand the required folder. The items in the selected folder are listed on the right pane.
  - From the left pane, select the checkboxes of the items that are to be restored.
- Click **Restore**.

4 On the **Restore** page, do the following as required:

- From the **Restore type** dropdown list, select **TeamsChat**.
- From the **Destination** dropdown list, select the Export service that is configured for your tenant.

  For more details, contact Cohesity Support.
- From the **Reference Time Zone** dropdown list, select the time zone that is to be stamped on the chats.
- Select the **Overwrite items** to overwrite the existing items by the items in the backup copy.
- Configure the **Restore all**, **Point-in-time**, and **Specific range** options.

  See "Configure Restore all, Restore all versions, Point-in-time, and Specific range restore options" on page 337.

- Enter the email addresses of the users to send a notification on restore completion. Use a semicolon to add multiple email addresses. After all the configurations are completed, click **Restore**.

5 Navigate to the destination location to confirm that the restore has happened successfully.

You can go to the **Restore dashboard** to see the status of the restore.

See "About Restore dashboard" on page 340.

Restore limitations for Teams chat

The following are the limitations of the Teams chat data restore:

- Restore of reactions on the chats is not supported.
- Restore of users' one-on-one chat is not supported.
  Downloading the one-on-one chats using the Administration portal or Export Utility lets you access the one-on-one chats. The chats are downloaded in HTML format.
- The **Type** column in the **Export Jobs** tab of the Export Service is displayed as **Unknown** for the Teams chat when restore is done using the Export service.
- Replies to the deleted, edited, or reacted messages do not show which message the reply is associated with.
  Example: A reply to an edited message does not specify which message it was in response to.
- Scheduled meetings are not restored correctly.

Restore O365 audit logs

To know how to restore O365 audit logs on the File server,

See "Restore data to File server" on page 336.

Restore Box data

Use the following procedure to restore data to the Box location. You can also download the items to the required location. See "Downloading an item" on page 338.

Before you begin:

Before you begin, consider the following points:

- **Export Service Configuration**:

Verify that the Export service is already configured for your tenant. Contact Cohesity Support if it is not configured.

- **Restore limitations**:
  Understand the restore limitations.
  See "Restore limitations for Box" on page 292.

Procedure to restore the Box data to the Box environment:

1. Open a web browser and access the Administration portal.
2. On the left, click **Content**.
3. On the **Content** page, do the following:
   - To display all data in the selected Stor, select **All content**.
   - To view specific data within the Discovery cases, select the required Discovery case.

   The users' names are displayed on the left pane. You can enter the name of a specific user in the **Filter by name** field to search for a specific user's mailbox.
4. From the left pane, expand the required folder. The items in the selected folder are listed on the right pane.
5. On the **Restore** page, do the following as required:
   - From the **Restore type** dropdown list, select **Box**.
   - From the **Destination** dropdown list, select the Export service that is configured for your tenant.
     For more details, contact Cohesity Support.
   - From the **Mailbox email address** field, select the email address of the user for which the data has to be restored.
   - If you choose the **Overwrite items** check box, select one of the following restore behaviors:
     - **Trash existing file before restoring**: Deletes the existing files and writes files in the backup.
     - **Restore as a new version to the existing file**: Creates a new version for the existing files.
   - For information on the following options, refer to See "Configure Restore all, Restore all versions, Point-in-time, and Specific range restore options" on page 337.
     Restore all
     Point-in-time
     Specific range

- Enter the email addresses of the users to send a notification on restore completion. Use a semicolon to add multiple email addresses. After all the configurations are completed, click **Restore**.

6 Navigate to the destination location to confirm that the restore has happened successfully.

You can go to the **Restore dashboard** to see the status of the restore.

See "About Restore dashboard" on page 340.

Restore limitations for Box

The following are not supported for restore for Box:

- Multiple versions of the files.
- Any content that was not backed up.
- Recreation of the permissions on restore.
- Recreation of the shares on restore.
- Custom metadata on folders and files.

Restore Google Drive data

Use the following procedure to restore Google Drive data to the Google Drive environment.

You can also download the items to the required location.

See "Downloading an item" on page 338.

Procedure to restore the Google Drive data to the Google Drive environment:

1 Access the Administration portal.

2 Click **Content**.

3 On the **Content** page, do the following:

- From the upper-left dropdown list, select the Stor that hold the data that you want to restore.
- From the dropdown list, which is next to the selected Stor, do any of the following:
  - Select **All content** to display the data in the selected Stor.

- Select a policy or a Discovery case to view specific items in the selected Stor.
  The connectors to which the selected Stor is mapped are listed in the left pane.

- On the left pane, do the following:
  - On the left pane, search for the required connector by entering its name in the **Filter by name** field.
  - Click the connector name.
    The Google Drive accounts backed using the selected connector are listed on the right pane.
- On the right pane, do the following:
  - Click the folder that has the account name.
  - Select the checkboxes of the items that you want to restore.
  - Click **Restore**.

4 On the **Restore** page, do the following:

- From the **Restore type** dropdown list, select **Google Drive**.
- From the **Destination** dropdown list, select the Export service location that is configured for your tenant.
  For more details, contact Cohesity Support.
- Do any of the following:

To restore data to the user's drive, do the following:	To restore data to the shared drive, do the following:
■ Click **User Drive**. ■ Enter the user's email address in the **Export user email address** field. ■ Click **Browse**. ■ From the **Restore** page, browse and select the target location for the restore.	■ Click **Shared Drive**. ■ Enter the user's email address in the **Export user email address** field. ■ From the **Shared drive name** dropdown list, select the target folder for the restore. ■ Click **Browse**. ■ From the **Restore** page, browse and select the target location for restore.

- For more information on the **Overwrite items** option, See "Overwrite restore behavior for Box/Google Drive data" on page 294.
- Do any of the following:

- Select the **Restore permissions** check box to restore the permissions on the backed-up items that are backed up at the time of backup.
- Do not select the **Restore permissions** check box to skip the permission restore.

- For more information on **Restore all**, **Point-in-time**, and **Specific range** options, See "Configure Restore all, Restore all versions, Point-in-time, and Specific range restore options" on page 337.
- For more information configuring email address, See "Configure email addresses for notifications" on page 338.
- Click **Restore**.
  To view the restore progress, go to the Home page. Click **Restore dashboard** option on the **Content** section.

5 Navigate to the destination to confirm that the restore is completed successfully.

Related topics:

See "Backup limitations for Google Drive" on page 175.

See "Downloading an item" on page 338.

Overwrite restore behavior for Box/Google Drive data

If you choose the **Overwrite items** check box for the Box/Google Drive data, select one of the following restore behaviors:

- **Trash existing file before restoring**: Deletes the existing files and writes files in the backup.
- **Restore as a new version to the existing file**: Creates a new version for the existing files.

Restore Gmail data

You can restore the user's entire mailbox, a specific folder, and any individual item from the mailbox.

The user's data can be restored to the same or a different user's mailbox.

Gmail allows users to classify email into various categories based on a Label concept (essentially tags). A single message may be tagged under several labels. The standard labels are UNREAD, SENT, or DRAFT. The user can also create their custom label.

You can also download the items to the required location. See "Downloading an item" on page 338.

Procedure to restore Gmail data to the Gmail environment:

1. Access the Administration portal.
2. On the left, click **Content**.
3. On the **Content** page, do the following:
   - From the top-left drop-down list, select the Stor that holds the data to be restored.
   - From the drop-down list, which is next to the selected Stor, Do one of the following:
     - Select **All content** to display all data in the selected Stor.
     - Select the required policy or Discovery case to view specific data in the selected Stor.
   - From the left pane, expand the required folder. The items in the selected folder are listed on the right pane.
   - From the right pane, select the checkboxes of the items that are to be restored and click **Restore**.
4. On the **Restore** page, do the following as required:
   - From the **Restore type** drop-down list, select **Gmail**.
   - From the **Destination** drop-down list, select the restore service that is configured for your tenant.
     For more details, contact Cohesity Support.
   - Do one of the following:
     - To restore data to the same user's mailbox, enter the same user's email address in the **Export user email address** field.
     - To restore data to the different user's mailbox, enter the user's email address in the **Export user email address** field.
   - Do the following:
     - The **Restore with Message Labels** check box is enabled by default. This option enables labels in the restore.
       If not selected, all messages are restored without any labels. You can find the emails only by search or when looking in the **All mail** location in Gmail.
     - Select the **Restore Deleted Labels** check box to recreate any labels that were deleted since the time of the backup.
       If you clear the check box, restored messages that are not tagged with labels are not restored.

- Select the **Restore Renamed Label Names** check box to reset the name of any label that was renamed since the time of the backup.
  If you clear the check box, any label that was renamed is left as-is (with the new name).

- Select the **Overwrite items**, if you want to overwrite the existing items at the destination with the backup copy.
- See "Configure Restore all, Restore all versions, Point-in-time, and Specific range restore options" on page 337.
- See "Configure email addresses for notifications" on page 338.
- Click **Restore**.

5 Navigate to the destination location to confirm that the restore has happened successfully.

About Salesforce Data, Metadata, and CRM Content restore and Sandbox seeding

Here is the overview on the restore procedure for you need to perform for Salesforce Data, Metadata, CRM Content, and Sandbox seeding.

Salesforce Data, Metadata, and CRM Content restore

Table 27-4

Restore of the Standard and Custom objects (Structured data)	This procedure restores structured data that includes standard and custom objects, its associated records, nested child objects and records, and linked files, attachments, documents, and notes. You can restore the structured data in two ways: ■ **Restore the whole object**: Restoring the whole object method is most suitable when restoring many or all records within the object. The process may take longer, as all records within the selected object are compared with records in the target Salesforce instance before the restore. See "Restore Standard and Custom objects (Structured data restore)" on page 301. ■ **Restore specific records within the object** : If the records to be restored are known, you can select the exact records using queries. This method is faster compared to restoring the whole object. See "Restore specific Records (Structured data) using Query filters" on page 305.
Restore of the Salesforce CRM Content (Unstructured data)	This procedure restores unstructured data, such as files and documents that are not linked to structured data. It includes files and documents from public/shared libraries created using the **File** tab tab. It also includes restoring all public/shared libraries. See "Restore Salesforce CRM Content (Unstructured data restore)" on page 309.
Restore of the custom Metadata	This procedure restores the metadata such as profiles, roles, settings, and so on associated with the data. See "Restore Salesforce Metadata" on page 323.

Note: Restoring the Connected app removes the ConsumerKey from the .zip file before restoring, as a new ConsumerKey is generated at the destination organization.

Sandbox seeding

You can restore the Salesforce data and metadata to the same or another Salesforce instance. Restoring data and metadata to another instance is also referred as

Sandbox seeding. Cohesity Alta SaaS Protection supports the following configurations for Sandbox seeding:

- Production to Sandbox
- Sandbox to Sandbox

The following are the prerequisites to perform Sandbox seeding:

- Configure a separate export location for the target Salesforce organization.

  Note: You are required to add a Salesforce connector for the target Salesforce organization. This process auto-creates an export location for it.

Note: To restore an inactive owner, refer to the link: https://help.salesforce.com/s/articleView?id=000386875&type=1

Guidelines for Schema changes in Salesforce organization to prevent restore failures

Schema mismatches can lead to restore failures, particularly when recovery points were created before schema changes. To minimize issues, follow these guidelines when modifying the schema in the Salesforce organization.

Table 27-5

Schema change	Description
Field size change	Widening a field size (for example, from 30 to 60 characters) ensures compatibility with older recovery points. Data from these recovery points can be restored seamlessly. For example, an older recovery point created with an Object Field size of 30 characters can easily restore data to a Field modified to 60 characters. However, it will fail if the Field is truncated to 15 characters.

Table 27-5 *(continued)*

Schema change	Description
Field type change	Changing a field to a compatible type (for example, from Text to TextArea) allows proper restores, as both store string data. However, Cohesity Alta SaaS Protection does not support changing a field to an incompatible type (for example, from Text to Number), which will result in restore failures.
Deletion of fields	Avoid deleting existing fields of an object, as recovery points rely on the schema captured during the backup process. If a field present in an older recovery point has been deleted in the Salesforce organization, restores will fail. Cohesity Alta SaaS Protection does not currently support restoring data to a schema where fields from the recovery point are missing at the time of restore in target organization.
Non-Null fields added later	Adding non-null fields to an object after a recovery point has been created is not currently supported for restores from those older recovery points. This functionality is planned for future product updates.

Table 27-5 *(continued)*

Schema change	Description
Picklist and Record Type modifications	■ **Deactivation of Picklist Values**: Deactivating a Picklist value that exists in older recovery points can cause restore failures. To prevent this, ensure that the picklist value is active in Salesforce before performing a restore. Note that the ability to replace deactivated Picklist values with new ones during the restore process is planned for future product updates. ■ **Deselection of Picklist Values in Record Types**: If a Picklist value associated with a record type is present in older recovery points but later removed from the Selected Value list in Salesforce, restore operations will fail. To avoid this, ensure that the Picklist value remains in the Selected Values list for the record type. Note that the ability to replace deselected Picklist values with new ones during the restore process is planned for future product updates. ■ **Deactivation of Record Types**: Deactivating a record type that exists in older recovery points will result in restore failures. To prevent this, ensure that the record type remains active in Salesforce before performing a restore. The ability to replace deactivated record types with alternative record types during the restore process is planned for future product updates.

Restore Standard and Custom objects (Structured data restore)

You can use this procedure to restore the standard and custom objects, its associated records, nested child objects and records, and linked files, attachments, documents, and notes.

Points to consider:

- To restore the contacts linked to multiple accounts:
  Make sure that the **Allow users to relate a contact to multiple accounts** setting is enabled during the restore process if it was enabled during the backup. If this setting is disabled before the restore operation is initiated, the restore fails.
- To restore **OpportunitySplit** records:
  Make sure the **OpportunitySplit** setting is enabled during the restore if it was enabled during the backup. If this setting is disabled before the restore operation is initiated, the restore fails.
- To restore **converted Lead records**: Ensure that the **View and Edit Converted Leads** setting is enabled during the restore if it was enabled during the backup. If this setting is disabled before the restore operation is initiated, the restore will fail.
- Refer to the following topics for limitations:
  See "Salesforce Objects not supported for restore" on page 315.
  See "Limitations of Salesforce Data restore" on page 313.

To restore Standard and Custom objects (Structured data)

1. Access the Cohesity Alta SaaS Protection Administration portal.
2. On the home page, click **Content**.
3. On the **Content** page, do the following:
   - From the upper left dropdown list, select the Salesforce Data Stor that contains backup of your organization.
     The associated recovery points are available in the dropdown list next to the selected Stor.
     By default, the latest restore point is selected. You can select the required restore point from the dropdown list if you need to restore data from a previous restore point.

     Note: Always select the restore point marked with a green tick as it indicates that the corresponding backup job is completed successfully, without any error.

Note: To set the other restore point as the default one, click the restore points dropdown list > **Specific restore point** link > on the **Set to specific restore point** page, select the restore point to be set as default, and then click **Set**.

The left pane lists all objects, and the right pane lists the records within the selected object.

- On the left pane, select the object you want to restore.
  To search for a specific object, enter its name in the **Filter by name** field.
  You can select the **All** check box to view all objects (including non-restorable objects).
- Click **Restore** at the upper right of the page.
  You are directed to the **Restore** page that displays the following details:

Restore Mode field	This field displays the value as **Data**. As you have initiated data restore.
Restore point field	This field displays the recovery point that you have selected using step 3. If you want to restore the data from other restore point, select the required one from the dropdown list.
Restore to Salesforce organization field	This field lists the Export services configured for different Salesforce organizations. By default, the same organization to which the data belongs is selected. In case you want to restore the data to another Salesforce organization, select the Export services of another organization from the dropdown list. Refer to the **Sandbox seeding** topic in the See "About Salesforce Data, Metadata, and CRM Content restore and Sandbox seeding" on page 296.

4 Do the following on the **Restore** page:

- From the **Restore type** section, click **Object**.
  By default, the object that is selected on the **Content** page (step 4) is displayed in the **Object** dropdown list.

If you want to change the object, click the dropdown list and select the required one.

- (Optional) Expand the **Advanced options** options, and do any of the following to configure the **Overwrite existing records** check box:
  - Select the **Overwrite existing records** check box to update existing records and their fields in the target Salesforce organization with the records and field values from the selected restore point.
  - Clear the **Overwrite existing records** check box to skip restoring existing records that are already present at the destination.

Note: The records are compared using the ID field.

- Refer to the following steps only for converted Lead object restore:
  If you are restoring the converted Lead objects, you can see the following two options:
  - **Update**: Select this option if Lead objects are intentionally converted to Account, Contact or Opportunity and you want to restore them in their converted format.
  - **Revert**: Select this option if Lead objects are accidentally converted and you want to revert them to their original format. Before selecting this option, do the following in your Salesforce organization:
    - Delete the newly created Contact, Opportunity, and Account records in the following order: Delete the Contact record first, followed by the Opportunity record, and finally the Account record.
    - To identify these newly created records, check their timestamps—they should be the same as or later than the timestamp of the converted Lead record.

5 Click **Next**.

All records in the selected object are displayed.

6 Click **Next**.

During this step, Cohesity Alta SaaS Protection analyzes and prepares a list of nested child records related to the selected parent records for restoration. This phase identifies all related records, including files, attachments, and documents associated with the parent records selected for the restore.

In Salesforce, when a parent record is deleted, nested child object records often get deleted too due to cascade delete operations. The Analyze phase addresses this by identifying all related records from the backup and selecting them for the restore by default.

The duration of the restore process may vary depending on the number and size of records and related nested child objects. At the end of the Analyze phase, all identified records for restoration are available for preview.

This lets you see which additional records will be restored alongside the selected parent object records. If the analyzed records are not satisfactory, you can abandon the restore at this stage.

7 Click **Next**.

8 On the **Email notifications** page, enter the email addresses of the users who need to be notified on the completion of the restore operation.

9 Click **Next**.

10 Verify the details and click **Restore**.

In case if you choose not to wait for the Analyze phase to finish, the restore operation gets queued and starts once the Analyzed operation is finished.

Depending upon the amount of the data Analyzed for the restore, the time required for restore operation can vary.

After the restore is initiated, you can go to the **Restore dashboard** to view the restore progress.

See “About Restore dashboard” on page 340.

11 Navigate to the destination Salesforce organization to confirm that the restore is completed successfully.

Custom Object restore - post processing steps

The restore of a custom object may also require the restoration of some related dependencies (metadata components) because such dependencies are not evaluated and restored automatically. The list of dependencies to be restored after restoring custom object are as follows:

- **Restore dependencies:**

If the custom object is related to any other custom or standard object, the related objects need to be restored after restoring the custom object.

- **Add AppExchange packages:**
  Add the custom object restored to any appropriate AppExchange packages that are referring to this custom object.
- **Restore custom tab and list views:**
  Restore a custom tab and any list views associated with the custom object restored.
- **Restore workflow rules:**
  Restore the workflow rules related to the custom object.
- **Restore validation rules:**
  Restore any custom validation rules for the custom object.
- **Restore approval processes:**
  Restore any approval processes associated with the custom object.
- **Enable formula fields:**
  Open and save any custom formula fields on the custom object to enable them.
- **Restore rules:**
  Restore any matching rules or duplicate rules for the custom object.
- **Page layouts:**
  On the page layouts of other objects, add the custom object-related list, option, or link to any page layouts that have been edited while the object is deleted. Related lists, options, or links to this object are automatically restored if the page layout is not edited while the object is deleted.
- **Custom report types:**
  For custom report types where the object is not the main object, add the reference to the custom object back to the custom report types. Reports based on the custom report type are automatically restored if not edited while the object is deleted. Recreate any reports that have been edited.
- **Deployment mode:**
  If the custom object was set to In Development mode, edit the object to change it to Deployed when all setup changes affected by the delete have been restored.

Restore specific Records (Structured data) using Query filters

Use the following procedure to select the specific records that are to be restored by applying filters. Use this method when you can search the records based on the known field value. For example, if the user wants to restore a Contact whose name

starts with **John** and belongs to a company **Infinity**. Such complex queries and filters enable you to search and select the specific records for the restore.

See "Salesforce Objects not supported for restore" on page 315.

See "Limitations of Salesforce Data restore" on page 313.

To restore specific Records (Structured data) using Query filters

1. Access the Cohesity Alta SaaS Protection Administration portal.
2. On the home page, click **Content**.
3. On the **Content** page, do the following:
   - From the upper left drop-down list, select the Salesforce Data Stor that contains backup of your organization.
     The associated recovery points are available in the drop-down list next to the selected Stor.
     By default, the latest restore point is selected. You can select the required restore point from the drop-down list if you want to restore data from a previous restore point.

     Note: Always select the restore point marked with a green tick as it indicates that the corresponding backup job is completed successfully, without any error.

     Note: To set the other restore point as the default one, click the restore points drop-down list > **Specific restore point** link > on the **Set to specific restore point** page, select the restore point to be set as default, and then click **Set**.

     The left pane lists all objects, and the right pane lists the records within the selected object.
4. On the left pane, select the object you want to restore. For example, ***Contact***.

   Note: You can filter the list to view specific object/record using the **Filter by name** field.

   Note: Select the **All** check box to view all objects (including non-restorable objects).

5 Click **Restore** at the upper right of the page.

You are directed to the **Restore** page that displays the following details:

Restore Mode field	This field displays the value as **Data** as you have initiated the data restore process.
Restore point field	This field displays the recovery point that you have selected using Step 3.
Restore to Salesforce organization field	This field displays the Export services configured for different Salesforce organizations. By default, the same organization to which the data belongs is selected. In case you want to restore the data to another Salesforce organization, select the Export services of another organization from the drop-down list. Refer to the **Sandbox seeding** topic in the See "About Salesforce Data, Metadata, and CRM Content restore and Sandbox seeding" on page 296.

6 From the **Restore type** section, click **Records**.

7 Do the following to apply filters to restore specific records within the selected object:

- Click **Add a filter**.
- From the drop-down list, select the required parameter.
  For example, ***BillingCity***.
  The filter is added. By default, the **equal** operation is selected for the filter.
- Select the required parameter that is either **equal** or **not equals** from the drop-down list.
- Enter an appropriate value in the next field. For example, **New York**.
  You can also add multiple filters to meet your specific data requirement. If you add multiple filters, you can choose to apply either **any** or **all** conditions. When we choose **any**, the records matching any of the defined filter criteria are selected for restore. When you choose **all**, the records matching all of the defined filter criteria are selected for restore.

8 (Optional) Expand the **Advanced options** options and select the **Overwrite existing records** check box to overwrite the content at the target organization.

If the check box is selected, the restore updates existing records and their fields in the target Salesforce organization with the records and field values captured in the selected restore point.

If this check box is not selected, the restore of the existing records is skipped.

Note: The records are compared using the ID field.

---

9 Click **Next**.

10 Click **Next**.

During this step, Cohesity Alta SaaS Protection analyzes and prepares a list of nested child records related to the selected parent records for restoration. This phase identifies all related records, including Files, Attachments, and Documents associated with the parent records selected for the restore.

In Salesforce, when a parent record is deleted, nested child object records often get deleted too due to cascade delete operations. The Analyze phase addresses this by identifying all related records from the backup and selecting them for the restore by default.

The duration of the restore process may vary depending on the number and size of records and related nested child objects. At the end of the Analyze phase, all identified records for restoration are available for preview.

This allows you to see which additional records will be restored alongside the selected parent object records. If the analyzed records are not satisfactory, you can abandon the restore at this stage.

11 Click **Next**.

12 On the **Email notifications** page, enter the email addresses of the users who need to be notified on the completion of the restore operation.

13 Click **Next**.

14 Verify the details and click **Restore**.

In case if you choose not to wait for the Analyze phase to finish, the restore operation gets queued and starts once the Analyzed operation is finished.

Depending upon the amount of the data Analyzed for the restore, the time required for restore operation can vary.

After the restore is initiated, you can go to the **Restore dashboard** to view the restore progress.

See "About Restore dashboard" on page 340.

15 Navigate to the destination Salesforce organization to confirm that the restore is completed successfully.

Restore Salesforce CRM Content (Unstructured data restore)

You can use this procedure to restore unstructured data such as files and documents that are not linked to structured data. It includes files and documents.

See "Salesforce Objects not supported for restore" on page 315.

See "Limitations of Salesforce Data restore" on page 313.

To restore Salesforce CRM Content (Unstructured data)

1 Access the Cohesity Alta SaaS Protection Administration portal.

2 On the home page, click **Content**.

3 On the **Content** page, do the following:

- From the upper left dropdown list, select the Salesforce Metadata Stor that contains backup of your organization.
  From the dropdown list next to the selected Stor, select **All content**.

  Note: You can search for the required item using the **Filter by name** field.

  The left pane lists all connectors that are mapped to the selected Stor.

4 On the left pane, do the following:

- Expand the connector name folder.
  The organizations mapped to this connector are listed.
- Expand the organization name folder.
- Select the **Data** folder.
  Browse for the required data that is to be restored.

5 Click **Restore** at the upper right of the page.

You are directed to the **Restore** page that displays the following details:

Restore Mode field	This field displays the value as **Metadata**.
Restore point field	This field displays the recovery point that you have selected using step 3. If you want to restore the data from another restore point, select the required one from the dropdown list.
Restore to Salesforce organization field	This field lists the Export services configured for different Salesforce organizations. Select the Export services for the destination organization.

6 Expand **Advanced options** and do any of the following:

- Select the **Validate only** check box to validate (pre-check) the selected Metadata type for dependencies without restoring them.
- Clear the **Validate only** check box to continue the restore.

7 Click **Next**.

8 On the **Email notifications** page, enter the email addresses of the users who need to be notified on the completion of the restore operation.

9 Click **Next**.

10 Verify the details and click **Restore**.

After the restore is initiated, you can go to the **Restore dashboard** to view the restore progress.

See "About Restore dashboard" on page 340.

11 Navigate to the destination Salesforce organization to confirm that the restore is completed successfully.

Restore Salesforce files/documents in Public/Shared libraries (Unstructured data restore)

You can use this procedure to restore unstructured data such as files and documents that are not linked to structured data. It includes files and documents from Public/Shared libraries created using the **File** tab.

See "Salesforce Objects not supported for restore" on page 315.

See "Limitations of Salesforce Data restore" on page 313.

To restore Salesforce CRM Content (Unstructured data)

1. Access the Cohesity Alta SaaS Protection Administration portal.
2. On the home page, click **Content**.
3. On the **Content** page, do the following:
   - From the upper left dropdown list, select the Salesforce Data Stor that contains backup of your organization.
     The associated recovery points are available in the dropdown list next to the selected Stor.
     By default, the latest restore point is selected. You can select the required restore point from the dropdown list if you need to restore data from a previous restore point.

     Note: Always select the restore point marked with a green tick as it indicates that the corresponding backup job is completed successfully, without any error.

     Note: To set the other restore point as the default one, click the restore points dropdown list > **Specific restore point** link > on the **Set to specific restore point** page, select the restore point to be set as default, and then click **Set**.

     Note: You can filter the list to view specific object/record using the **Filter by name** field. Also, you can select the **All** check box to view all objects (including non-restorable objects).

     The left pane lists all objects, and the right pane lists the records within the selected object.
4. On the left pane, do any of the following:
   - To restore the documents within the Public/Shared libraries, in the **Filter by name** filed, type **ContentDocument**.
   - To restore the libraries within the Public/Shared libraries, in the **Filter by name** field, type **ContentWorkspace**.

5 Click **Restore** at the upper right of the page.

You are directed to the **Restore** page that displays the following details:

Restore Mode field	This field displays the value as **Data** as you initiated the data restore process.
Restore point field	This field displays the recovery point that you have selected using step 3. If you want to restore the data from another restore point, select the required one from the dropdown list.
Restore to Salesforce organization field	This field displays the Export services configured for different Salesforce organizations. By default, the same organization to which the data belongs is selected. In case you want to restore the data to another Salesforce organization, refer to the **Sandbox seeding** topic in the See "About Salesforce Data, Metadata, and CRM Content restore and Sandbox seeding" on page 296.

6 (Optional) Expand the **Advanced options** options and select the **Overwrite existing records** check box to overwrite the content at the target organization.

If the check box is selected, the restore updates existing records and their fields in the target Salesforce organization with the records and field values captured in the selected restore point.

If this check box is not selected, the restore of the existing records is skipped.

Note: The records are compared using the ID field.

---

7 Click **Next**.

8 Click **Next**.

During this step, Cohesity Alta SaaS Protection analyzes and prepares a list of nested child records related to the selected parent records for restoration. This phase identifies all related records, including Files, Attachments, and Documents associated with the parent records selected for the restore.

In Salesforce, when a parent record is deleted, nested child object records often get deleted too due to cascade delete operations. The Analyze phase addresses this by identifying all related records from the backup and selecting them for the restore by default.

The duration of the restore process may vary depending on the number and size of records and related nested child objects. At the end of the Analyze phase, all identified records for restoration are available for preview.

This lets you see which additional records will be restored alongside the selected parent object records. If the analyzed records are not satisfactory, you can abandon the restore at this stage.

9 Click **Next**.

10 On the **Email notifications** page, enter the email addresses of the users who need to be notified on the completion of the restore operation.

11 Click **Next**.

12 Verify the details and click **Restore**.

In case if you choose not to wait for the Analyze phase to finish, the restore operation gets queued and starts once the Analyzed operation is finished.

Depending upon the amount of the data Analyzed for the restore, the time required for restore operation can vary.

After the restore is initiated, you can go to the **Restore dashboard** to view the restore progress.

See “About Restore dashboard” on page 340.

13 Navigate to the destination Salesforce organization to confirm that the restore is completed successfully.

Limitations of Salesforce Data restore

Following are the limitations of the Salesforce data restore for the current release:

- **Restore with schema mismatch**:
  Restores fail if the target schema differs from the schema at the time of the backup.

Note: If the schema in the target organization is an extension of the schema at the time of backup and remains compatible, the restore will function.

See "Guidelines for Schema changes in Salesforce organization to prevent restore failures" on page 298.

- **Restore limitations due to API limitations**:
  - Emails with attachments uploaded via the Salesforce Lightning portal to the Account object are restored to draft status, including their attachments.
    For more information, refer to the following link:
    About EmailMessage
  - The Public URL and password of files in Salesforce cannot be restored.
    The **DistributionPublicUrl** and **Password** fields are stored in the **ContentDistribution** table and are not updatable.
    You must recreate the Public URL and assign a new password after restoring the document (if the document was publicly distributed).
  - The image in the ContentNote cannot be backed up.
- ContentNote is a non-restorable object. To restore it, you must restore it via ContentDocument.
- The restore from the End-User portal is not supported.
- The restore can fail if the target schema is incompatible with the schema captured at the time of the backup. You must update the target schema before initiating a data restore.
- If the Record type functionality is enabled for any object, older records with a Record type equal to Null cannot be restored.
- If the Export location is configured by the **VASP Backup Admin**, the Private Library Documents of the non-**VASP Backup Admin** are not restored to their own library. Instead, these documents are restored in the **VASP Backup Admin's** Private Library.
- Some Salesforce fields, such as **Currency**, are internally stored as Double data types. As a result, these values are rounded off when backed up.
- A few objects are not supported for the backup and restore. Refer to the following topics to know to get the list:
  See "Salesforce Objects not supported for backup" on page 211.
  See "Salesforce Objects not supported for restore" on page 315.

Salesforce Objects not supported for restore

A few objects cannot be restored due to the following reasons:

- **History** objects are not restorable. They should only be selected for backup if there is a strong need to retain historical information on record or field-level changes for auditing purposes.
- **Share** objects of the type Manual only can be restored. Other types of Share records cannot be restored due to Salesforce API limitations.
- You cannot restore a few Salesforce objects, as Salesforce APIs do not restore the objects for which Salesforce supports query() operations such as insert(), update(), and upsert(). This limitation restricts insert and update operations on some entities.
- The **TrackedChanges** type in the **FeedItem** standard object cannot be restored.
- The restore of **ContentWorkspace** is not supported for the **Partner Enterprise** type organization.
- The Salesforce objects that are not backed up by Cohesity Alta SaaS Protection cannot be restored.
  See "Salesforce Objects not supported for backup" on page 211.
- Apart from the above objects, some additional objects that are not supported for restore are listed as follows:
  - *Events
  - *Feed
  - *Share
  - FAQ*
  - AcceptedEventRelation
  - AccountPartner
  - ActiveFeatureLicenseMetric
  - ActivePermSetLicenseMetric
  - ActiveProfileMetric
  - ApexLog
  - ApexPageInfo
  - ApexTypeImplementor
  - AppAnalyticsQueryRequest
  - AppDefinition

- Approval
- AppTabMember
- AsyncApexJob
- AttachedContentDocument
- AuraDefinition
- AuraDefinitionBundleInfo
- AuthConfig
- AuthConfigProviders
- AuthSession
- BackgroundOperation
- BriefcaseAssignment
- BriefcaseDefinition
- BriefcaseRule
- BriefcaseRuleFilter
- Calendar
- CallCenter
- CampaignMemberStatus
- CaseArticle
- CaseExternalDocument
- CaseMilestone
- CaseStatus
- ChatterActivity
- ClientBrowser
- CollaborationGroupRecord
- CollaborationInvitation
- ColorDefinition
- CombinedAttachment
- Community
- ContentDistribution
- ContentDistributionView

- ContentDocumentSubscription
- ContentTagSubscription
- ContentUserSubscription
- ContractStatus
- CronJobDetail
- CronTrigger
- CustomHttpHeader
- CustomObjectUserLicenseMetrics
- CustomPermission
- CustomPermissionDependency
- DataAssessmentFieldMetric
- DataAssessmentMetric
- DataAssessmentValueMetric
- DataStatistics
- DataType
- DeclinedEventRelation
- DelegatedAccount
- DocumentAttachmentMap
- Domain
- DomainSite
- EmailCapture
- EmbeddedServiceDetail
- EmbeddedServiceLabel
- EntityDefinition
- EntityMilestone
- EntityParticle
- EventBusSubscriber
- EventLogFile
- EventRelayConfig
- EventRelayFeedback

- ExpressionFilterCriteria
- ExpressionSetView
- ExternalDataSource
- ExternalDataSrcDescriptor
- ExternalDataUserAuth
- ExternalSocialAccount
- FeedPollChoice
- FeedPollVote
- FeedRevision
- FeedTrackedChange
- FieldDefinition
- FieldPermissions
- FieldSecurityClassification
- FileSearchActivity
- FiscalYearSettings
- FlexQueueItem
- FlowDefinitionView
- FlowInterview
- FlowInterviewLog
- FlowInterviewLogEntry
- FlowOrchestrationInstance
- FlowOrchestrationStageInstance
- FlowOrchestrationStepInstance
- FlowOrchestrationWorkItem
- FlowRecordRelation
- FlowStageRelation
- FlowTestResult
- FlowTestView
- FlowVariableView
- FlowVersionView

- FormulaFunction
- FormulaFunctionAllowedType
- FormulaFunctionCategory
- GrantedByLicense
- GroupMember
- IconDefinition
- IdpEventLog
- Image
- InstalledMobileApp
- KnowledgeableUser
- KnowledgeArticle
- KnowledgeArticleVersion
- KnowledgeArticleViewStat
- KnowledgeArticleVoteStat
- LeadStatus
- LightningExitByPageMetrics
- LightningToggleMetrics
- LightningUsageByAppTypeMetrics
- LightningUsageByBrowserMetrics
- LightningUsageByFlexiPageMetrics
- LightningUsageByPageMetrics
- ListView
- ListViewChartInstance
- LoginGeo
- LoginIp
- LogoutEventStream
- LookedUpFromActivity
- MacroUsage
- ManagedContent
- ManagedContentChannel

- ManagedContentSpace
- ManagedContentVariant
- MatchingInformation
- MatchingRuleItem
- MyDomainDiscoverableLogin
- Name
- NamedCredential
- NetworkActivityAudit
- NetworkDiscoverableLogin
- NetworkFeedResponseMetric
- NetworkModeration
- NetworkSelfRegistration
- NoteAndAttachment
- OauthToken
- ObjectPermissions
- OpenActivity
- OpportunityPartner
- OpportunityStage
- OrderStatus
- OrgLifecycleNotification
- OwnedContentDocument
- OwnerChangeOptionInfo
- PackageLicense
- PartnerRole
- Period
- PermissionSetLicense
- PermissionSetTabSetting
- PersonalizationTargetInfo
- PicklistValueInfo
- PlatformAction

- PlatformCachePartition
- PlatformEventUsageMetric
- ProcessDefinition
- ProcessInstance
- ProcessInstanceNode
- ProcessInstanceStep
- ProcessNode
- PromptAction
- PromptError
- PromptVersion
- Publisher
- QueueSobject
- QuickTextUsage
- RecentlyViewed
- Recommendation
- RecommendationResponse
- RelatedListColumnDefinition
- RelatedListDefinition
- RelationshipDomain
- RelationshipInfo
- ReputationLevel
- ReputationPointsRule
- ScorecardAssociation
- SearchActivity
- SearchLayout
- SecurityCustomBaseline
- ServiceSetupProvisioning
- SessionPermSetActivation
- SetupAuditTrail
- Site

- SiteDetail
- SiteIframeWhiteListUrl
- SiteMarketingDataExtensionMapping
- SlaProcess
- SolutionStatus
- SPSamlAttributes
- StaticResource
- TaskPriority
- TaskStatus
- TenantUsageEntitlement
- ThirdPartyAccountLink
- Translation
- UiFormulaCriterion
- UiFormulaRule
- UndecidedEventRelation
- UserAppMenuItem
- UserEntityAccess
- UserFieldAccess
- UserLicense
- UserLogin
- UserPermissionAccess
- UserRecordAccess
- UserSetupEntityAccess
- VisualforceAccessMetrics
- Vote
- WorkOrderLineItemStatus
- WorkOrderStatus

Key considerations for Salesforce Metadata restore

Before initiating metadata restore, you must consider the following points:

- The **Document** object records are backed up by both Data and Metadata backups. However, for restoring the Document object records, use the Metadata restore method.
- Always select the related metadata component files along with the specific metadata component file that you want to restore. The related metadata component files include ***meta.xml*** and ***.html*** files.
  For example, if you want to restore the **ApexClass** component file named Calculator.cls, you must select the related metadata file named ***Calculator.cls-meta.xml*** for restore.
- To restore a **LightningExperienceTheme**, you must first restore the associated **BrandingSet** linked to the **LightningExperienceTheme** being restored.
  To identify which BrandingSet is associated with the LightningExperienceTheme, start restoring the LightningExperienceTheme. After the restoration is complete, an error message appears that displays the name of the associated BrandingSet, which needs to be restored first before restoring the LightningExperienceTheme.
- If you are restoring metadata component for **Profile** metadata type and the targeted Salesforce organization does not have the **Quick Text** settings enabled, the restore fails with an error.
  To address this issue, do the following:
  - Enable the **Quick Text** settings in the Salesforce organization for Classic and Lightning modes.
  - Go to the Cohesity Alta SaaS Protection Administration portal and initiate the restore process. Select the **Remove Standard tab settings for QuickText** check box in **Advanced options**. This action removes the tab settings for Quick Text during the restore process.
  - Set the **activateRSS** value to **False**.

Restore Salesforce Metadata

This procedure restores the Metadata such as profiles, roles, settings, and so on associated with the data. Before initiating Metadata restore, refer to the following topic:

See "Key considerations for Salesforce Metadata restore" on page 322.

To restore Salesforce Metadata

1. Access the Cohesity Alta SaaS Protection Administration portal.
2. On the home page, click **Content**.

3 On the **Content** page, select the required Salesforce Metadata Stor from the upper left drop-down list.

Note: Metadata for all the Salesforce organizations that is backed up through different connectors can be stored in one Stor (unlike Data which is captured in separate Structured Stors).

---

4 On the left pane, do the following:

Note: To view a specific connector, organization, or Metadata type, you can enter its name in the **Filter by name** field.

- Expand the required connector.
  The names of the associated Salesforce organizations are listed.
- Expand the Salesforce organization name.
- Click the **Metadata** folder.
  The restore points available in the backup are displayed on the right pane.
- Click the required restore point.
- Click the **unpackaged** folder. It contains all the unmanaged Metadata type.
- Click the Metadata type that is to be restored.
  For example, *applications*.

5 On the right pane, do the following:

- Select checkbo(s) of the Metadata components that are to be restored.
- Click **Restore** at the upper right of the page.

Note: You can download a Metadata component by clicking **Download** if you want to review the contents of the Metadata component.

You are directed to the **Restore** page that displays the following details:

Restore Mode field	This field displays the value as **Metadata** as you have initiated the Metadata restore process.
Restore point field	This field displays the recovery point that you have selected using Step 3.

Restore to Salesforce organization field	This field displays the Export services configured for different Salesforce organizations. Select the Export services for the destination organization.

6 Expand **Advanced options** and do one of the following:
   - Select the **Validate only** check box to validate (pre-check) the selected Metadata type files for dependencies without restoring them.
   - Clear the **Validate only** check box to continue the restore.

7 Click **Next**.

8 Enter the email addresses of the users who need to be notified on the completion of the restore operation.

9 Click **Next**.

10 Verify the details and click **Restore**.

   After the restore is initiated, you can go to the **Restore dashboard** to view the restore progress.

   See "About Restore dashboard" on page 340.

11 Navigate to the destination Salesforce organization to confirm that the restore is completed successfully.

Limitations of Salesforce Metadata backup and restore

The following are the limitations of Salesforce Metadata backup and restore:

- The Metadata types listed in the following link are not supported by Salesforce. As a result, Cohesity Alta SaaS Protection cannot back up or restore these Metadata types.
  Unsupported Metadata Types
- The backup and restore of the **unpackaged** Metadata are only supported as it is a common use case.

  Note: The managed packages, such as Apex classes, Triggers, and Lightning Web Components, are accessible only to the providers of the Managed package.

- After restoring a **Dashboard** that is created in Salesforce Lightning, its display name appears as a unique numeric ID instead of its original name.

- **Action Plan Template Standard Object Permission** in the **Profile Metadata** type will not be backed up unless user has customize application permission and **IndustriesActionPlans** license.
- The following Metadata types cannot be restored properly due to Salesforce Metadata API limitation:
  - The PathAssistant Metadata type does not restore **CelebrationSettings**.
  - The ChatterExtension Metadata type does not restore **CompositionComponentEnumOrId** field.
  - The Sites Metadata type does not restore **Guest access to the Support API** .
  - The PresenceUserConfig Metadata type does not restore **InterruptibleCapacity** and **After conversation work time** .
- For the objects with **topics for object** enabled, the **Select the text fields you want to use for topic suggestions** (the text fields in the object) are not restored using Metadata API.
- The **ReadOnly.profile** cannot be restored due to Salesforce Metadata API limitation.
- The backup and restore of the following Metadata components is not supported:
  - **DataCloudCompanyMatch.cleanDataService**
  - **DataCloudLeadAppend.cleanDataService**
  - **Calendar2.sharingRules**
  - **OpportunityCompetitor.standardValueSet**
  - **Crisis Layout.layout**
  - **Delivery Task Layout.layout**
  - **Employee Crisis Assessment Layout.layout**
  - **Employee Layout.layout**
  - **Employee User Provisioning Process Layout.layout**
  - **Employee User Provisioning Process Error Layout.layout**
  - **Internal Organization Unit Layout.layout**
  - **Vehicle User Assignment Layout.layout**
  - **StandardLayouts.layout**
- The backup and restore for the following Standard Tab settings is not supported:
  - **standard-DelegatedAccount**

For more information, refer to the following link:
Enable tab settings on DelegatedAccount object

- **standard-PricebookEntry**
- **standard-JournalType**
- **standard-ManufacturingProgram**
- **standard-MfgProgramCpntFrcstFact**
- **standard-MfgProgramVariantFrcstFact**
- **standard-MfgProgramForecastFact**
- **standard-RevenueAsyncOperation**
- **standard-PromotionMarketSegment**
- **standard-GoalAssignment**
- **standard-GoalDefinition**

About Entra ID (Azure AD) objects and records restore

You can restore Entra ID objects and records to the same or another environment. You can restore entire objects like users, groups, application registrations, enterprise applications, or selectively restore specific records within these objects.

Cohesity Alta SaaS Protection supports restore to the following two environments:

- Only to the Entra ID environment
  For more information, See “Restore an Entra ID object” on page 328. and See “Restore specific records within Entra ID objects” on page 332.
- Hybrid setups with on-premises Active Directory configured for one-way synchronization to Entra ID.
  For more information, refer to the Entra ID restore workflows link.

Permissions requirement

You must have the following permissions to perform the restore:

- Within Cohesity Alta SaaS Protection: **Access All Items**
- Within the Entra ID environment:
  - **Global Administrator** if the restore includes users or groups.

- **Global Administrator** or **Application Administrator** if the restore includes Application Registrations or Enterprise Applications.

Best practices to restore Entra ID objects

When performing a restore, there can be a case where a set of entities have a relationship with each other. In this case, the restore for that set of entities needs to happen within the same restore job because, during the restore of permanently deleted items, new Entra IDs are generated.

Performing the restore of a subset of these entities in two separate jobs is not supported, as there is no way for the other restore job to identify the corresponding new IDs that have been generated against the ones in the backup.

Restore an Entra ID object

You can restore an object such as users, groups, app registrations, or enterprise apps using any of the following procedures:

To restore an Entra ID object

1. Access the Administration portal.
2. Click **Content** and do the following:
   - Select the required Stor from the upper left drop-down list.
   - Watch the video or close the pop-up.
   - Click the drop-down list next to the selected Stor and select the required restore point.

     Note: Recovery points represent the point in time when selected objects or records are backed up. Selecting a specific recovery point lets you restore the object or record as it was at the time of backup.

     Note: The latest restore point is selected by default. You can also set another point as the default.

     To set the other restore point as the default one, click the restore points drop-down list > **Specific restore point** link > on the **Set to specific restore point** page, select the restore point to be set as default, and then click **Set**.

   - In the left pane, select the required object, for example, *User*.
   - In the right pane, select all records.

- Click **Restore**.
  The **Restore** page is displayed.

3 On the **Restore** page, do the following:

- If required, change the destination from the **Restore to Microsoft Entra ID** drop-down list. Ensure that you contact Cohesity Support for this change.
- If you are restoring a user object, assign a password in the **Assign default password** field.

  Note: To ensure that your password meets the required guidelines, click the **Password guidelines** link to know more.

- Expand the **Advanced options** section and do the following:
  - Select **Overwrite existing directory** check box to overwrite the items at the destination. If this check box is not selected, existing items at the destination are skipped during restore.
  - Select the **Restore from recycle bin, if it exists there** check box to restore the objects available in the Recycle bin.
  - Select the **Force restore of on-premises synchronized directory objects/records** check box if you cannot restore the object to the on-premises Active Directory. If this check box is selected, the on-premises synchronized objects are restored to the targeted Entra ID. The objects are restored with new IDs and are no longer linked to the on-premises Active Directory.
- Click **Next**.
  Cohesity Alta SaaS Protection verifies the permissions that you have within Entra ID. You cannot proceed if you do not have the required permissions. The items that are to be restored are displayed.
- Click **Next**.
  The items are being analyzed. Depending on the number of items, this operation may take some time. You can also skip analyzing the records and proceed by clicking **Next**.
- On the **Email notifications** page, do the following:
  - Enter the email addresses of the users who must be notified after the restore operation is completed.
  - Click **Next**.
- On the **Review** page, do the following:

- Verify all the details.
- Click **Restore**.
  After the restore is initiated, you can go to the **Restore dashboard** to view the restore progress.

Note: The time required to restore records to the destination can vary.

---

4 Navigate to the destination to confirm that the object is restored successfully.

To restore an Entra ID object

1 Access the Administration portal.

2 Click **Content** and do the following:

- Select the required Stor from the upper left drop-down list.
- Watch the video or close the pop-up.
  - Select the required Stor from the upper left drop-down list.
  - Watch the video or close the pop-up.
  - Click the drop-down list next to the selected Stor and select the required restore point.

    Note: Recovery points represent the point in time when selected objects or records are backed up. Selecting a specific recovery point lets you restore the object or record as it was at the time of backup.

    Note: The latest restore point is selected by default. You can also set another point as the default.

    To set the other restore point as the default one, click the restore points drop-down list > **Specific restore point** link > on the **Set to specific restore point** page, select the restore point to be set as default, and then click **Set**.

  - Click **Restore**.
    The **Restore** page is displayed.

3 On the **Restore** page tab, do the following:

- If required, change the destination from the **Restore to Microsoft Entra ID** drop-down list. Ensure that you contact Cohesity Support for this change.

- Click **Directory object**.
- From the **Resource** drop-down list, select the object that you want to restore.
- If you are restoring a user object, assign a password in the **Assign default password** field.

  Note: To ensure that your password meets the required guidelines, click the **Password guidelines** link to know more.

- Expand the **Advanced options** section and do the following:
  - Select **Overwrite existing directory** check box to overwrite the items at the destination. If this check box is not selected, existing items at the destination are skipped during restore.
  - Select the **Restore from recycle bin, if it exists there** check box to restore the objects available in the Recycle bin.
  - Select the **Force restore of on-premises synchronized directory objects/records** check box if you cannot restore the object to the on-premises Active Directory. If this check box is selected, the on-premises synchronized objects are restored to the targeted Entra ID. The objects are restored with new IDs and are no longer linked to the on-premises Active Directory.
- Click **Next**.
  Cohesity Alta SaaS Protection verifies the permissions that you have within Entra ID. You cannot proceed if you do not have the required permissions. The items that are to be restored are displayed.
- Click **Next**.
  The items are being analyzed. Depending on the number of items, this operation may take some time. You can also skip analyzing the records and proceed by clicking **Next**.
- On the **Email notifications** page, do the following:
  - Enter the email addresses of the users who must be notified after the restore operation is completed.
  - Click **Next**.
- On the **Review** page, do the following:
  - Verify all the details.
  - Click **Restore**.

After the restore is initiated, you can go to the **Restore dashboard** to view the restore progress.

Note: The time required to restore records to the destination can vary.

---

4 Navigate to the destination to confirm that the object is restored successfully.

Restore specific records within Entra ID objects

You can restore specific records within the object such as users, groups, application registrations, or enterprise applications using any of the following procedures.

To restore specific records within Entra ID objects

1 Access the Administration portal.

2 Click **Content** and do the following:

- Select the required Stor from the upper left drop-down list.
- Watch the video or close the pop-up.
- Click the drop-down list next to the selected Stor and select the required restore point.

Note: Recovery points represent the point in time when selected objects or records are backed up. Selecting a specific recovery point lets you restore the object or record as it was at the time of backup.

Note: The latest restore point is selected by default. You can also set another point as the default.

To set the other restore point as the default one, click the restore points drop-down list > **Specific restore point** link > on the **Set to specific restore point** page, select the restore point to be set as default, and then click **Set**.

- In the left pane, select the required object. For example, *User*.
- Click **Restore**.
  The **Restore** page is displayed.

3 On the **Restore** page, do the following:

- If required, change the destination from the **Restore to Microsoft Entra ID** drop-down list. Ensure that you contact Cohesity Support for this change.

- If you are restoring a user object, assign a password in the **Assign default password** field.

  Note: To ensure that your password meets the required guidelines, click the **Password guidelines** link to know more.

- Expand the **Advanced options** section and do the following:
  - Select **Overwrite existing directory** check box to overwrite the items at the destination. If this check box is not selected, existing items at the destination are skipped during restore.
  - Select the **Restore from recycle bin if it exists there** check box to restore the objects available in the Recycle bin.
  - Select the **Force restore of on-premises synchronized directory objects/records** check box if you cannot restore the object to the on-premises Active Directory. If this check box is selected, the on-premises synchronized objects are restored to the targeted Entra ID. The objects are restored with new IDs and are no longer linked to the on-premises Active Directory.
- Click **Next**.
  Cohesity Alta SaaS Protection verifies the permissions that you have within Entra ID. You cannot proceed if you do not have the required permissions. The items that are to be restored are displayed.
- Click **Next**.
  The items are being analyzed. Depending on the number of items, this operation may take some time. You can also skip analyzing the records and proceed by clicking **Next**.
- On the **Email notifications** page, do the following:
  - Enter the email addresses of the users who must be notified after the restore operation is completed.
  - Click **Next**.
- On the **Review** page, do the following:
  - Verify all the details.
  - Click **Restore**.
    After the restore is initiated, you can go to the **Restore dashboard** to view the restore progress.

Note: The time required to restore records to the destination can vary.

4 Navigate to the destination to confirm that the object is restored successfully.

To restore specific records within Entra ID objects using filters

Filters let you select specific data for restore based on certain criteria. It is useful when you know exactly what needs to be restored, for example, if you want to restore a user named *John* in the company *Infinity*.

1 Access the Administration portal.

2 Click **Content**.

3 On the **Content** page, do the following:

- Select the required Stor from the upper left drop-down list.
- Watch the video or close the pop-up.
  On the **Content** page, do the following:
  - Select the required Stor from the upper left drop-down list.
  - Watch the video or close the pop-up.
  - Click the drop-down list next to the selected Stor and select the required restore point.

    Note: Recovery points represent the point in time when selected objects or records are backed up. Selecting a specific recovery point lets you restore the object or record as it was at the time of backup.

    Note: The latest restore point is selected by default. You can also set another point as the default.

    To set the other restore point as the default one, click the restore points drop-down list > **Specific restore point** link > on the **Set to specific restore point** page, select the restore point to be set as default, and then click **Set**.

  - Click **Restore**.
    The **Restore** page is displayed.

4 On the **Restore** page tab, do the following:

- If required, change the destination from the **Restore to Microsoft Entra ID** drop-down list. Ensure that you contact Cohesity Support for this change.

- Click **Records**.
- From the **Resource** drop-down list, select the object of which records you want to restore.
- To configure a filter to select the specific records that you want to restore, do the following:
  - Click **Add a filter**.
    The filter parameters are displayed based on the selected object.
    For example, the user object presents filter parameters such as **displayename**, employeeId, and so on.
  - Select the required parameter from the list.
    For example, ***displayname***. The equal operation is selected for this parameter by default. Enter the value, such as the display name of the user.
  - Add multiple filters to meet your specific data requirements.
    With multiple filters, you can choose to apply either **any** or **all** of the filters using the **Filters** drop-down list.
- If you are restoring a user object, assign a password in the **Assign default password** field.

  Note: To ensure that your password meets the required guidelines, click the **Password guidelines** link to know more.

- Expand the **Advanced options** section and do the following:
  - Select **Overwrite existing directory** check box to overwrite the items at the destination. If this check box is not selected, existing items at the destination are skipped during restore.
  - Select the **Restore from recycle bin if it exists there** check box to restore the objects available in the Recycle bin.
  - Select the **Force restore of on-premises synchronized directory objects/records** check box if you cannot restore the object to the on-premises Active Directory. If this check box is selected, the on-premises synchronized objects are restored to the targeted Entra ID. The objects are restored with new IDs and are no longer linked to the on-premises Active Directory.
- Click **Next**.
  Cohesity Alta SaaS Protection verifies the permissions that you have within Entra ID. You cannot proceed if you do not have the required permissions.

The items that are to be restored are displayed.

- Click **Next**.
  The items are being analyzed. Depending on the number of items, this operation may take some time. You can also skip analyzing the records and proceed by clicking **Next**.
- On the **Email notifications** page, do the following:
  - Enter the email addresses of the users who must be notified after the restore operation is completed.
  - Click **Next**.
- On the **Review** page, do the following:
  - Verify all the details.
  - Click **Restore**.
    After the restore is initiated, you can go to the **Restore dashboard** to view the restore progress.

Note: The time required to restore records to the destination can vary.

---

5 Navigate to the destination to confirm that the object is restored successfully.

Restore Slack data

The Slack data can be restored on the File server using the File restore or the Slack Administrator's utility.

See “Restore data to File server” on page 336.

Restore data to File server

You can restore any data on the file server irrespective of Stor and data type.

To restore data to a File server

1 Access the Administration portal.

2 On the left, click **Content**.

3 On the **Content** page, do the following:

- Select the Stor that holds the data to be restored.

- Either select **All content** to view all data in the selected Stor; or select a policy or case to view a specific items within.
- Select the data to be restored and click **Restore**.

4 On the **Restore** page, do the following as required:

- From the **Restore Type** drop-down list, select **File folder**.
- Select the **Overwrite items** check box, to replace the existing item at the destination with the backup copy.
- For more information on **Restore all**, **Point-in-time**, and **Specific range** options, See "Configure Restore all, Restore all versions, Point-in-time, and Specific range restore options" on page 337.
- For the procedure to configure email address, See "Configure email addresses for notifications" on page 338.
- Click **Restore**.

5 Navigate to the destination location to confirm that the restore has happened successfully.

Set default restore point

To set the restore point

◆ To set the other restore point as the default one, click the restore points drop-down list. Click **Specific restore point** link. On the **Set to specific restore point** page, select the restore point to be set as default, and then click **Set**.

Configure Restore all, Restore all versions, Point-in-time, and Specific range restore options

To select the data to restore from the backup location, configure one of the following options:

- To restore all available data in the selected backup location, click **Restore all**.
  This option is applicable for all the data types.
- To restore data from a specific point in time within the selected backup location, click **Point-in-time** and then set the date, time, and time zone.
  This option is applicable for all the data types.
- To restore the data that is backed up within a specific range, click **Specific Range** and specify criteria such as the **last 7 days**, **last 7 hours**, and so on.
  This option is applicable to all data types.

The **Restore all versions** option enables you to restore all versions of the data in the selected backup location, depending on the selected restore behavior: all, point-in-time, or specified range.

This option is applicable for the following data:

- SharePoint Online
- OneDrive for Business data
- Box data
- Google Drive

See "Configure email addresses for notifications" on page 338.

Configure email addresses for notifications

In the **Send notification to** field, enter the email addresses of the users to send a notification on restore completion. Use a semicolon to add multiple email addresses. After all the configurations are completed on the **Restore** page, click **Restore**.

Downloading an item

You can download a single item to your local computer using the following procedure.

Note: You can only download one file at a time.

To download an item

1. Access the Administration portal.
2. Click **Content**.
3. From the drop-down list, select the Stor that contains the data to be downloaded. For example, *M365 Mailboxes*.
4. On the left pane, browse for the required folder.
5. On the right pane, select the item that you want to download.
6. From the **Actions** menu, click **Download**.

Note: If you cannot find an extension for an Exchange item after downloading it, you must add the '.eml' extension manually.

The SharePoint files for which IRM setting is enabled at the time of backup cannot be opened after their download.

Chapter 28

Restore dashboard

This chapter includes the following topics:

- About Restore dashboard
- Restore job statuses
- How to cancel a restore job?
- View the restore events

About Restore dashboard

The Restore dashboard provides a complete view of restore job statuses across all workloads that are configured within Cohesity Alta SaaS Protection for your tenant.

Key features:

- **Detailed restored job information**
  Each restore job is displayed with various details that includes its state progress, the number of errors (if any), the name of the user who initiated the job, start time, end time, and the duration of the restore process.
  You can click within the row of the job; it takes you to a page with more detailed information about that particular restore job. This page displays all the events for that specific job. You can also filter the list of events based on event types, such as **Error**, **Warning**, and **Information**. By default, **Error** events are listed at the top of the list.
- **Event listing and export**
  When more than 10,000 events are present, the Restore dashboard lists a maximum of 10,000 events with pagination, showing 100 events per page. However, exporting the data to a CSV file includes all events, regardless of the total number.

You can export the details of the restore jobs that are displayed on the page to a CSV format for further analysis or record-keeping.

- **Auto-refresh and manual refresh**
  The Restore dashboard automatically refreshes every 2 seconds to keep you updated with any changes. You can also manually refresh the page to reload the details.
- **Job filtering**
  You can filter the listed restore jobs by workload and state to quickly find the required job.
- **Job re-running**
  You can rerun the **Completed**, **Canceled**, and **Failed** jobs using the **Rerun** option in the associated action menu.
- **Job cancellation**
  You can cancel the **Queued** and **In-progress** restore jobs using the **Cancel** option in the associated action menu.
- **Help video**
  A help video is available when you open the Restore dashboard. If you prefer not to see this video in the future, you can select the **Don't show again** check box.

Navigate to the Restore dashboard

1. Access the Administration portal URL.

   The home page of the Administration portal is displayed.
2. Click **Restore dashboard**, below the **Content** option.

   The **Restore dashboard** is displayed.

Related topics:

- See “Restore job statuses” on page 341.
- See “How to cancel a restore job?” on page 342.
- See “View the restore events” on page 343.

Restore job statuses

The different statuses of the restore jobs are described in the following table:

Table 28-1

Statuses of restore jobs	Description
Queued	It indicates that the user initiated a restore job through the Administration portal, and it is now queued for processing. **Note:** The restore jobs that are initiated through the Export Utility are not displayed here. If required, you can cancel the **Queued** job using the **Cancel** option in the action menu (represented by a hamburger icon).
In-progress	It indicates that the Export service is currently processing the restore job. If required, you can cancel the **In-progress** job using the **Cancel** option in the action menu (represented by a hamburger icon).
Completed	It indicates that the restore process is successfully finished with or without errors for this job. The number of errors (if any) are displayed in the **No. of errors** column. You can click the errors to view more details. If required, you can rerun the **Completed** job using the **Rerun** option in the action menu (represented by a hamburger icon).
Failed	It indicates that the restore process is finished, but no data is restored. If required, you can rerun the **Failed** job using the **Rerun** option in the action menu (represented by a hamburger icon).
Canceled	It indicates that the job is canceled. The restore job can be canceled if it is in the **Queued** or **In-progress** states. If required, you can rerun the **Canceled** job using the **Rerun** option in the associated action menu (represented by a hamburger icon).

How to cancel a restore job?

You can cancel restore jobs with the **Queued** or **In-progress** states.

To cancel a restore job

1. Access the Administration portal URL.

   The home page of the Administration portal is displayed.

2. Click **Restore dashboard**, below the **Content** option.

   The **Restore dashboard** is displayed.

3. Click the **Cancel** option in the associated action menu (represented by a hamburger icon).

View the restore events

To view the restore events

1. Open a web browser and access the Administration portal URL. The home page of the Administration portal is displayed.

2. Click **Restore dashboard**, below the **Content** option.

   The **Restore dashboard** is displayed.

3. Click within the job row for which events are to be viewed.

   The page is displayed that lists all the related events of that particular restore job. By default, **Error** events are listed at the top of the list. You can also filter the list of events based on event types, such as **Error**, **Warning**, and **Information**.

Chapter 29

Install services and utilities

This chapter includes the following topics:

- About services and utilities
- Pre-requisites to download and install services and utilities
- Downloading services and utilities
- Where to install the services and utilities
- Installing or upgrading services and utilities
- Configuring service accounts for services and utilities
- About the Apps Consent Grant Utility

About services and utilities

Cohesity Alta SaaS Protection requires a few services and utilities. The services or utilities may be installed on-premises, or in the cloud on a supported Windows operation system. A Windows computer can host multiple services.

To know more about the supported Windows Operating systems.

Table 29-1

Services and Utilities	Description
Connector service	Used for managing connectors.
Export service	Used for managing bulk data restore.
Retrieval service	Used for restoring data with seamless and link-based stubs.

Table 29-1 *(continued)*

Services and Utilities	Description
Export utility	Used for restoring granular or bulk data and recovery of Discovery cases.
Slack administration utility	Used to backup and restore data in Slack.
Apps Consent Grant utility	Used to approve Microsoft 365 apps in bulk. See "About the Apps Consent Grant Utility" on page 350.

Pre-requisites to download and install services and utilities

The prerequisites to download and install services and utilities are given in the following table.

Table 29-2

Requirement	Description
Operating system	■ Microsoft Windows Server 2025 ■ Microsoft Windows Server 2022 ■ Microsoft Windows Server 2019 **Note:** Only the English versions of the above Operating systems are supported.
CPU	2.3 GHz
RAM	8 GiB

Other requirements:

- Dedicated service accounts for each service and utility.
- Administrator's permissions on the VM.
- Access to the Administration portal.
- One of the following web browsers:
  - Microsoft Edge
  - Google Chrome

If you want to upgrade any services or utilities to 2.15 or later, you get a pop-up message to install the .Net framework.

You must install the .Net framework to proceed with the upgrade.

Downloading services and utilities

Use the following procedure to download services and utilities.

To download services and utilities

1. Open a web browser and access the Administration portal.
2. On the Administration portal, click **Administration**.
3. On the left pane, click **Software download**.

   The page that lists the services and utilities is displayed.
4. Click **Download** which corresponds to the required service or utility.
5. Click **Learn more** to refer to the prerequisites and procedure to install the service and utility.

   See "Installing or upgrading services and utilities" on page 347.

Where to install the services and utilities

Note the following recommendations for installing the services and utilities:

Table 29-3

Services and utilities	Where to install
Connector service	The best practice would be to install it close to your source data on a Windows computer running a supported OS. For example: ■ The Connector service for Microsoft 365 data should be install on an Azure virtual machine in a region close to where Microsoft 365 is installed but with low latency. ■ A Connector service for an on-premises file server must be located on-premises, either on the source server or on a server with low latency to the source data.
Export service	A Windows computer with a supported OS.

Table 29-3 *(continued)*

Services and utilities	Where to install
Retrieval service	A Windows computer with a supported OS. The Retrieval service is only required to access stubbed data. For seamless stubs, the Retrieval service must be installed on the file server where the stubs exist.
Export utility	A Windows computer with a supported OS.
Slack administration utility	A Windows computer with a supported OS.
Apps Consent Grant utility	A Windows computer with a supported OS.

Installing or upgrading services and utilities

Use the following procedure to install or upgrade services and utilities.

To install or upgrade services and utilities

1. Open Windows Explorer > **Downloads**.
2. Double-click the installer file.
3. Click **Run**.
4. In the ***<Setup>*** window, click **Next**.
5. Select the **I accept the terms in the License Agreement** check box.
6. Enter the credentials of the Windows account that you want to use to run this service. This account should be a domain account or a local computer account with the **Log on as a service** permission.
7. Click **Validate**.
8. Click **OK**.
9. Click **Next**.
10. If required, change the installation path.

    The default installation path is **C: \Program Files(x86)\HubStor*<Name of the service or utility>***.
11. Click **Next**.
12. Click **Install**.
13. Click **Finish**.

See "About the Apps Consent Grant Utility" on page 350.

Credentials not needed for service upgrades

In previous versions of Cohesity Alta SaaS Protection, before 2.16.1 and 2.16.1, upgrading services (Connector service, Export service, and Retrieval service) required Windows Administrator credentials.

Cohesity Alta SaaS Protection 2.16.1 release onwards, this step is no longer necessary for service upgrades.

However, if you change the password for the Windows Administrator between releases, you may encounter issues after upgrading to the next release. Specifically, the services may fail to start. In such cases, you must manually update the password for the targeted service.

Configuring service accounts for services and utilities

Typically, there are two different account types used to configure each service,

- A Windows domain or local computer account that you to be used to run this service.
- An Azure account that has the appropriate access in Cohesity Alta SaaS Protection.

For ease of use, the following service accounts are created as part of the Cohesity Alta SaaS Protection provisioning process.

- Connector service account
- Retrieval service account
- Full admin account

This information will be provided by the Cohesity Alta SaaS Protection support team during the post-provisioning call.

If you do not want to use the default service accounts, you can create your own accounts with the correct permissions as described in the Authorizations required for the service account table. If you create your own accounts, you could use the same account to run the service and connect to Cohesity Alta SaaS Protection.

Authorizations required for the service account in Cohesity Alta SaaS Protection

The service account must be authorized with the following permissions Cohesity Alta SaaS Protection:

Table 29-4 Authorizations required for the service account Cohesity Alta SaaS Protection

Services and utilities	Authorizations in Cohesity Alta SaaS Protection	Authorizations in the customer's domain
Connector service	■ API ■ Add Content.	■ Read permission. ■ Write Attributes permission.
Export service	■ API ■ API Impersonation ■ Access All Items	
Retrieval service	■ API ■ API Impersonation ■ Access All Items	
Export utility	For the administrator: ■ API ■ Access All Items For the end user: ■ End-User Retrieval ■ End-User Portal ■ Export Utility	
Apps Consent Grant utility		Global Administrator

Table 29-5 Authorizations required for the service accounts in Windows

Services and utilities	Windows Permissions when running the service
Connector service	■ **Log on as a service** permission If running a Connector for File System Archiving: ■ **Standard Read** permissions ■ **Write Attributes** permission The Write Attributes permission is required as Cohesity Alta SaaS Protection suppresses updating the Last Accessed time. ■ Write permission is also required when using the `.Hubstorinfo` file, which is enabled by default.
Export service	■ **Log on as a service** permission ■ **Modify** permissions to the export locations

Table 29-5 Authorizations required for the service accounts in Windows *(continued)*

Services and utilities	Windows Permissions when running the service
Retrieval service	■ **Log on as a service** permission ■ **Full control** permissions

To configure a service account for services and utilities

1. Open a web browser and access the Administration portal.
2. Click **Administration**.
3. On the left, expand **Permissions** > **Users and groups**.
4. Click **Refine search**.
5. In the **Refine search** window, enter the user account, and then click **Run search**.
6. Click **Manage permissions**.
7. In the **Manage permissions** window, select the required permissions for the service account and then click **Assign**.

About the Apps Consent Grant Utility

The Apps Consent Grant utility helps you grant consent to many apps at once.

For example, for some connector types, it is recommended having a minimum of 25 applications; in this case, you need to grant consent for 25 times. You can use the App Consent Grant utility to grant admin consent to these applications at once.

For the prerequisites to install services and utilities, See "Pre-requisites to download and install services and utilities" on page 345.

Downloading the Apps Consent Grant Utility

You can use the following procedure to download services and utilities.

To download the Apps Consent Grant Utility

1. Access the Administration portal.
2. On the Administration portal, click **Administration**.

3 On the left pane, click **Software download**.

The page that lists the services and utilities is displayed.

4 Click **Download**, which corresponds to the required service or utility.

The installer is downloaded to your local computer.

Installing or upgrading the Apps Consent Grant Utility

You can install and upgrade the services and utilities.

To install and upgrade the Apps Consent Grant Utility

1 Open Windows Explorer > **Downloads**.

2 Double-click the installer file.

3 Click **Run**.

4 In the ***<Setup>*** window, click **Next**.

5 Select the **I accept the terms in the License Agreement** check box.

6 Enter the credentials of the Windows account that you want to use to run this service. This account must be a domain account or a local computer account with the **Log on as a service** permission.

7 Click **Validate**.

8 Click **OK**.

9 Click **Next**.

10 If required, change the installation path.

The default installation path is **C: \Program Files(x86)\HubStor\<*Name of the service or utility*>**.

11 Click **Next**.

12 Click **Install**.

13 Click **Finish**.

Credentials not needed for service upgrades

In earlier versions, before 2.16.1 and 2.16.1, upgrading services (Connector, Export, and Retrieval services) required Windows Administrator credentials.

From the 2.16.1 release onwards, this step is no longer necessary for service upgrades.

If you change the password for the Windows Administrator between releases, you may encounter issues after upgrading to the next release. Specifically, the services

may fail to start. In such cases, you must manually update the password for the targeted service.

Prompt for .Net Framework 4.8 installation

During installation or upgrade of any service or utility for version 2.15.1, you are prompted to install the .Net Framework 4.8 on the computer.

Post-installation activities for the Apps Consent Grant Utility

The following are the post-installation activities to install and manage the Apps Consent Grant utility:

- **Install module**
  The **Az.account PowerShell** module must be installed on the Windows computer using the following command:
  ```
  Install-Module Az.Accounts -RequiredVersion 2.12.1
  ```

  Note: The version of the module must be 2.12.1 or lower with PowerShell version 5.1.

- **Assign permissions**
  You must have the following permissions:
  - Full Admin
  - Access All Items
  - API Impersonation
- **Unblock the PowerShell script**
  Unblock the PowerShell script, which is located at the following path:
  ```
  C:\Program Files (x86)\HubStor\BulkAppConsentGrantUtility
  \BulkAppConsent\Scripts\bulk_activate_apps.ps1
  ```
  On the properties window that opens, click **Unblock** > **OK**.
- **Setup policies**
  Set the execution policy as Unrestricted for both 64-bit and 32-bit PowerShell using the following command:
  ```
  Set-ExecutionPolicy Unrestricted
  ```

Chapter 30

Discovery

This chapter includes the following topics:

- About eDiscovery/searches
- Add search templates
- Add Discovery cases
- Perform ad hoc search and add data to Discovery cases
- View data in Discovery cases
- Edit Discovery cases
- DeleteDiscovery cases
- Assign Discovery cases to users

About eDiscovery/searches

The eDiscovery feature enables you to search the required data for legal and investigative needs. A Discovery case is a data organizational unit which can be created to hold the data that is searched through eDiscovery. You can perform the following tasks on the **Discovery** page of the Administration portal:

- Perform ad hoc searches.
- Save searches.
- Create templates for searches.
- Create cases.
- View an overview on the Discovery dashboard.

Elasticsearch

Cohesity Alta SaaS Protection leverages Elasticsearch to perform eDiscovery searches. Elasticsearch can be configured according to your requirements. In most cases, the default general settings are sufficient. However, if you need custom settings to handle specific scenarios contact Support.

Elasticsearch configuration reference

Limitations

- Location searches could perform poorly or fail when large folder hierarchies (65K folders or more) are involved.
- Custodian searches will not work reliably with large groups (65K principals or more).
- Wildcard queries using * and ? operators can introduce significant computational overload.

Add search templates

You can use the search templates to define the search queries which can be used across multiple searches.

See "Perform ad hoc search and add data to Discovery cases " on page 355.

To add a search template

1. Access the Administration portal.
2. Click **Discovery**.
3. On the left, click **Templates**.
4. Click **+ New template**.
5. On the **Template** page, do the following:
   - Click **+ New template**.
   - On the **Template** page, enter a name for the template.
   - Set search criteria as required.
6. Click **Create**.

Add Discovery cases

To ad Discovery cases

1. Access the Administration portal.
2. Click **Discovery**.
3. On the left, click **Cases**.
4. Click **+ New case**.
5. On the **Case** page, do the following actions:
   - Enter a name for the Discovery case.
   - Enable the **Suppress legal hold** option to stop the records from being preserved\secured on legal hold.
   - Enable the **Enhanced Case** option if you want to view analytics of the Discovery case. The **Analytics** tab are displayed on the Discovery case properties page.
     The Enhanced cases should only be used when one of the following is required:
     - Case/search dashboards
     - Case browsing on the **Content** page
     - User holds

     Note: Creating many enhanced cases requires the tenant to be scaled-up and results in incurring additional costs.
6. Click **Create**.

Perform ad hoc search and add data to Discovery cases

To perform an ad hoc search and add data to Discovery cases

1. Access the Administration portal.
2. Click **Discovery**.
3. On the left, click **Ad hoc search**.

4 On the **Search** page, set a search criteria as required, and then click **Run Search**.

For more information about search syntax refer to the following link:

Search syntax

The data that meets the search criteria is displayed on the page.

Note: You can use an existing search template by clicking the **Use template** option that usage the search criteria that are defined in the template. See "Add search templates" on page 354.

---

5 Click **Add to Case**.

6 On the **Add search to case** page, do the following:

- Enter a name for the search.
- From the **Case** dropdown list, select the required Case to add this search.
- Select one of the following options from **Search mode**.
  By default, the **One-time** option is selected. However, if the selected Discovery case is created to suppress a legal hold, then this option is not displayed. Alternatively, the **Daily** option is available to update the Discovery case on a daily basis.

7 Click **Add**.

Using contains and equal operators for ad hoc search criteria

Table 30-1

Operators	Description
contains	■ Use the full or partial name of the item. For example, to search for the file **Test data.txt**, you can use any of the following: ■ **Test data.txt** (full name). ■ **Test data** (partial name). ■ Enclose the full name in inverted commas. For example, to search for the file **Test data.txt**, you can use **"Test data.txt"**. Enclosing the search term in inverted commas limits the results if the exact text does not match. For example, **"Test data"** will not retrieve the required result.

Table 30-1 *(continued)*

Operators	Description
equal	■ Use the exact full name of the item. ■ Do not use partial names of the item. ■ Do not use inverted commas around the item name. For example, to search for the file **Test data.txt**, use **Test data.txt**. Using any of the following will not retrieve the result: ■ **"Test data.txt"** ■ **Test data** ■ **"Test data"**

View data in Discovery cases

To view data in Discovery cases

1. Open a web browser and access the Administration portal URL.
2. Click **Discovery**.
3. On the left, click **Cases**.
4. Click **Content**.

The content in the Discovery case is displayed.

Edit Discovery cases

To edit the Discovery cases

1. Open a web browser and access the Administration portal URL.
2. Click **Discovery**.
3. On the left, click **Cases**.
4. Click the required Discovery case.
5. Click **Details**.
6. Edit the name and description of the Discovery case as required, and then click **Save**.

DeleteDiscovery cases

To delete Discovery cases

1. Open a web browser and access the Administration portal URL.
2. Click **Discovery**.
3. On the left, click **Cases**.
4. Click within the row of the Discovery case that is to be deleted.
5. Click **Delete**.
6. Click **Delete** on the **Delete case** page.

Assign Discovery cases to users

To assign the Discovery cases to users

1. Open a web browser and access the Administration portal URL.
2. Click **Discovery**.
3. On the left, click **Cases**.
4. Click the required Discovery case.
5. Click **Permissions**.
6. Click **+ Assign permissions**.
7. On the **Assign permissions** page, add the users to whom to assign the Discovery case.
8. From the **Permissions** section, assign one of the following permissions, and then click **Assign**.
   - **Read**: This permission allows the user to read the particular Discovery case and view its configuration details.
   - **Modify**: This permission allows the user to modify the particular Discovery case, including the ability to add search results to it.
   - **Export Utility**: This permission allows the user to run the Export Utility in the Case mode. The user still needs to have access to the items they want to restore (they will need permissions such as Access All Items or Read Case Items).
   - **Read Case Items**: This permission allows the user to read items in the assigned Discovery case.

Chapter 31

Configure Tagging policies

This chapter includes the following topics:

- About the Tagging policy
- Add Tags
- Add/edit Tagging policies
- Adding regular expressions

About the Tagging policy

Tagging policies act as protection to prevent accidental exposure of organizational data by assigning tags to data policies. These tags function at the Hub level and are assigned upon ingestion or when content matches specified RegExs or Tagging policies. The assigned Tags outline the output behaviors for the data.

Table 31-1

Tag policy	Description
Regular expressions (RegExs)	RegExs can identify patterns representing sensitive content and associate one or more tags to determine protection behaviors. They are evaluated during Cohesity Alta SaaS Protection search indexing.
Tagging policies	Tagging policies offer a more granular way of applying Tags at the Stor level. Use Tagging policies if a particular Stor's content needs a unique level of protection that requires you to leverage Stor-level metadata in the policy definition for applying Tags.

The tags can have one or more Tag Behaviors enforced on items with the associated Tag through RegEx or Tagging policy.

Table 31-2 Tag Behavior

Tag Behavior	Description
Legal Hold	It assigns a legal hold status, which blocks any deletion.
Prevent Discovery Export	It prevents internal and external sharing and blocks access to the item by the Cohesity Alta SaaS Protection End-User portal or a stub.
Prevent User Retrieval	It blocks any user from retrieving the item, either through the Cohesity Alta SaaS Protection End-User portal or a stub, and also works to prevent sharing (both internal and external).
Prevent deletion	It blocks the user from deletion of items.

For more information on adding Tags and Tagging policies,

See "Add Tags" on page 360.

See "Add/edit Tagging policies " on page 361.

Add Tags

To add Tags

1. Open a web browser and access the Administration portal URL.

   The home page of the Administration portal is displayed.
2. Click **Tagging**.
3. On the left, click **Tags**.
4. Click **New Tag**.
5. On the **New Tag** page, do the following:
   - Enter a descriptive name for the tag.
   - Select all behaviors you want to be assigned to the Tag.

Tag Behavior	Description
Legal Hold	It assigns a legal hold status, which blocks any deletion.
Prevent Discovery Export	It blocks export of data in the in Discovery cases.

Tag Behavior	Description
Prevent User Retrieval	It blocks any end user from retrieving the item, either through the Cohesity Alta SaaS Protection End-user portal or a stub, and also works to prevent sharing (both internal and external).
Prevent deletion	It prevents deletion of data.

6 Click **Create**.

Add/edit Tagging policies

If the policy is configured to run in Production mode, the Tag is applied to all items meeting the selection criteria.

See "About the Tagging policy" on page 359.

To add/edit a Tagging policy

1 Access the Administration portal.

   The home page of the Administration portal is displayed.

2 Click **Tagging**.

3 On the left, click **Tagging policies**.

4 Do one of the following:

   - To add a new policy, click **New policy**.
   - To update existing policy, click the name of the policy.

5 On the **Create policy** page, do the following:

   - Enter a descriptive name for the policy. This name is displayed in policy dropdown lists on several pages.
   - From the **Stor name** dropdown list, select the Stor where you want to create the tier policy.
   - Select one of the following schedules to run the policy:
     - **One time**: Runs as per the policy interval settings, and then its schedule changes to **Never**.
     - **Continuous**: Runs as per the policy interval settings.
     - **Date range**: Lets you specify a **From** and **To** date range to run the policy.

- **Never**: Set this option if you are not ready to run the policy or want to stop the policy from running. The schedule of the **One time** policy is converted to **Never** after its runs.

- Select one of the following modes as required:
  - **Preview**: Lists the items for tagging.
    To ensure that you understand fully the scope of data that will be tagged, run the policy in Preview mode initially.
  - **Production**: Tags the items as per policy.
- By default, the policy is disabled; it is saved but cannot not run. Toggle the **Status** option to enable the policy.
  As soon as the policy is enabled, it runs per the schedule set in the **Schedule** section.
- Select the required tag from the dropdown list.
- Select the required retention period from the **Retention period** section. (In days, months, or years).
- (Optional) Configure filters to include or exclude specific locations or data from having the policy applied.
  See "How to add a Location filter?" on page 237.
  See "How to add a filter?" on page 238.
- Click **Create** to add a policy or click **Update** to save the changes.

The policies are displayed on the **Tagging policies** page under the Stor for which you have added the policy.

See "How to edit the policy evaluation interval?" on page 237.

Adding regular expressions

Unlike Tagging policies which are deployed per Stor, RegExs are deployed globally at the Hub level and are applied across all Stors those are PII enabled.

To add regular expressions

1. Open a web browser and access the Administration portal URL.

   The home page of the Administration portal is displayed.
2. Click **Tagging**.
3. On the left, click **Regular expressions**.
4. Click **New Regular expressions**.

5 On the **Update Regular expressions** page, enter the following details:

Single Term Regexp	Lets you compose a regular expression that will work against a single term (For example, 4543934039222343).
Query String	Lets your query for strings, supports wildcards, and so on. It operates on individual words.
Advanced Elastic Search Query	Allows a raw query to be composed. Here you can use span_near to provide matching over multiple terms (for example, credit card numbers with dashes or spaces).

6 Select the required output tag from the drop-down list.

7 Click **Create**.

The RegEx is now active and will be evaluated during the next policy interval with the same scope as your indexing policies.

RegEx and query examples for PII detection

Use the following examples to query data.

Table 31-3 RegEx and query examples for PII detection

Data	Use RegEx type:
To find MasterCard numbers without spaces (for example, 5500000000000004)	Single Term Regexp
To find MasterCard numbers that might have spaces or dashes (for example, 5500 0000 0000 0004)	Advanced ElasticSearch Query `"clauses": [{ "span_multi": { "match" : { "regexp": { "blob.content": "5[1-5][0-9]{2}" } } } }, { "span_multi": { "match" : { "regexp": { "blob.content": "[0-9]{4}" } } } }, { "span_multi": { "match" : { "regexp": { "blob.content": "[0-9]{4}" } } } }, { "span_multi": { "match" : { "regexp": { "blob.content": "[0-9]{4}" } } } }], "slop": 0, "in_order": true } }`
To find Visa numbers without spaces (for example, 4111111111111111),	Single Term Regexp 4[0-9]{15}

Table 31-3 RegEx and query examples for PII detection *(continued)*

Data	Use RegEx type:
To find the Visa numbers that might have spaces or dashes (for example, 4111-1111-1111-1111)	Advanced ElasticSearch Query `{"regexp":{"attachment.content":"4[0-9]{3}[ ]?[0-9]{4}[ ]?[0-9]{4}[ ]?[0-9]{4}|4[0-9]{3}[-]?[0-9]{4}[-]?[0-9]{4}[-]?[0-9]{4}"}}`
To find American Express numbers without spaces (for example, 340000000000009)	Single Term Regexp
To find the American Express numbers that might have spaces or dashes (for example, 3400 0000 0000 009)	Advanced ElasticSearch Query `{"regexp":{"attachment.content":"3[47][0-9][ ]?[0-9]{6}[ ]?[0-9]{6}|3[47][0-9][-]?[0-9]{6}[-]?[0-9]{6}"}}{`
To find the United States Social Security Network (SSN)	Advanced ElasticSearch Query `{"regexp": {"attachment.content": "~(000|666)[0-8][0-9]{2}[-]?~(00)[0-9]{2}[- ]?~(0000)[0-9]{4}"}}{`
To find content with particular text\phrase (for example, Good Admin)	Query String 'Good Admin'

Chapter 32

Configure Tiering policy

This chapter includes the following topics:

- About the Tiering policy
- Add/edit Tiering policies

About the Tiering policy

You can use the following types of tiers on the storage (Stors):

Table 32-1

Tier types	Usage	Storage cost	Access cost
Hot tier	Frequently accessed or modified. Designed for data needing immediate access and frequent modifications.	Higher than Cool and Archive tiers	Lower than Cool and Archive tiers

Table 32-1 *(continued)*

Tier types	Usage	Storage cost	Access cost
Cool tier	Infrequently accessed or modified data is ideal for storage in the Cool tier. This type of data may not require immediate access but should still be accessible. The data that is stored in the Cool tier should be kept for at least 30 days; otherwise, Microsoft charges a prorated penalty. Cohesity recommends using the Cool storage for the workloads that have occasional retrieval activity.	Lower than Hot and Archive tiers	Higher than Hot tiers

Table 32-1 *(continued)*

Tier types	Usage	Storage cost	Access cost
Archive tier	Data that is not frequently accessed and needs to be stored for long-term retention can be stored in the Archive tier. The retrieval times may be longer. The data in the Archive tier should be stored for at least 180 days, or Microsoft charges you a prorated penalty. While you can view the content in Cohesity Alta SaaS Protection, it may take several hours to be fully retrieved and available. Initiating a request to access data on this tier starts the rehydration process.	Lower than Cool and Hot tiers	Higher than Cool and Hot tiers

The data that is stored in the Hot or Cool tiers can be retrieved instantly. The data that is stored in the Archive tier may take several hours to be available for retrieval. For more detailed information about blob storage operations and pricing, refer to the following knowledge base article:

Access tiers for blob data

See "Add/edit Tiering policies" on page 368.

Storage tiering and full-text search

Cohesity Alta SaaS Protection search cluster can perform full-text indexing of content, item-level metadata, folders, and access rights. This indexing enables the searchability of all data based on metadata.

Initially, data chosen for the Cool or Archive tiers is stored on the Hot tier to reduce access and transaction charges. This placement facilitates tasks like full-text search, data classification, and using Microsoft Cognitive Services.

Data accessed from the Cool tier remains in the same tier and is not recalled to the Hot tier. Accessing data from the Archive tier first needs to be changed to the Hot or Cool tier from the archive. The Read operations on the Cool tier may incur higher costs. Also, changing the tier, also called rehydration, involves additional Azure costs. Once data is indexed, it remains searchable regardless of the storage tier. To avoid early deletion fees from Azure, it's recommended to maintain data on the Cool tier for a minimum of 30 days and 180 days for the Archive tier.

User experience on storage tiering

The storage tiering system has three tiers - Hot, Cool, and Archive. The Hot tier stores frequently access that content that needs to be readily available. The Cool tier stores less regularly accessed content but still needs to be easily accessible. From a user's perspective, the data that is stored in the Cool tier is similar to the data that is stored in the Hot tier. The Archive tier is designated for data tolerating retrieval latencies of up to 15 hours or more. When you design an Archive tier policy, you should select the content that does not require timely access and does not have stubs.

Priority for storage Tiering

In Cohesity Alta SaaS Protection, the storage Tiering priority is organized in the following order: Hot Tier, Cool Tier, and Archive Tier. This means that the Hot Tier is given the highest priority, followed by the Cool and Archive Tiers. For example, if overlapping policies select the same data for Cool or Archive Tierings, the data is directed to the Cool Tier. The warmer Tier (Hot Tier) always takes precedence in such cases. The Stors that have Storage tiering settings overrides the tiering to the Archive Tier. These settings are based on the last accessed or captured configuration.

Add/edit Tiering policies

See “About the Tiering policy ” on page 365.

To add/edit a Tiering policy

1. Access the Administration portal.

   The home page of the Administration portal is displayed.

2. Click **Tiering**.

3 On the left, click **Cool storage tier policies** or **Archive storage tier policies** as required.

Cool tier	Cool tier is an online tier optimized for storing the data that is infrequently accessed. Data in the Cool tier should be stored for a minimum of 30 days. The Cool tier has lower storage costs and higher access costs as compared to the Hot tier.
Archive tier	Archive tier is an offline tier optimized for storing the data that is not accessed frequently and that has flexible latency requirements on the order of hours. Data in the Archive tier should be stored for a minimum of 180 days.

4 Do any of the following:

- To add a new policy, click **New policy**.
- To update existing policy, click the name of the policy.

5 On the **Create policy** page, do the following:

- Enter a descriptive name for the policy. This name is displayed in policy dropdown lists on several pages.
- From the **Stor name** dropdown list, select the Stor where you want to create the tier policy.
- Select any of the following schedules to run the policy:
  - **One time**: Runs once as per the policy interval settings, and then its schedule gets changed to **Never**.
  - **Continuous**: Runs as per the policy interval settings.
  - **Date range**: Lets you specify a **From** and **To** date range to run the policy.
  - **Never**: Set this option if you are not ready to run the policy or want to stop the policy from running. The **One time scheduled policies** gets converted to **Never** after its runs.
- Select any of the following modes as required:
  - **Preview**: Lists the items for tiering.
    To ensure that you understand fully the scope of data that will be tiered, run the policy in Preview mode initially.
  - **Production**: Retains the items as per policy.
- By default, the status of the policy is disabled; it is saved but cannot not run. Toggle the **Status** option to enable the policy.

As soon as the policy is enabled, it runs as per the schedule set in the **Schedule** section.

- (Optional) Configure filters to include or exclude specific locations or data from having the policy applied.
  See "How to add a Location filter?" on page 237.
  See "How to add a filter?" on page 238.
- Click **Create** to add a policy or click **Update** to save the changes.

For Cool tier policies, it can be useful to add a clause for **Archived At** while adding a filter. It is the date the file was uploaded to Cohesity Alta SaaS Protection. The default or older than one month is typically sufficient as it ensures that the data has time for any post-processing, such as full-text indexing; while on the Hot tier where the data has the lowest access costs.

Archive tier policies automatically exclude data based on the Stors storage tiering settings for the last accessed and items captured in the last N days. The policy runs according to the Policy Evaluation Interval for the selected Stor.

Warning: Removing a Cool or Archive tier policy causes the data to be moved back to the Hot tier unless there is an overlapping Cool or Archive tier policy. Unwanted access and transaction costs incur and also could charge deletion costs if the data hasn't been on the tier long enough.

See "How to add a Location filter?" on page 237.

See "How to add a filter?" on page 238.

See "How to edit the policy evaluation interval?" on page 237.

Chapter 33

Auditing

This chapter includes the following topics:

- Auditing

Auditing

All user activity within Cohesity Alta SaaS Protection is audited to maintain a comprehensive history of user actions. This includes activities by end users, such as retrieval and sharing, and system activities involving data manipulation, like deletions. Administrative actions, such as modifying configuration settings or managing policies, are also tracked. Additionally, actions performed by privileged users in Cohesity Alta SaaS Protection data governance applications, such as removing legal holds in discovery cases, are audited. Activity intelligence data can be filtered by date ranges, locations, users, and groups and can be exported at any time for further analysis.

Table 33-1 Auditing categories

Pages	Description
Activities page	All the activities that the Administrator and the privileged users perform on the Administration portal are displayed on this page. The page lists the events with its time of occurrence, user, event type, and other details.
Item actions page	All system-related activities, such as Personally Identifiable Information (PII) detection, indexing, and retention errors are displayed on this page.
Data retrievals page	All data retrieval activities internal and external users performs, are displayed on the page.

Table 33-1 Auditing categories *(continued)*

Pages	Description
Sharing page	All sharing activities users perform internally or externally, are displayed on the page.

The **Export as CSV** option on each page lets you export the list of event logs to the CSV format.

The **Refine search** option on each page lets you perform an advanced search for the required event. It opens the page within the main page. On the **Search** section, set the required search criteria based on time range, Stor type, Discovery case, or user.

Chapter 34

Manage Stors (Storages)

This chapter includes the following topics:

- Viewing Stors (Storages)
- Requesting a new Stor
- General tab
- Version control settings
- Metadata tab
- Statistical policies tab
- Location-Mapping tab
- Backup tab
- Custodian Groups tab
- Advanced tab
- Analytics tab

Viewing Stors (Storages)

To view Stors (Storages)

1. Open a web browser and access the Administration portal URL.

   The home page of the Administration portal is displayed.

2. Click **Administration**.

3 On the left, click **Storage**.

The **Storage** page lists all the sites that are configured for your tenant and also the Stors that are configured for these StorSites.

4 Click the required StorSite to view the details such as the **StorSite name**, its **State**, **Region**, **Web service URL**, **Size**, and the list of Stors that are configured for this StorSite.

5 Click the required Stor to view its details.

Requesting a new Stor

To request a new Stor

1 Open a web browser and access the Administration portal URL.

The home page of the Administration portal is displayed.

2 Click **Administration**.

3 On the left, click **Storage** > ***<StorSite>***.

4 Click **+ Request new Stor**.

5 On the **Request new Stor** page, enter a name for the Stor, your contact information, and other details.

6 Click **Send request**.

General tab

The **General** tab displays the following options:

Table 34-1 General tab options

Fields	Description
Basic settings	
Stor name	Displays the name of the Stor.
Stor type	Displays the type of the Stor.

Table 34-1 General tab options *(continued)*

Fields	Description	
State	Displays one of the following states of the Stor:	
	Not Provisioned	■ The Stor is created but not provisioned yet. ■ The StorDB and Azure containers for the Stor do not exist. ■ A Stor in this state is not usable; you cannot configure policies. ■ You can configure only limited settings.
	Provisioned	■ The Stor is created and provisioned. ■ The StorDB and Azure containers exist. ■ A Stor in this state is not usable; you cannot configure policies. ■ You can configure only limited settings.
	Online	■ The Stor is created, provisioned. ■ A Stor in this state is available for writing and reading. ■ You can configure only limited settings.
	Online ReadOnly	■ The Stor is created and provisioned. ■ A Stor in this state is available only for reading the existing content. ■ You can configure limited settings only.
Size	Displays the size of the Stor that is same as the total size of the Blob.	
Options		
PII	Select the check box to enable Personal Identifiable Information (PII) detection. If PII is enabled, the Stor is evaluated according to the policy interval and the content indexing scope.	
Versioning	Select the check box to enable file versioning for the Stor.	
Encrypt data at	Select the check box to encrypt the data at rest. **Note:** Data in the rest is the data that is stored for later use.	
Support storage tiering	Select the check box to support the storage tierings for the Stor.	

Table 34-1 General tab options *(continued)*

Fields	Description
Support pre-ingest encryption	Select the check box if the Stor supports pre-ingest encryption. The **PreIngestEncrypted** metadata field is added to the Stor. **Note:** If the pre-ingested encryption is enabled, the data in any Blobs gets decrypted during the export.
Hide from End-User Portal	Select the check box to hide the Stor from the End-User portal.
Stor-level WORM	Select the check box to enable Stor-level WORM for the Stor. Stor-level WORM provides a single WORM retention period for all content in the Stor. This setting is optionally configured on a Stor at the time of provisioning the Stor. Before performing the process of provisioning, you are required to discuss with the Cohesity Alta SaaS Protection technical support team. After a Stor is provisioned in WORM mode, the settings cannot be changed. Specify a retention period for WORM. The specified WORM retention protection is applied to all data that is archived in the Stor. After the WORM retention period is completed, the content is deleted.
Item-level WORM	Select the check box to enable Item-level WORM for the Stor. Item-level WORM supports one or more WORM retention periods on the Stor. Item-level WORM retention periods are driven by the document-level policies that are run in real time during the write process. Multiple item-level WORM policies can be used within a Stor. The setting for item-level WORM is configured on the Stor at the time of provisioning the Stor, the settings cannot be modified.
Blob replication settings	

Table 34-1 General tab options *(continued)*

Fields	Description
Locally Redundant Storage (LRS)	Select this option to enable Locally Redundant Storage for the Stor. LRS is the default Blob replication configuration that Cohesity Alta SaaS Protection provides. Three synchronous copies of the data are maintained in a single datacenter. LRS replicates the data within the region of the customer. To maximize durability, every request that is made for the content is replicated thrice. These three replicas are each placed in Fault Domains (FD) and Upgrade Domains (UD). The three replicas are spread across UDs and FDs to ensure that data is available even if hardware failure affects a single rack or when nodes are upgraded during a rollout.
Geo Redundant Storage (GRS)	Select this option to enable Geo Redundant Storage for the Stor. Six copies of the data are made (three synchronous copies in one datacenter + three asynchronous copies in a second datacenter). GRS replicates the data to a secondary region that is hundreds of miles away from the primary region. The data is durable even in the case of a complete regional outage or a disaster in which the primary region is not recoverable. An update is first committed to the primary region, where it is replicated three times. Then the update is replicated to the secondary region, where it is also replicated three times, across separate FDs and UDs.
Read-Access Geo Redundant Storage (RAVersion control settings -GRS)	Select this option to enable Read-Access Geo Redundant Storage for the Stor. Six copies are replicated to a second datacenter. RA-GRS maximizes availability for the storage account, by providing read-only access to the data in the secondary location, in addition to the replication across two regions that are provided by GRS. If data becomes unavailable in the primary region, the application can read data from the secondary region.
Version control settings	For more details, refer to the following topic: See “Version control settings” on page 378.

Table 34-1 General tab options *(continued)*

Fields	Description
Policy evaluation interval in minutes	Displays an interval to auto-run the policies defined for this Stor. By default, it is 15 minutes. You can edit the values as required. **Note:** Each Stor have its policy evaluation interval setting. Stor that contain data, which is accessed rarely may not need frequent policy evaluation. Stor that contain data, which is accessed actively by users and has indexing, and security requirements may need a policy evaluation interval to ensure policies run closer to real time.
Policy evaluation last ran	Displays the time when the policy evaluation was last run.

Version control settings

This feature lets you gradually reduce the number of backed up versions over time to optimize storage within Cohesity Alta SaaS Protection.

By default, all versions are retained in Cohesity Alta SaaS Protection unless you enable the Version control feature.

Version control feature optimizes backup storage by keeping only the most relevant backed up versions and removing older, redundant ones.

Retention settings

The following retention settings are used to configure this feature for the selected Stor:

Enable this feature

You must click this option to enable the version control feature.

Once this feature is enabled and the configuration is saved, it cannot be disabled. Also, the following default settings can only be edited once.

Table 34-2

Settings	Time period	Pruning action	Retention strategy
Keep all versions for [14] days:	First 14 Days	No pruning occurs.	All newly added versions are retained.

Table 34-2 *(continued)*

Settings	Time period	Pruning action	Retention strategy
Then reduce to one daily version for the next [90] days:	Day 15 to Day 105 (Next 90 Days)	Pruning starts; scans from feature enablement date.	Only one daily version is retained.
Then reduce to one weekly version for the next [52] weeks:	Day 106 to Week 52 (Next 52 Weeks)	Further pruning occurs.	Only one weekly version is retained.
Then reduce to one monthly version for the next [240] months:	After 52 Weeks to 240 Months	Final pruning phase.	Only one monthly version is retained for long-term storage.

After 240 months, for versions beyond all retention periods (daily, weekly, and monthly), only the latest version will be retained, and all other versions will be pruned based on the last modified date.

Starting from Cohesity Alta SaaS Protection version 2.36.2, version pruning for versions beyond all retention periods is disabled for SharePoint Online.

Note: For each time period, the backed-up version retained depends on whether the Stor supports versionings at the source. In Cohesity Alta SaaS Protection, SharePoint and Box are the two Stors that can have backed up items which are versioned at source. For example, a SharePoint Stor can have backup copies all versions of an item that are also present in a SharePoint Document Library that supports versioning.

- **Items that are not versioned at the source**: For a given time period, the most recent backed-up version (based on the archived time) is retained, and the rest are pruned.
  Example: From day 15 to day 105, when only one version is retained per day, the most recent backed-up version from all item modifications on that day is retained.
- **Items that are versioned at the source**: For a given time period, the version with the highest version number, as per the source, is retained, and the rest are pruned.
  Example: From day 15 to day 105, when only one version is retained per day, the version with the highest version number from all item modifications on that day is retained.

SharePoint scenario: If a file in a versioned SharePoint Document Library was modified three times in a day, creating versions 8, 7, and 6, and all these versions were backed up, the Version Control feature in Cohesity Alta SaaS Protection will retain only version 8 for that day.

This behavior applies from the Cohesity Alta SaaS Protection 2.36.2 release.

Note: For SharePoint, for a given time period, if the version to be considered for retention is less than 1 KB, pruning action is not done for all the versions in that batch for the item, when executing the retention strategy. This behavior is applicable from 2.36.2.

Note: If a file is modified multiple times within the same day and the most recent changes occur within a span of a minute, Cohesity Alta SaaS Protection may retain any one of those versions. This behavior is applicable for any version control behavior before the Cohesity Alta SaaS Protection 2.36.2 release.

Metadata tab

You can view the fields that are included for the Stor. You can also customize the metadata by requesting Cohesity Support.

Table 34-3 Metadata tab

Fields	Description
Item Version Metadata Fields	This option is configured with a metadata definition based on the content that will be archived to the Stor. These fields are defined during provisioning using Cohesity Alta SaaS Protection templates (Email, SharePoint, Files, and so on). Once the tenant is provisioned, fields cannot be removed, and their settings cannot be easily changed. As well, new fields cannot be easily added to the Stor after it is provisioned.
Advanced Database Indexes	Based on the selection criteria in your policies, you may find that certain fields are commonly leveraged together in a policy. Cohesity Alta SaaS Protection makes it easy to create database indexes to enhance query performance for faster and more efficient policy execution. Any configuration of database indexes is performed in consultation with Cohesity Support.

Statistical policies tab

Policies can be very useful if you want specific analytics within Cohesity Alta SaaS Protection. You can set them to run once, continuously, or for a specific date range. Policies are built using clauses to filter the data selection. When a policy is created and processed by the internal policy update, it can be viewed in the analytics dashboard.

Once a policy has run, if it's not scheduled to run again, the run mode well be set to **None**. That is an indication that your policy has run.

Location-Mapping tab

Content can be replicated virtually to additional locations within a Stor using Location mapping policies. Based on user attributes (such as OU or department), data flowing into a Stor can be replicated in the presentation layer to other locations.

Note: Location Mapping applies to data when added to Cohesity Alta SaaS Protection. It is not retroactively applied to data.

Backup tab

The Cohesity Alta SaaS Protection Backup destination option supports recovery and failover. Customers with the appropriate license model or SKU can choose to add backup destinations for their data storage.

When backup is enabled, it serves as a safeguard for your data against rogue administrators. Also, it can be used as an alternative to GRS or RA-GRS replication, especially if the secondary storage is hosted in a different Azure region.

The supported storage types are,

- Azure Blob Storage Container
- AWS S3 Bucket
- AWS S3 Bucket on-premises

Required information for the backup destinations:

- Azure Blob Storage Container
  - Azure Storage Connection String
- AWS S3 Bucket
  - AWS Region

  - Access key ID
  - Secret access key
  - Bucket Name
- AWS S3 Bucket on-premises
  - Endpoint URL
  - Access key ID
  - Secret access key
  - Bucket Name
- Blob Tiering Mode: You have the option to:
  - Use the current tier of the storage account.
  - Use the Archive tier for Azure or Glacier for AWS (not applicable for S3 Bucket on-premises)
- Deletion Propagation Mode provides the customer with the following options:
  - **None**: Never replicate deletions to the backup destination.
  - **Delayed**: Delay deletions by **N** days (allowing for a period of time to discover any malicious or accidental deletion).
  - **Immediately**: Immediately replicate deletions.

Custodian Groups tab

If this option is enabled, Custodian Groups allow multi-tenancy within the Hub. Users belonging to one or more Custodian Groups can only view Stors that are enabled for their group. Custodian groups are set up in COPS by Cohesity Alta SaaS Protection support when requested by a customer. Some resellers use Custodian Groups to provide a multi-tenant option to customers that are too small to justify their own tenant.

Advanced tab

You are required to configure the following options:

Table 34-4 Advanced tab options

Fields	Description
Storage tiering settings	

Table 34-4 Advanced tab options *(continued)*

Fields	Description
Exclude items accessed in last -- months from Archive Tier	Specify the range in which the items that are accessed should be excluded from the archive tier. The default value is 1 month.
Exclude items captured in last -- days from Archive Tier	Specify the range in which the items that are captured should be excluded from the archive tier. It is used to ensure that the content is indexed before tiered. The default value is 14 days.
End-User Portal settings	
Limit End-User Portal 'My content' to Mailbox/OneDrive owner	This option is applicable only for SharePoint's OneDrive and Exchange mailbox content. Select the check box to show only locations on **My Content** of the End-User portal of the user's OneDrive or mailbox.
Visible End-User Portal grid columns	The selected columns are displayed on the End-User portal on the **My Content** page.
Hidden End-User Portal fields	The selected fields that are hidden from the End-User portal.
Hidden End-User Portal locations	Add the locations that you want to hide from the End-User portal.
Permit Anonymous Shares	Select the check box to allow anonymous (link-based) shares to be created on the Stor.
Accepted SMTP Domains	The list of domains that are accepted for SMTP principal identifiers. Any ACEs that are submitted for domains not in this list are removed automatically during ingestion. If the value is empty, no SMTP domain restriction is applied, and all ACEs will be accepted.

Analytics tab

The **Analytics** tab displays the total size and the number of items in:

- Stors
- Legal hold
- Full text indexed

- Tagged

The different graphs on the page are described in the following table:

Table 34-5 Graphs on the Analytics page

Graphs	To know...
Data volume by size	The volume of the data on the Stor by the item's sizes.
Data volume by item version	The volume of the data on the Stor by the item's versions.
Breakdown by content type	The breakdown of the content in Stor as per the items' sizes.
Storage tiering	The spread of the items as per its sizes or counts in the Hot, Cool, or Archive tiers.
History	The timeline of data ingestion to the Stor based on either items' size or items' count. You can adjust the timeline as required using the bar given within the graph action.
Hover the mouse on any graph to get the details in percentage.	