Relativity aiR

Collect

October 12, 2026

For the most recent version of this document, visit our **documentation website**.

Table of Contents

1 Collect **13**

1.1 Data sources 13

1.2 Commercial and Government support 14

2 Installing Collect **14**

2.1 System requirements for Collect 14

2.2 Installing Collect 15

2.2.1 Installing Collect from the application library 15

2.3 Permissions to run Collect 16

2.4 Uninstalling the application 17

3 Matters **17**

3.1 Creating a matter 18

3.2 Matter Details layout fields 18

3.3 Viewing or editing matter details 18

4 Custodian targets **19**

4.1 Custodians 19

4.2 Fields 20

4.3 Creating a custodian target 20

4.3.1 Generating targets in the wizard 21

4.4 Removing custodian targets 21

5 Data sources **21**

5.1 Creating a collect data source 22

5.1.1 Third-party vendor 22

5.2 Data source types 22

6 Bloomberg chats and emails data source **24**

6.1 Consideration 24

6.2 Collection size 24

6.3 Creating the data source instance 25

6.4 Settings fields 25

6.5 Configuring the data source 25

6.5.1 Bloomberg chat 26

6.5.2 Bloomberg email 26

7 Box data source **26**

7.1 Collection size ... 27
7.2 Task checklist ... 27
7.3 Box application setup ... 27
7.3.1 Creating an application with Box ... 27
7.3.2 Authorizing an application ... 28
7.4 Creating the data source instance in Collect ... 28
7.5 Settings fields ... 29
7.5.1 Data source details ... 29
7.6 Configuring the data source in Collect ... 29
8 Cellebrite data source ... 30
8.1 Considerations ... 30
8.2 Prerequisites ... 31
8.3 Collection size ... 31
8.4 Task checklist ... 31
8.4.1 Support resources ... 32
8.5 Create the OAuth2 Client ... 32
8.6 Set permissions in Relativity aiR ... 32
8.7 Connect Cellebrite to Relativity aiR ... 32
8.8 Generate API key for Cellebrite data source ... 33
8.9 Create the data source in Relativity aiR ... 33
8.9.1 Settings fields ... 34
8.10 Create entities in Relativity aiR ... 34
8.11 Create a Collect job in Relativity aiR ... 34
8.12 Mobile data collection results ... 34
8.13 Troubleshooting ... 35
9 ChatGPT Enterprise data source ... 36
9.1 Considerations ... 36
9.2 Prerequisites ... 37
9.3 Collection size ... 37
9.4 Collected metadata ... 37
9.5 Creating the data source ... 38
9.6 Settings fields ... 38
9.7 Configuring the data source ... 39
10 Claude ... 39

10.1 Considerations ... 40
10.2 Prerequisites ... 40
10.3 Collected data ... 40
10.3.1 Collected metadata ... 41
10.3.2 Retention expectations and data availability ... 41
10.4 Creating the data source ... 41
10.5 Settings fields ... 42
10.6 Configuring the data source ... 42
11 Google ... 43
11.1 Google Workspace account setup ... 44
11.1.1 Create a Google Cloud project ... 44
11.1.2 Enable required APIs for the project ... 44
11.1.3 Set up OAuth2 consent screen ... 45
11.1.4 Add scopes ... 45
11.1.5 Create credentials ... 46
11.1.6 Set reauthentication policy ... 48
11.2 Google Workspace user account setup ... 48
11.2.1 Create admin role for Vault API ... 48
11.2.2 Create admin role for the user accounts listing ... 49
11.2.3 Create admin role for the groups listing ... 49
11.2.4 Enable required privileges ... 49
11.3 Restricting collections to the selected user accounts ... 50
11.3.1 Create an organizational unit ... 50
11.3.2 Add users to the organization unit ... 50
11.3.3 Scope user privileges to the organizational unit ... 51
11.4 Google data sources ... 51
12 Google Workspace data source ... 51
12.1 Considerations ... 51
12.1.1 Grouped collection ... 52
12.2 Collection size ... 52
12.2.1 Chat ... 52
12.2.2 Drive ... 52
12.2.3 Gmail ... 52
12.2.4 Groups ... 53

12.3 Create the data source in Collect ... 53
12.4 Configure the data source in Collect ... 54
12.4.1 Google Groups ... 55
12.4.2 Gmail ... 56
12.4.3 Google Drive ... 59
12.4.4 Google Chat ... 60
12.5 Troubleshooting ... 61
13 Google Gemini data source ... 61
13.1 Considerations ... 62
13.2 Advanced Gemini features ... 62
13.3 Prerequisites ... 62
13.4 Collection size ... 63
13.5 Create the data source ... 63
13.5.1 Settings fields ... 64
13.6 Configure the data source in Collect ... 64
14 iManage data source ... 65
14.1 Considerations ... 65
14.2 Prerequisites ... 65
14.3 Collection size ... 66
14.4 Task checklist ... 66
14.5 Setting up Relativity Collect in iManage ... 66
14.5.1 Permissions ... 67
14.5.2 Throttling ... 67
14.6 Creating the data source in Collect ... 67
14.7 Settings fields ... 68
14.7.1 Data source details ... 68
14.8 Configuring the data source in Collect ... 68
15 Microsoft 365 - Inactive mailboxes data source ... 71
15.1 Considerations ... 71
15.2 Collection size ... 72
15.2.1 Export duration for large mailboxes ... 72
15.3 Task checklist ... 72
15.4 Accessing Microsoft 365 tenants ... 73
15.4.1 Registering the Collect application ... 73

15.4.2 Obtaining a client secret ... 74
15.4.3 Setting API permissions ... 74
15.5 Adding a redirect URI ... 75
15.6 Finding Azure credentials ... 76
15.7 Limiting application registration access to accounts ... 76
15.8 Revoking application access ... 76
15.8.1 Revoking access via Azure Portal ... 76
15.8.2 Revoking access via Powershell ... 77
15.9 Creating the data source in Collect ... 77
15.10 Settings fields ... 78
15.10.1 Data source details ... 78
15.11 Configuring the data source in Collect ... 78
15.11.1 Data source criteria ... 78
15.11.2 Criteria ... 79
16 Microsoft 365 - Inactive OneDrive data source ... 79
16.1 Considerations ... 79
16.2 Collection size ... 80
16.3 Inactive OneDrive data ... 80
16.4 Task checklist ... 80
16.5 Accessing Microsoft 365 tenants ... 81
16.5.1 Registering the Collect application ... 81
16.5.2 Obtaining a client secret ... 82
16.5.3 Setting API permissions ... 83
16.6 Adding a redirect URI ... 83
16.7 Finding Azure credentials ... 84
16.8 Limiting application registration access to accounts ... 84
16.9 Revoking application access ... 84
16.9.1 Revoking access via Azure Portal ... 84
16.9.2 Revoking access via Powershell ... 85
16.10 Creating the data source in Collect ... 85
16.11 Settings fields ... 86
16.11.1 Data source details ... 86
16.12 Configuring the data source in Collect ... 86
16.12.1 Data source criteria ... 86

16.12.2 Criteria ... 86
16.13 Troubleshooting ... 88
17 Microsoft 365 - Mailboxes data source ... 88
17.1 Considerations ... 88
17.1.1 API and connector ... 88
17.1.2 Purview case ... 89
17.1.3 Preserved files ... 89
17.1.4 Requirements and limitations ... 89
17.2 Collection size ... 89
17.2.1 Export duration for large mailboxes ... 89
17.2.2 Phase 2: Data transfer ... 90
17.3 Accessing Microsoft 365 tenants ... 90
17.3.1 Registering the Collect application ... 90
17.3.2 Obtaining a client secret ... 91
17.3.3 Setting API permissions ... 92
17.4 Adding a redirect URI ... 93
17.5 Finding Azure credentials ... 93
17.6 Limiting application registration access to accounts ... 94
17.7 Revoking application access ... 94
17.7.1 Revoking access via Azure Portal ... 94
17.7.2 Revoking access via Powershell ... 94
17.8 Creating the data source in Collect ... 94
17.8.1 Data source details ... 95
17.9 Configuring the data source in Collect ... 96
17.9.1 Data source criteria ... 96
17.9.2 Criteria ... 96
18 Microsoft 365 - OneDrive data source ... 97
18.1 Considerations ... 97
18.2 Collection size ... 97
18.3 Task checklist ... 97
18.4 Accessing Microsoft 365 tenants ... 98
18.4.1 Registering the Collect application ... 98
18.4.2 Obtaining a client secret ... 99
18.4.3 Setting API permissions ... 99

18.5 Finding Azure credentials ... 101
18.6 Revoking application access ... 102
18.6.1 Revoking access via Azure Portal ... 102
18.6.2 Revoking access via Powershell ... 102
18.7 Creating the data source in Collect ... 103
18.8 Settings fields ... 103
18.8.1 Data source details ... 103
18.9 Configuring the data source in Collect ... 103
18.9.1 Data source criteria ... 104
18.9.2 Collecting preserved files ... 105
19 Microsoft 365 - Outlook data source ... 105
19.1 Considerations ... 106
19.1.1 Mailbox types and required permissions ... 106
19.1.2 Search and pre-collection filtering ... 106
19.1.3 Data source capabilities and limits ... 106
19.1.4 Government cloud and environment considerations ... 107
19.1.5 Network access and IP restrictions ... 107
19.2 Collection size ... 107
19.2.1 Mailbox ... 107
19.2.2 Calendar ... 107
19.3 Task checklist ... 108
19.4 Accessing Microsoft 365 tenants ... 108
19.4.1 Registering the Collect application ... 108
19.4.2 Obtaining a client secret ... 109
19.4.3 Setting API permissions ... 110
19.5 Finding Azure credentials ... 112
19.6 Limiting application registration access to accounts ... 113
19.7 Revoking application access ... 113
19.7.1 Revoking access via Azure Portal ... 113
19.7.2 Revoking access via Powershell ... 113
19.8 Creating the data source in Collect ... 114
19.9 Settings fields ... 114
19.9.1 Data source details ... 114
19.10 Configuring the data source in Collect ... 115

19.10.1 Data source criteria ... 115
19.10.2 Criteria ... 115
19.11 Collecting preserved files ... 119
19.12 Viewing collected data ... 119
19.12.1 File names for Outlook email ... 119
19.12.2 Files names on a preservation hold ... 119
19.12.3 Email considerations ... 120
19.13 Troubleshooting ... 120
20 Role-based access control ... 121
20.1 Azure application permissions ... 121
20.2 Prerequisites ... 121
20.3 Permission architecture ... 121
20.4 Permissions assigned directly to the Azure App ... 121
20.4.1 Permissions assigned with RBAC (Mailbox-Scoped) ... 122
20.5 Configuration steps ... 122
20.5.1 Connect to Exchange Online PowerShell ... 122
20.5.2 Create a Service Principal in Exchange Online ... 123
20.5.3 Create a Management scope for custodians ... 124
20.5.4 Assign permissions to custodians ... 124
20.5.5 Verify the configuration ... 125
20.6 Troubleshooting ... 125
20.6.1 Application can still access unscoped mailboxes ... 125
20.6.2 Test-ServicePrincipalAuthorization shows no permissions ... 125
20.6.3 PowerShell commands return an error or unexpected results ... 126
20.6.4 macOS: zsh: command not found ... 126
21 Microsoft 365 - SharePoint data source ... 126
21.1 Considerations ... 126
21.2 Collection size ... 126
21.3 Task checklist ... 127
21.4 Accessing Microsoft 365 tenants ... 127
21.4.1 Registering the Collect application ... 127
21.4.2 Obtaining a client secret ... 128
21.4.3 Setting API permissions ... 129
21.5 Finding Azure credentials ... 131

21.6 Revoking application access ... 131
21.6.1 Revoking access via Azure Portal ... 131
21.6.2 Revoking access via Powershell ... 132
21.7 Creating the data source in Collect ... 132
21.7.1 Settings fields ... 132
21.7.2 Data source details ... 133
21.8 Configuring the data source in Collect ... 133
21.8.1 Data source criteria ... 133
21.8.2 Collecting preserved files ... 134
21.9 Troubleshooting ... 134
22 Microsoft 365 - Teams data source ... 134
22.1 Considerations ... 134
22.1.1 Grouped collection ... 135
22.1.2 Attachments and linked cloud files ... 135
22.1.3 Collection size ... 135
22.2 Task checklist ... 135
22.3 Accessing Microsoft 365 tenants ... 136
22.3.1 Licensing requirements ... 136
22.3.2 Registering the Collect application ... 136
22.3.3 Obtaining a client secret ... 137
22.3.4 Setting API permissions ... 138
22.4 Finding Azure credentials ... 140
22.5 Revoking application access ... 141
22.5.1 Revoking access via Azure Portal ... 141
22.5.2 Revoking access via Powershell ... 141
22.6 Creating the data source in Collect ... 141
22.7 Settings fields ... 142
22.7.1 Data source details ... 142
22.8 Configuring the data source in Collect ... 142
22.8.1 Data source criteria ... 142
22.8.2 Modern attachments ... 143
23 Refinitiv Eikon data source ... 144
23.1 Consideration ... 144
23.2 Collection size ... 144

23.3 Creating the data source ... 145
23.4 Settings fields ... 145
23.5 Configuring the data source ... 145
24 Slack data source ... 146
24.1 Considerations ... 146
24.1.1 Grouped collection ... 146
24.1.2 Attachments and linked cloud files ... 147
24.1.3 Collection size ... 147
24.2 Task checklist ... 147
24.3 Slack application setup ... 147
24.4 Creating the data source in Collect ... 148
24.5 Settings fields ... 150
24.6 Configuring the data source in Collect ... 150
24.6.1 Criteria ... 150
24.6.2 Configuration considerations ... 152
25 Slack best practices ... 152
25.1 Date range ... 152
25.2 Channel scope ... 152
25.3 Recommended approach for large collections ... 153
25.4 Intended use ... 153
26 X1 data source ... 153
26.1 Considerations ... 154
26.2 Collection size ... 154
26.3 Creating the data source ... 154
26.4 Settings fields ... 154
26.5 Configuring the data source ... 155
26.5.1 Data source criteria ... 155
27 Collection ... 158
27.1 Considerations ... 158
27.2 Best practices for time-sensitive collections ... 159
27.3 Creating a collection ... 159
27.4 Using the Collect wizard ... 159
27.4.1 Collection Details ... 159
27.4.2 Data source ... 161

27.4.3 Custodians ... 161
27.4.4 Non-custodial ... 162
27.4.5 Collection Summary ... 162
28 Viewing or editing Collection data ... 163
28.1 Collection details ... 163
28.2 Viewing collected data ... 165
28.3 Collect console ... 165
28.3.1 Preview ... 165
28.3.2 Collection ... 166
28.4 Delete collections ... 167
29 Grouped collections ... 167
29.1 Grouped data sources ... 168
29.2 Grouping messages ... 168
29.3 Custodian assignment considerations ... 168
29.4 Manual processing guidance ... 169
30 Migrate Collect workspaces ... 169
30.1 Migrate Collect workspaces ... 169
30.2 Credentials do not migrate ... 169
30.3 After migration ... 169
30.3.1 Considerations ... 170
31 Identifying Collection data in Staging Explorer ... 170
32 Reports ... 172
32.1 Running reports ... 172
32.1.1 Collection Summary report ... 172
32.1.2 Collection Details report ... 172
32.1.3 Results report ... 172
32.1.4 Errors report ... 173
33 Status Summary ... 174
33.1 Job status ... 174
33.2 Reviewing job statuses ... 175
34 Target Status ... 175
35 Monitor ... 176
36 Index ... 179

1 Collect

Use this application for collecting your custodian's data through different sources. Start by setting up Collect as an application within your data source. For information on registering an app, see the source's documentation on their website. Once registered, start adding custodians, data sources, and targets to Collect. Once connected, start the collect job and begin collecting data from custodians.

Note: This document covers the Collection source source.

1.1 Data sources

In Collect, you can collect data from a variety of data sources. For more information, see Data sources on page 21.

- **Bloomberg**—collect short message data from Bloomberg Chat and Email sources. For more information, see Bloomberg. For more information on short messages, see the Relativity User site.
- **Box**—collect data from Box cloud storage sources.
  - You can also collect files from Box directly into Relativity aiR Government.
  - This data source requires application setup before you can add it as a data source in Collect.
  - For more information, see Box application setup on page 27.
- **Cellebrite**—collect data from Cellebrite. For more information, see Cellebrite data source on page 30.
- **ChatGPT Enterprise**—collect data from ChatGPT Enterprise. For more information, see ChatGPT Enterprise data source on page 36.
- **Claude**—select to collect from Anthropic's Claude. For more information on specific fields and settings, see Claude on page 39.
- **Google Workspace**—collect documents from Chat, Drive, Gemini, Gmail, and Groups. You can also collect files directly into Relativity aiR Government.
  - A license for Vault is required to collect data from Google Workspace. For more information, see Google's Vault Help documentation..
  - Google Chat is collected as RSMF files. For more information on short messages, see the Relativity User site.
  - This data source requires application setup before you can add it as a data source in Collect. For more information, see Google Workspace data source on page 51 and Google Gemini data source on page 61i.
- **iManage**—collect document and email data from the iManage application.
  - You can collect files and emails directly into Relativity aiR Government from iManage's private cloud, Cloud Classic.
  - For more information, see iManage.
- **Microsoft 365**—collect documents from a custodian's OneDrive account, a custodian's Outlook mailbox, inactive mailbox, calendar, and contacts list, a custodian's Team account, and SharePoint sites.
  - You can collect chats from Teams directly into Relativity aiR Government. Teams is collect as RSMF files. For more information on short messages, see the Relativity User site.
  - This data source requires application setup before you can add it as a data source in Collect. For more information, see Microsoft 365 setup.

Notes: Depending on your Relativity aiR license, your Microsoft tenant might be Microsoft 365 or Microsoft 365 Government. When using Microsoft 365 Government, all fields, workflows, and processes will be the same. The only difference will be the Microsoft 365 source icon you select when setting up a data source or creating a collection.

- **Refinitiv Eikon**—collect short messages from within your organizations Refinitiv Eikon chats. For more information, see Refinitiv Eikon. For more information on short messages, see the Relativity User site.
- **Slack**—collect short messages from within an organization's or custodian's Slack Enterprise application.
  - You can also collect chats from Slack Enterprise Grid directly into Relativity aiR Government.
  - For more information on short messages, see the Relativity User site.
  - This data source requires application setup before you can add it as a data source in Collect.
  - For more information, see Slack data source on page 146.
- **X1**—collect documents from within the X1 file system or emails and attachments from within a custodian's email that is a part of the X1 system.
  - You can inspect file names and other metadata, as well as collect files for this data source.
  - You can also configure collection parameters and specify a date range for email messages that you want to discover.
  - For more information, see X1.

1.2 Commercial and Government support

There are no other limitations compared to Relativity aiR commercial instances aside from data source connector availability.

Use the following table to see available connectors in Relativity aiR Government instances compared to commercial instances.

Note: Inactive mailbox, and Inactive OneDrive for Government is currently only supported for customers in Microsoft GCC tenants.

2 Installing Collect

You can install Collect in a workspace by using the functionality available through the Application Deployment System (ADS). This system provides you with the option to install Collect by selecting it from the list of existing applications in the Application Library tab or by importing it from an external application file.

To install Collect, install Collect from the Application Library tab and, if required, enable access for the data source.

Confirm that you have the appropriate system admin permissions to install an application. For more information, see Workspace security on the Relativity aiR documentation site.

2.1 System requirements for Collect

Collect uses the ADS framework, so you install it as an application within a Relativity instance. Consequently, Collect has the same system requirements as Relativity aiR. For Relativity aiR's system requirements, see System Requirements on the Relativity aiR Documentation site.

2.2 Installing Collect

Collect is compatible with Relativity aiR. See Getting started in Relativity aiR on the Documentation site for requirements.

For a Collect-only installation, you do not need the following pre-requisities:

- Analytics server setup
- Database server for processing or native imaging
- Worker server for processing or native imaging
- Obtaining applications for native imaging and processing

Because Collect uses the ADS framework, you can install through the Relativity Application tab from the library. See Installing Collect from the application library below.

Note: You configure security permissions on Collect just as you would for any other Relativity application. For more information, see Workspace security on the Relativity aiR documentation site.

2.2.1 Installing Collect from the application library

If Collect is in the application library, you can install it to the current workspace. Confirm that you have the appropriate system admin permissions to install an application. For more information, see Workspace security on the Relativity aiR Documentation site.

Note: Analytics, Case Dynamics, Collect, Legal Hold, and Processing all share the Entity object. You may be prompted to complete additional steps to unlock and resolve conflicts of the listed applications in order to complete installation. For information, see Troubleshooting application installation errors on the Relativity aiR documentation site.

Use the following procedure to install Collect from the application library:

1. Navigate to the workspace where you want to install the application.
2. Navigate to the **Application Admin** tab.
3. Click **New Relativity Application** to display an application form.
4. Click the **Select from Application Library** radio button in the Application Type section.
5. Click the ellipses button in the **Choose from Application Library** field.
6. Select Collect on the Select Library Application dialog. This dialog only displays applications added to the Application Library. If Collect is not included in the list, see the Installing applications topic.
7. Click **Ok** to display the application in the **Choose from Application Library** field. The application form also displays the following fields:
    - **Version**—displays the version of the application that you are installing.
    - **User-friendly URL**—displays a user-friendly version of the application's URL. This field may be blank.
    - **Application Artifacts**—displays object types and other application components.
    - **Map Fields**—there are no fields available in Collect for mapping.
8. Click **Import** to install Collect into the workspace.
9. Review the import status of the application. Verify that the install was successful or resolve errors.

2.3 Permissions to run Collect

The following security permissions are required to run and complete the collection process:

Note: Feature Permissions provide an alternative to Relativity's security management by shifting the focus from Object Types and Tab Visibility to feature-based permissions. This method is an alternative option. Any feature-specific permissions information already in this and other topics is still applicable. The Feature Permissions interface enables administrators to manage permissions at the feature level, offering a more intuitive experience. By viewing granular permissions associated with each feature, administrators can ensure comprehensive control, ultimately reducing complexity and minimizing errors. For details see Instance-level permissions and Workspace-level permissions.

Object Security	Tab Visibility	Other Settings
Collect Objects: • **Collection** — View, Edit, Add • **Collection Detail Custodian** — View, Edit, Add, Delete • **Collection Detail Custodian Target** — View, Edit, Add, Delete • **Collection Detail Custodian Target Result** — View, Edit, Add, Delete • **Collection Detail Noncustodial Source** — View, Edit, Add, Delete • **Collection Detail Noncustodial Target** — View, Edit, Add, Delete • **Collection Detail Request** — View, Edit, Add, Delete • **Collection Detail Source Instance** — View, Edit, Add, Delete • **Collection Detail Source Type** — View, Edit, Add, Delete • **Collection Detail Summary** — View, Edit, Add, Delete • **Collection Matter** — View, Edit, Add • **Collection Run** — View, Edit, Add • **Collection Source Instance** — View • **Collection Source Instance Parameter** — View • **Collection Source Target Parameter Instance** — View • **Collection Source Target Parameter Type** — View	• Collections • Monitor • Custodian Targets • Status Summary • Custodial Target Status • Non-Custodial Target Status • Entities (only needed if user must see Entities) • Any processing tabs (only needed if user will access Processing)	• None

Object Security	Tab Visibility	Other Set-tings
• **Collection Source Type** — View • **Collection Source Type Criteria** — View • **Collection Source Type Criteria Validator** — View • **Collection Source Type OAuth Definition** — View • **Custodian Target** — View, Edit, Add, Delete • **Custodian Target Generation Error** — View, Edit, Add, Delete • **Entity** — only View, unless user needs to manage Entities in which case include Edit, Add • **Noncustodial Data Source Instance** — View, Edit, Add, Delete • **Noncustodial Target Generation Error** — View, Edit, Add, Delete Objects required for integrated Processing functionality: • **Folder** — View, Edit, Add • **Processing Data Source** — View, Edit, Add • **Processing Error** — View, Edit, Add • **Processing Profile** — View, Edit, Add • **Processing Set** — View, Edit, Add • **Relativity Time Zone** — View, Edit, Add		

2.4 Uninstalling the application

If you need to remove the Collect application from your workspace, contact Relativity Support.

3 Matters

In Collect, a matter represents a legal action or case requiring you to collect electronic data from sources such as Collection source. Matters can be used to group multiple related collection jobs.

You manage matters that are associated with a collection. You can create each of these items on their respective tabs, or you can create them when you add a new collection.

Note: Matters created from Home aren't available for use in Collect nor listed on the Matters tab in this application. Additionally, the matters created on this tab are only available for use in Collect.

3.1 Creating a matter

Use the following procedure to create a matter that you can associate with a collection:

1. Navigate to the Matters tab. Collect displays a list of the active matters currently available to this application.
2. Click **New Collection Matter**.
3. Complete the fields in the Matter Details layout. See Matter Details layout fields below.
4. Click **Save**. Collect displays the matter details. See Viewing or editing matter details below.

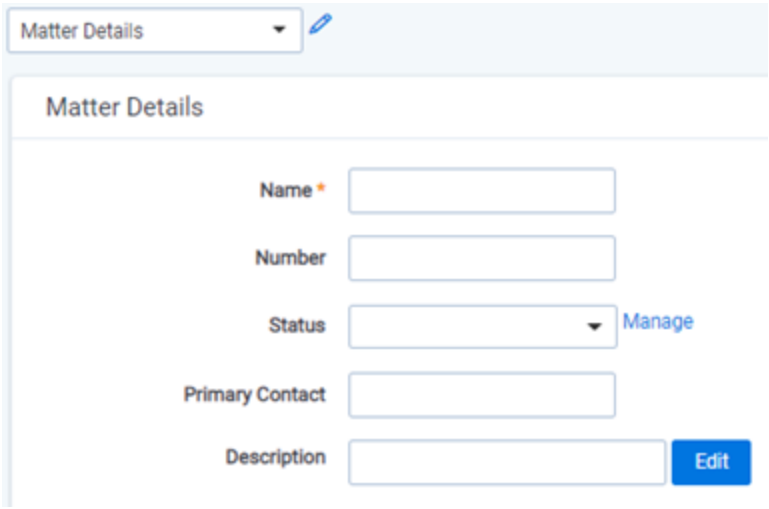
You can also create a matter when you add a new collection. Click the **Add** link next to the Matter field in the Collection layout. See Creating a collection on page 159.

3.2 Matter Details layout fields

The Matter Details layout contains the following fields:

- **Name**—the name of the matter.
- **Number**—the number you assign to the matter for reporting purposes.
- **Status**—the status you assign to the matter for reporting purposes. Select an existing status from the drop-down menu or click **Add** to define a new one. Existing statuses include **Active** and **Closed**.

  Note: Assigning a status of Closed to a matter hides it from the Active Collect view on the Collect tab.
- **Primary Contact**—the name of an individual who handles communications related to the matter.
- **Description**—the description of the matter used for reporting purposes. Click **Edit** to display an HTML text editor where you can enter the description.



3.3 Viewing or editing matter details

Display the matter details by clicking the name of a matter on the Matters tab. Collect also displays these details immediately after you add a new matter. You can use the buttons at the top of the page to edit, delete, or perform other tasks with the matter.

The details page includes the following sections:

- **Matters Details**—lists the name, number, status, primary contact and description of the matter.
- **Collect**—lists all collections associated with the matter. You can also perform the following tasks in this section:
    - **Associate the matter with a new collection**—to create a new collection, click **New**. See Creating a collection on page 159.
    - **Remove a collection from Relativity**—click **Delete** to display a pop-up window. To view child objects and associated objects, click **Dependencies**.
    - **Modify collection details**—click the **Edit** link for a collection. To modify the matter, click the **Edit** button at the top of the page.
    - **Display the collection details**—click the name of the collection.

4 Custodian targets

In Collect, you manage custodians that have an associated data source. The custodian target is the combination of a custodian and data source. It is an endpoint from which Collect can connect to and collect from. For example, a custodian's Google Workspace Gmail account is a custodian target. For example, a custodian's Microsoft Outlook account is a custodian target.For example, a custodian's X1 email endpoint is a custodian target.

To collect from custodians, entities either have to already exist, be created, or be imported in Relativity. The custodian and their primary email address must also be associated to the data source. When the primary email address field for a custodian is present, Collect automatically generates the required targets for each data source while setting up a collection job.

Note: Custodian targets are automatically generated based on the primary email address in the Entity record for the Collection source data source. Custodian targets can still be generated manually. The auto-generation of targets is based on the custodian's email address. For more information, see Creating a custodian target on the next page.

4.1 Custodians

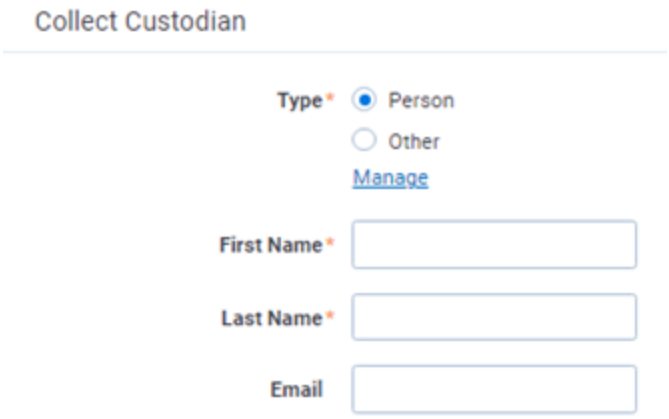
Once you create an entity in the Collect Custodian view and add it to a collect project, it becomes a custodian.

If a custodian does not exist, you can manually create an entity from the Entities tab. If a custodian does exist, you can create a custodian target. For more information, see Creating a custodian target.

You can add custodians to Collect at different times throughout the collection process. There are different ways to populate the entity list including using Integration Points, Import/Export, or manually. For more information, see Integration Points and Import/Export. To manually create a new custodian, follow the steps below:

1. Navigate to the **Entities** tab.
2. Click **New Entity** on the Custodians tab.
3. Select the **Collection History** layout from the drop-down menu and complete the fields. See Fields on the next page.
4. Click **Save**.

Note: When creating a custodian from Legal Hold, the **Custodians - Legal Hold View** is selected by default. If Collection or Processing is also installed in the same workspace, you can view the **Custodians - Processing View** or **Custodians - Collection View**.



4.2 Fields

When creating an entity, the Collection Custodian layout provides the following fields and others. To successfully create a collect entity, at a minimum, complete the following fields:

- **Custodian Type** (Required)—select one of the following:
  - **Person**—select this option to enter first and last name of the individual acting as custodian of the data you wish to process.
  - **Other**—select this option if the custodian of the data to process is not an individual but is, for example, just a company name.
    - Selecting this option changes the Custodian layout to remove the required First Name and Last Name fields and instead presents a required Full Name field.
    - You can also select this option to enter an individual's full name without having that name include a comma once you export the data associated with it.
- **First Name** (Required)—the first name of the custodian. This field is only available if you've set the Custodian Type to Person.
- **Last Name** (Required)—the last name of the custodian.
  - This field is only available if you've set the Custodian Type to Person.
- **Full Name**—the full name of the custodian of the data you wish to process.
  - Required when you set the Custodian Type to Other, Organization, or a custom choice type.
  - When you enter the full name, it does not contain a comma when you export the data associated with it.
- **Email** (Required)—the email the custodian uses in the target.
  - The entity's email is required to connect the entity to a custodian target. The email is not required to save the entity.
  - This email address must match the email address within the connected data source.

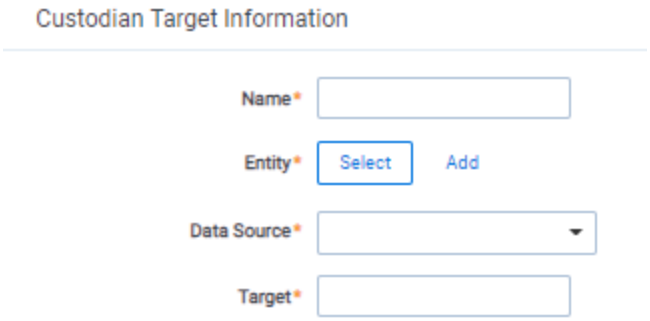
4.3 Creating a custodian target

You can collect electronic data from custodians who are individuals, or entities, involved in a legal action or case. You may perform multiple collections from a single custodian.

On the Custodians tab, you can create and edit custodians as well as view their details, associate them with collections, and perform other tasks. Custodian Targets can also be automatically generated in the Collection Summary step of the Collect wizard. For more information, see Collection Summary on page 162.

Use the following procedure to create a custodian target that you can associate with a collection:

1. Enter the **Name** of the custodian target.
2. Click **Select** to select available custodians. If the custodian does not exist, click **Add** and complete additional steps.
3. Click the **Data Source** drop-down menu to select a data source. For more information Collection data sources, see Data source types on the next page.
4. Enter the custodian's email address in the **Target** field.



To avoid duplicate custodians, a custodian with multiple emails, you will need to link a second custodian target to the same entity. To make a second custodian target for the same entity, you will need to create another target.

In the target, select the same entity. Then, select the other data source and enter the target value. This way you can have multiple targets, different from the primary email address, for a single entity record.

4.3.1 Generating targets in the wizard

Custodian Targets can also be automatically generated in the Collection Summary step of the Collect wizard. For more information, see Collection Summary on page 162.

Click **Generate Targets** to check if targets exist for the custodians you've selected for collection. If the targets do not exist, Collect creates them based on the email address in the Entity details in each custodian.

If an invalid custodian target is created manually, the auto-generation of custodian targets does not remove the invalid custodian target. Remove it manually. Any errored targets display in the Collection Summary step or on the Status Summary tab.

To delete a custodian target from the Custodians Targets tab, click the data source's checkbox and use the Delete mass operation.

4.4 Removing custodian targets

To remove any custodian target, first remove the custodian from the collection or collections. You can use the Mass delete operation to delete collect custodians, also known as entities. For more information, see the Admin Guide.

Trying to delete a custodian target before removing a custodian results in an error.

5 Data sources

A data source allows you to define where and how you pull data from a communication channel. A data source stores the configuration necessary to retrieve data from a communication channel, process that data, and ingest it into Collect.

Set up workspace data sources before beginning collections. Data sources are stores of information from which you collect data. These data sources have parameters that you can set during the creation of a collection job.

Note: Data sources cannot be deleted once it's been run on a collection.

5.1 Creating a collect data source

The Collection Admin tab is where you create, edit, and remove data sources from your workspace. Setup only needs to be done once for each data source. You must create your data sources prior to setting up your custodian targets. For more information, see Custodian targets on page 19.

When creating data sources, you can select different types of data sources for obtaining files.

It is possible to collect Microsoft data placed on a preservation hold through Legal Hold. For more information on preserving Microsoft 365 data using Legal Hold, see the Legal Hold guide.

Use the following procedure to create a new Collect source instance:

1. Navigate to **Collection Admin**.
2. Click the **New Collection Source Instance** button.
3. Do the following:
    - **Name**—enter in a unique name for the data source.
    - **Type**—select the type of data source. For more information, see Data source types below.

      Note: Collect automatically collects any data that is preserved due to an in-place hold or litigation hold. Data on a hold is stored in a preservation library and separate folders. For more information, see Microsoft Retention Policies.
    - **Settings**—enter the data source-specific settings. For more information on specific fields and settings, locate your data source topic from Data source types below.
4. Click **Save**.

After clicking Save, Relativity verifies the parameters and connectivity to the data source instance. If successful, the data source is saved. If the connection fails, a message displays indicating that the connection failed. If verification fails, verify that the values are correct. The data source will save when it is corrected and is verified.

Once the data source is set up, you'll see the data source information on the Collection Admin page.

5.1.1 Third-party vendor

If you are a vendor setting up a data source on behalf of a client, the client does not need access to the Relativity workspace. You manage the workspace setup on their behalf. The client only needs to provide admin credentials for their platform to complete the data source setup. The client has two options:

- The platform admin shares their credentials with you directly.
- The client creates a dedicated admin account for you to use.

We recommend completing this step in a screenshare session with the client's admin to avoid sharing credentials outside of the client's organization.

5.2 Data source types

You can select any of the following data source types for step 3 of Creating a collect data source above:

- **Bloomberg**—select to collect data from Bloomberg Chat. For more information on specific fields and settings, see Bloomberg chats and emails data source on page 24.

- **Box**—select to collect data from Box cloud storage. For more information on specific fields and settings, see Box data source on page 26.
- **Cellebrite**—collect data from Cellebrite. For more information, see Cellebrite data source on page 30.
- **ChatGPT**—select to collect data from ChatGPT. For more information on specific fields and settings, see ChatGPT Enterprise data source on page 36.
- **Claude**—select to collect from Anthropic's Claude. For more information on specific fields and settings, see Claude on page 39.
- **Google Workspace**—select to collect data from Google Chat, Drive, Gmail, or Groups.
    - Google Chat is collected as grouped collections. At the data source level, the custodian appears as the data source name.
    - For more information on specific fields and settings, see Google Workspace data source on page 51.
- **Google Gemini**—select to collect data from Google Gemini. For more information on specific fields and settings, see Google Gemini data source on page 61
- **iManage**—select to collect data from the iManage document and email management application. For more information on specific fields and settings, see iManage data source on page 65.
- **Microsoft 365 Inactive mailbox**—Outlook mailboxes become inactive mailboxes when an account is deleted while under a preservation hold.
    - When deleted, Microsoft does not throw the mailbox away. Microsoft keeps it in inactive state until the related preservation or retention hold is over.
    - Relativity can collect these mailboxes.
    - For more information on specific fields and settings, see Microsoft 365 - Inactive mailboxes data source on page 71.
- **Microsoft 365 Mailbox**—select to collect data from a custodian's primary mailbox, archived online mailbox, and inactive mailboxes in a single collection job.
    - Collect retrieves all mailbox types the Purview API supports for a custodian. You do not need to configure each mailbox type separately.
    - Relativity creates a case in Microsoft Purview, adds the custodian, runs the search, and exports the results to Collect.
    - For more information on specific fields and settings, see Microsoft 365 - Mailboxes data source on page 88
- **Microsoft 365 OneDrive**—select to collect data from OneDrive accounts.
    - Unable to collect from inactive employee sites.
    - The Graph API does not support access to inactive user accounts.
    - For more information on specific fields and settings, see Microsoft 365 - OneDrive data source on page 97.
- **Microsoft 365 Outlook**—select to collect data from Microsoft's email application.
    - You can choose archived mailbox, calendar, contacts, and mailbox.
    - For more information on specific fields and settings, see Microsoft 365 - Outlook data source on page 105.

- **Microsoft 365 SharePoint**—select to collect data from Micrsoft SharePoint sites.
  -
  - For more information on specific fields and settings, see Microsoft 365 - SharePoint data source on page 126.
- **Microsoft 365 Teams**—select to collect data from Microsoft's short-messaging application. This data source is only available for commercial, Microsoft 365 tenants.
  - Requires enhanced licensing (E5) and access to Microsoft Protected APIs.
  - For more information on specific fields and settings, see Microsoft 365 - Teams data source on page 134.
- **Refinitiv Eikon**—select to collect data from Refinitiv Eikon chats. For more information on specific fields and settings, see Refinitiv Eikon data source on page 144.
- **Slack**—select to collect data from an organization or custodian's Slack profile.
  - Slack is collected as grouped collections. At the data source level, the custodian appears as the data source name.
  - For more information on specific fields, settings, temporary code, and access token, see Slack data source on page 146.
- **X1**—select to collect data from a custodian's emails or files stored in an X1 endpoint. Requires separate licensing, configuration, and training through a third party. For more information on specific fields and settings, see X1 data source on page 153.

6 Bloomberg chats and emails data source

This topic provides details on how to capture Bloomberg chats and emails with Collect.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

6.1 Consideration

Note the following consideration about this data source:

- Bloomberg chat data is collected into grouped collections, resulting in a different data count compared to standard collections.
- These grouped collections comprise a set of RSMFs (Relativity Short Message Format) containing all the chats for the assigned custodians. Due to this grouping, it is expected that custodian targets will have identical counts.
- Essentially, when collecting data from multiple custodian targets, the item counts and sizes for each will match. This uniformity arises because the item count reflects the number of RSMF files generated for the job, while the size reflects the total size of the created RSMF file set.

6.2 Collection size

Bloomberg sources follow familiar email and chat scaling patterns.

Category	Details
Hard limits (enforced)	No global hard cap
Planning thresholds (guidance)	Long chat histories (Chat) Large mailboxes with attachments (Mail)
When to split	Long date ranges
Notes	Chat = short-message data Mail = email-like scaling

Treat Chat like messaging data and Mail like traditional email when planning splits.

6.3 Creating the data source instance

Use the following procedure to create a new Collect source instance in Relativity aiR.

1. Navigate to **Collection Admin** within Collect Admin of Set Up.
2. Click the **New Collection Source Instance** button.
3. Do the following:
   - **Name**—enter in a unique name for the data source.
   - **Type**—select **Bloomberg Chat** or **Bloomberg Email** data source.
   - **Settings**—enter the required information in the Settings fields. For more information on the fields, see Settings fields below.
4. Click **Save**. The data source displays on the Collection Admin page.

6.4 Settings fields

Gather the information listed below, and enter it into the Settings fields:

- **Host**—enter the address of the Bloomberg host. For example, sftp.bloomberg.com.
- **Port**—enter the port used for Bloomberg.
- **Path**—enter the folder address where you store the files.
- **Username**—enter the user name to your organization's Bloomberg site.
- **Password**—enter the password to your organization's Bloomberg site.
- **Pass Phrase**—enter the pass phrase to your organization's Bloomberg site.
- **PGP Key**—enter the key used to decrypt the data that's transferred from the Bloomberg to Collect.

6.5 Configuring the data source

Each data source used in Collect has different search criteria on the Collection Details step when creating a collection job. The criteria needs to be configured next.

1. Configure search criteria to collect specific data.

   Note: Leave the data source criteria empty to collect all data from the sources.

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.
- **Operator**—choose an operator such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

2. Click **Add Criteria**. Each criteria is separated by an AND operator.

Filter a data source's data that you want to collect by adding criteria. This section covers the different criteria for each data source. It also includes what you can search within each data source. The criteria options change based on the selected data source.

All dates are in Coordinated Universal Time (UTC).

6.5.1 Bloomberg chat

The following table lists the filter criteria support for Bloomberg chat collections. Entering the start date and end data criteria is not required.

Relativity collects Bloomberg chat data in Relativity Short Message Format (RSMF).

Property	Operators	Description	Example
Start Date	Equals	When you use the Start Date property in a query, the search returns chats that exist the day of and after the entered date.	When you search a Start Date of 1/1/2001 and an End Date of 1/1/2020, all calendar items on and between the two dates are returned.
End Date	Equals	When you use the End Date property in a query, the search returns all chats the day of and before the entered date.	When you search a Start Date of 1/1/2001 and an End Date of 1/1/2020, all calendar items on and between the two dates are returned.

6.5.2 Bloomberg email

The following table lists the filter criteria support for Bloomberg email collections. Entering the start date and end data criteria is not required.

Relativity collects Bloomberg email data in Relativity's short message format (RSMF).

Criteria	Operators	Description	Example
Start Date	Equals	When you use the Creation Date property in a query, the search returns all messages that equal/-doesn't equal, greater/less than the date entered.	If you search "Greater Than 1/1/2001," your results include all messages created after January 1, 2001.
End Date	Equals	When you use the Modification Date property in a query, the search returns all updated files that equal/doesn't equal, greater/less than the date entered.	If you search "Less Than 1/1/2020," your results include all files modified before January 1, 2020.

7 Box data source

This topic provides details on how to capture Box with Collect.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

7.1 Collection size

Box collections are constrained primarily by API rate limits rather than strict job limits.

Category	Details
Hard limits (enforced)	No custodian hard stop.
Planning thresholds (guidance)	Greater than 20 custodians with large folder trees often throttled.
When to split	Sustained throttling.
Notes	API rate limits dominate.

Monitor for throttling and split jobs reactively when limits are encountered.

7.2 Task checklist

The table lists the order to set up this data source for Relativity aiR Collect.

Order	Application Used	Task
1	Box	Create and authorize Collect as an application in Box
2	Relativity aiR	Create the Box data source instance in Collect
3	Relativity aiR	Configure the Box data source in Collect

7.3 Box application setup

Before using the Box data source in Collect, you must create and authorize Collect as an application in Box.

Note: The Box connector relies on Server Authentication, with JWT. SSO is currently not supported.

7.3.1 Creating an application with Box

Create and download a config.json file. For more information, see Box's https://developer.box.com/guides/authentication/jwt/jwt-setup/.

The config.json file will contain the values required to configure a data source connection in Collect.

In Box:

1. Log into Box.
2. Navigate to the Developer Console.
3. Click **Create New App**.
4. Click **Custom App**.
5. Select **Server Authentication (with JWT)**.

6. Enter an App Name.
7. Click **Create App**.
8. In App Access level, select **App Access + Enterprise Access**.
9. In Content Actions, select **Read all files and folders stored in Box** and **Write all files and folders stored in Box**.
10. In Advanced Features, select **Make API calls using as-user header** and **Generate user access tokens**.
11. Add and Manage Public Keys clicking **Generate a Public/Private Keypair**. Authentication is required for this step.

A .json file will be downloaded to your machine. Save the file in a secure location. This file contains the values required to configure a data source connection in Collect. This file can also be downloaded from the App Settings section.

7.3.2 Authorizing an application

Ensure you get approval to use the Box application within your enterprise. Follow the steps provided by Box to submit for approval. For more information, see the Box documentation.
Finally, you must get authorization from a Box admin to use the authentication application. For more information, see the Box documentation.

7.4 Creating the data source instance in Collect

Use the following procedure to connect the Box data source instance to Collect.

In Relativity aiR:

1. Navigate to **Collection Admin** within Collect Admin of Set Up.
2. Click the **New Collection Source Instance** button.
3. Do the following:
    - **Name**—enter in a unique name for the data source instance.
    - **Type**—select the **Box** data source.

- **Settings**—enter the required information in the Settings fields. For more information on the fields, see Settings fields below.

4. Click **Save**. The data source displays on the Collection Admin page.

7.5 Settings fields

Gather the information listed from the .json file, and enter it into the Settings fields:

- **Client ID**—enter the Client ID of the requesting application. This can be found with authorization_code, client_credentials, or urn:ietf:params:oauth:grant-type:jwt-bearer as the grant_type.
- **Client Secret**—enter the client secret of the requesting application to gain an access token.
- **Public Key ID**—enter the Public Key ID of the requesting application that you found in your app configuration settings .json file.
- **Private Key**—enter the encrypted private key that you found in your app configuration settings .json file.
- **Passphrase**—enter the pass phrase that you found in your app configuration settings .json file.
- **Enterprise ID**—enter the Enterprise ID that you found in your app configuration settings .json file.

7.5.1 Data source details

Each data source details page includes an Actions console. The options available will be different for each data source.

You can click **Validate Connection** to validate the client ID, client secret, and other credentials with Box.

7.6 Configuring the data source in Collect

Each data source used in Collect has different search criteria on the Collection Details step when creating a collection job. The criteria needs to be configured next.

1. Configure search criteria to collect specific data.
   - **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
   - **Field**—choose the field to filter on within the data source.
   - **Operator**—choose an operator such as equals, contains, greater than, or less than.
   - **Value**—enter a value to find in the selected field.
2. Click **Add Criteria**.

The following table lists the filter criteria support for Box collections. Entering the start date and end data criteria is not required.

All dates are in Coordinated Universal Time (UTC).

Criteria	Operators	Description	Example
Creation Date	Greater Than or Equals, Less Than or Equals	When you use the Creation Date property in a query, the search returns all messages that equal/doesn't equal, greater/less than the date entered.	If you search "Greater Than 1/1/2001," your results include all messages created after January 1, 2001.

Criteria	Operators	Description	Example
Modification Date	Greater Than or Equals, Less Than or Equals	When you use the Modification Date property in a query, the search returns all updated files that equal/doesn't equal, greater/less than the date entered.	If you search "Less Than 1/1/2020," your results include all files modified before January 1, 2020.

8 Cellebrite data source

This topic provides details on how you can remotely capture mobile device messages and attachments from Android or iOS devices using the Cellebrite data source within Collect.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

Note: The steps below apply whether you are using Cellebrite Endpoint Inspector or Endpoint Mobile Now. Going forward in this topic, we will simply refer to them as Cellebrite.

8.1 Considerations

Review the list of considerations before starting your collection:

- This functionality is available to Relativity aiR US and UK-based commercial clients. It is not yet available to US Government clients or those outside the US and UK.
- Cellebrite data source requires separate licensing, configuration, and training through Cellebrite.
  - For more information, log in to your account at MyCellebrite.com to download the installation files and manuals based on which product you are using:

    Note: To ensure a successful data collection, be sure that you and the custodian familiarize yourselves with Cellebrite's documentation, recommendations, and tips for mobile collections before you begin collecting. Also be sure to review the What's New in Version <#.#> chapter of the Cellebrite Endpoint Inspector or Endpoint Mobile Now user guides.

    - Cellebrite Endpoint Inspector User Guide
    - Cellebrite Endpoint Inspector SaaS Communication and Security Guide
    - Cellebrite Endpoint Mobile Now User Guide
- The output generated from mobile device collections consists of all short message-type data in Relativity Short Message Format (RSMF) files.
  - The corresponding Cellebrite Universal Forensic Electronic Device (UFD) file is also uploaded to your StagingArea.
  - An example of a UFD file is a forensic image.
- UFD files cannot be processed. However, they are made available if you need the UFD downloaded for examination outside of Relativity aiR.
- Collect captures all short message data that Cellebrite successfully extracts from a device and, converted to RSMF.

- This includes original UFD image and collection reports.
- Support for specific apps depends on whether Cellebrite can extract and decode that app's data for the device, operating system, and app version.

8.2 Prerequisites

Basic configuration for your instance of Cellebrite and Relativity aiR must be completed as follows:

- In Cellebrite:
  - Set up your instance.
  - If using Endpoint Inspector, create the required user account with the Examiner role.
  - Ensure the required ports are open.
  - For use with Relativity aiR, you do not need to set up a storage repository.
- In Relativity aiR: The Collect application must be installed into the Relativity workspace that is used to perform Cellebrite collections. For more information on installing Collect in a workspace, see Installing Collect.

8.3 Collection size

Cellebrite data volume depends on the size and scope of the original device extraction.

Category	Details
Hard limits (enforced)	Extraction-defined
Planning thresholds (guidance)	Full device extractions can be large
When to split	Very large extractions
Notes	Mobile data post-extraction

Use extraction scope to guide splitting decisions rather than custodian count.

8.4 Task checklist

The table below outlines the tasks in the order they need to be performed and within which application to perform them.

Order	Application Used	Task Type	Task
1	Relativity aiR	Configuration	Create the OAuth2 Client on the next page
2	Relativity aiR	Configuration	Set permissions in Relativity aiR on the next page
3	Cellebrite	Configuration	Connect Cellebrite to Relativity aiR on the next page
4	Cellebrite	Configuration	Generate API key for Cellebrite data source on page 33
5	Relativity aiR	Configuration	Create the data source in Relativity aiR on page 33
6	Relativity aiR	Configuration	Create entities in Relativity aiR on page 34
8	Relativity aiR	Collecting	Create a Collect job in Relativity aiR on page 34

8.4.1 Support resources

If you have questions or issues while going through these procedures, please contact the following resources depending on the application:

- **Cellebrite (Endpoint Inspector or Endpoint Mobile Now)**—contact Cellebrite Customer Support or log in to your MyCellebrite account to view Cellebrite's documentation.
- **Relativity aiR Collect**—contact Relativity Customer Support or refer to Relativity Documentation or Community Site for more information.

8.5 Create the OAuth2 Client

To facilitate data transfers and communication of collection status updates from Cellebrite to Relativity aiR, an OAuth2 client must be configured in Relativity aiR. Use the following steps to create a new OAuth2 Client. For more detailed instructions, see documentation on creating and editing an OAuth2 client.

In Relativity aiR:

1. Navigate to the **OAuth2 Client** tab within Authentication.
2. Click the **New OAuth2 Client** button.
3. Do the following:
    - **Name**—enter a unique name for the OAuth2 client.
    - **Enabled**—ensure the **Enabled** toggle is on.
    - **Flow Grant Type**— select **Client Credentials** from the list.
    - **Context User**—select a user account from the list. The Context User will also generate the Cellebrite API key that is used to configure the Collect data source.
    - **Access Token Lifetime** (in minutes)—enter **60**.
4. Click **Save**.
5. Make note of the **Client ID** and **Client Secret** values that were generated. These values are needed when connecting Cellebrite to Relativity aiR.

8.6 Set permissions in Relativity aiR

Ensure the following account permissions are properly set up. For additional information, see Adding user to groups and Setting workspace permissions.

- **For Context Users**—The Context User selected in the previous section must be added to a group in Relativity aiR that is assigned to the workspace in which Cellebrite collections are run. The group within the workspace must have **Allow Export** and **Allow Import** permissions selected (enabled) under Admin Operations on the Other Settings tab. See Manage Workspace Permissions for more information.
- **For Relativity Service Account**—assign the Relativity Service Account (**Service Account, Relativity**) user to a group (other than the System Admin group) that has been assigned to the workspace in which Cellebrite collections are run.

8.7 Connect Cellebrite to Relativity aiR

Next, you must connect Cellebrite to Relativity aiR using the Client ID and Client Secret obtained in Create the OAuth2 Client above.

In Cellebrite:

1. Navigate to **Settings**.
2. Scroll to the **Relativity aiR** section and do the following:
    - **Client ID** and **Client Secret**—enter the ID and secret generated previously when creating the OAuth2 client in Relativity aiR.
    - **Domain**—enter the Relativity aiR domain. For example, esus019064-t066.r1.kcura.com. This is not the full URL address, so you do not include "https://" or the ending slash.
3. Click **Save**.

8.8 Generate API key for Cellebrite data source

After connecting Cellebrite to Relativity aiR, you must generate and save the API key. This API key is entered in Relativity aiR when creating a new data source outlined in the next section.

Note: The user generating the API key must be the Context User set up in Create the OAuth2 Client on the previous page.

In Cellebrite:

4. Navigate to **User Settings** if using Endpoint Inspector or to **Settings** if using Endpoint Mobile Now.
5. Click **Generate Key**.
6. Copy the **API Key** and save it securely.

    Caution: You will not be able to see this API key again in Endpoint Inspector or Endpoint Mobile Now so be sure to copy and save it.

This API key is required when you create a new data source next in Relativity aiR. You must also provide the following information:

- The exact username that was used to generate the API key if you used Endpoint Inspector.
- The exact email address that was used to generate the API key if you used Endpoint Mobile Now.
- The URL for your instance of Endpoint Inspector or Endpoint Mobile Now. For example: https://example.ei.cellebrite.cloud/

8.9 Create the data source in Relativity aiR

Next, create a new Collect data source instance in your Relativity aiR workspace.

Note: You must have previously installed the Collect application into your workspace. For more information on installing Collect, see Installing Collect.

In Relativity aiR:

7. Navigate to **Collection Admin** within Collect Admin in Set Up.
8. Click **New Collection Source Instance**.

9. Do the following:
    - **Name**—enter a unique name for the data source.
    - **Type**—select the **Cellebrite** data source.
    - **Settings**—enter the required information in the Settings fields. For more information, see Settings fields below.
10. Click **Save**. The data source displays on the Collection Admin page.

8.9.1 Settings fields

To connect Relativity to the Cellebrite data source, you need to gather and enter the information for the following fields. This information was generated in the Generate API key for Cellebrite data source on the previous page section.

- **API Key**—the API key previously generated in Cellebrite.
- **API Username**—the Cellebrite user account used to generate the associated API Key.
    - If Endpoint Inspector was used to create the API key, then enter the user's username (for example, jane.-smith).
    - If Endpoint Mobile Now was used to create the API key, then enter the user's email address (for example, jane.smith@relativity.com).
- **API URL**—the Cellebrite server URL for the associated API Key.

8.10 Create entities in Relativity aiR

Within your Relativity aiR workspace, populate the Entities list with those individuals from which you wish to collect data. For more information on populating Relativity with entities, see Entity object documentation.

Note: Ensure that the Email address field for the Entity (such as, custodian) contains the primary email address to which you want Cellebrite collection requests emailed. The Secondary Email address information for the entity is not used.

8.11 Create a Collect job in Relativity aiR

You can begin creating and running collections in Relativity aiR. For more information, see Collections.

Be aware of the following when performing Cellebrite collections:

- You cannot combine other data source types with the Cellebrite data source.
- You can collect from multiple custodians in the same job when using the Cellebrite data source.

All dates are in Coordinated Universal Time (UTC).

8.12 Mobile data collection results

The export package created by Cellebrite for ingestion by Relativity aiR includes these files:

- Original collection file in UFED zip format
- Messages and attachments in an RSMF collection
- UFED reader file (UFD)

- Device Report
- Collection Report
- Results.csv file

The nature of data collections from Android and iOS devices differs due to the inherent differences between platforms. These are the most noteworthy differences:

- iOS message collections target messages from native apps and the most popular third-party apps that iTunes can back up. Attached media and document files are included.
- Android message collections target SMS, MMS, and RCS text messages from native apps. Attached media and document files are included.

8.13 Troubleshooting

This table includes troubleshooting for Cellebrite data source.

Area	Issue	Resolution

Data Source setup	User is unable to save a Cellebrite data source configuration in Collect or validation fails on an existing source.	• Verify the user has entered the correct value for the API key.
		• Verify the API Username is the Cellebrite account used to generate the API key in Cellebrite.
		  • For Endpoint Inspector, this is the user account name.
		  • For Endpoint Mobile Now, this is the email address of the user.
		• Verify the Context User who configured the OAuth2 client in Relativity aiR is also the same user who generated the API key in Cellebrite.
		• If the problem still exits after verifying the information in the previous bullets, then generate a new API key in Cellebrite.

Job start	The Collect job fails when the user clicks the Start button.	• Verify in Cellebrite Settings that the OAuth2 client setup for Relativity aiR has the correct values for the Client ID and Secret. They must match the values in Relativity aiR for the OAuth2 client configured. • Verify in Cellebrite Settings that the Domain for the OAuth client setup for Relativity aiR points to the correct Relativity aiR instance. The Domain should NOT contain “https://” or end with a trailing slash. For example, the domain should look like this *esus019064-t066.r1.k-cura.com* and not this *https://esus019064-t066.r1.kcura.com/*. • In very rare cases, C4 may be down, in which case Collect jobs will not start regardless of the collection data source. This issue usually resolves itself after a short waiting period. C4 is the shared compute platform on which jobs are run.
Custodian Email Notification	The Collect job started successfully, but the custodian never received the collection request email.	• Verify that the custodian's email address is the same as the one entered in the Email address field of their corresponding entity record. The Secondary Email address information for the entity is not used. • Verify that the email is not in the Spam or Junk folder.

Area	Issue	Resolution
		• Verify that the custodian's organization has not intercepted or quarantined the email via an email security policy or software, such as Proofpoint. • If the problem still exits after verifying the information in the previous bullets, then please contact Cellebrite Customer Support to verify that there are no issues sending email messages from Cellebrite.
File Transfers	The file transfers into Relativity aiR are failing.	• Verify that the Context User account used to configure the OAuth2 client is in a group assigned to the workspace, and the group has been given the "Allow Import" and "Allow Export" permissions in Relativity aiR. See Set permissions in Relativity aiR on page 32. • Verify that the Relativity Service Account user is assigned to one of the groups assigned to the workspace. See Set permissions in Relativity aiR on page 32.
Target Failure	The target collection fails after successful start.	If a job successfully started (e.g., was received by Cellebrite), but failed prior to the collection being uploaded to Relativity aiR, then the problem resides within Cellebrite. Please contact Cellebrite Customer Support for assistance.

9 ChatGPT Enterprise data source

This topic provides details on how to capture OpenAI's ChatGPT Enterprise with Collect.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

9.1 Considerations

Note the following considerations about this data source:

- This connector requires a ChatGPT Enterprise subscription.
- OpenAI's Compliance API only keeps data for 30 days. Collect can only retrieve ChatGPT data from the past 30 days.
    - OpenAI does not keep deleted data for more than 30 days, unless legally required otherwise.
    - Temporary chats, also called ephemeral chats, are only available for 30 days. These are conversations where OpenAI's Memory feature is disabled. The chat session is not saved to the user's history.
        - Temporary chats are accessible through the OpenAI Compliance API. They are included in Collect if your date filters are set correctly.
        - Temporary chats must fall within the 30-day retention window to be collected.
    - To avoid missing data, we recommend scheduling regular, ongoing collections before data is removed at the end of the 30-day retention window.

- Before your first collection, confirm that your organization enabled the Compliance API in its OpenAI account. This setting supports retrieval of both persistent and temporary conversations.
- For date criteria, ChatGPT Enterprise supports a start date. Collect retrieves all prompts and responses from the date you specify through the current date.
- If your organization has multiple ChatGPT Enterprise workspaces, you must configure a separate data source for each workspace in the Collect application. Name each data source to identify the workspace connects to.
- Relativity automatically converts collected conversation prompts and responses to Relativity's short message format (RSMF).
- ChatGPT metadata is collected. For more information, seeCollected metadata below.

9.2 Prerequisites

Complete the following before setting up a ChatGPT data source in Relativity:

- Eligible Enterprise and Education workspace owners can create a workspace-scoped Admin key with the permissions needed by the integration.
  - Create Admin key on the *Admin Console* > *Credentials* > *Admin keys* page.
  - For more information, see OpenAI's documentation.
  - Existing authorized keys do not need replacing just because self-service is available.
  - Contact OpenAI Support only self-service is unavailable.
- Confirm that the Compliance API is enabled in your organization's OpenAI account to support retrieval of both persistent and temporary conversations.

Once you complete the prerequisites, you can begin creating the data source.

9.3 Collection size

ChatGPT Enterprise collections scale with conversation volume and duration.

Category	Details
Hard limits (enforced)	No explicit hard cap published
Planning thresholds (guidance)	High-usage enterprise tenants
When to split	Long date ranges
Notes	Conversion-based scaling

Focus on limiting time ranges in high-usage environments to control collection size.

9.4 Collected metadata

As of the current integration with OpenAI's Compliance API, the metadata fields are captured and included in collections:

The following metadata fields are captured from ChatGPT Enterprise conversations via the Compliance API and included in Collect:

Metadata	Collected
Conersation ID	Always
Conversation title	Always
User ID	Always
User name	When user is logged in.
User email	When user is logged in.
Timestamp of prompt	Always
Timestamp of response	Always
Prompt text	Always
Response text	Always
Edit history	When a prompt was edited before re-execution.
Source attributions	URLs of any publicly cited websites when browsing was enabled.
Attachments	Uploaded files submitted by users during the conversation. For example, PDFs, DOCX, images, CSV files. Generated files. For example, documents or images created by ChatGPT in response to prompts.

These fields are extracted for both persistent and ephemeral (temporary) conversations, as long as they fall within OpenAI's 30-day retention window and meet your search criteria in Collect.

9.5 Creating the data source

Use the following procedure to connect the ChatGPT Enterprise workspace data source to Collect.

In Relativity aiR:

1. Navigate to **Collection Admin** within Collect Admin of Set Up
2. Click the **New Collection Source Instance** button.
    - **Name**—Enter in a unique name for the data source.
    - **Type**—Select the **ChatGPT Enterprise** data source.
    - **Settings**—enter the required information in the Settings fields. For more information, see Settings fields below.
3. Click **Save**. The data source displays on the Collection Admin page.

9.6 Settings fields

To connect Relativity to a ChatGPT Enterprise workspace, you need to gather and enter the information for the following fields.

- **API Key**—enter the API Key that you created in OpenAI.
    - You can use the same API Key when configuring multiple ChatGPT Enterprise data sources from which you wish to collect.

- For more information, see OpenAI's documentation.

  Note: Only contact OpenAI Support if you cannot create your own API Key.

- **Workspace ID**—enter the ChatGPT Enterprise WorkspaceID to which you want to connect.

9.7 Configuring the data source

Each data source used in Collect has different search criteria on the Collection Details step when creating a collection job. The criteria needs to be configured next.

Relativity collects ChatGPT Enterprise chat data in Relativity's short message format (RSMF).

Add search criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.

  Note: You must set a Start Date to complete the Data Sources step.

- **Operator**—choose an operator. For example, equals or greater than.
- **Value**—enter a value to find in the selected field.

The following table lists the filter criteria supported for ChatGPT Enterprise collections.

All dates are in Coordinated Universal Time (UTC).

Criteria	Operators	Description	Example
Start Date	Greater Than or Equals	When you use the Start Date property in a query, the search returns prompts and responses that exist the day of and after the entered date.	When you search a Start Date of 1/1/2024, Relativity collects all prompts and responses from that date to today.

Note: Temporary, or ephemeral, chats will also be returned if they occurred within the 30-day retention window and meet your search criteria.

10 Claude

Collect integrates with Claude (Anthropic) to collect enterprise AI conversations and generated content. This integration uses Anthropic's Compliance API and provides read-only access to in-scope data that exists at the time of collection.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

This topic provides details on how to capture Anthropic's Claude Enterprise with Collect.

10.1 Considerations

Note the following considerations about this data source:

- **Account and API access**
  - This connector requires a Claude Enterprise account.
  - The Anthropic Compliance API is only available with an Enterprise subscription.
  - Admin or standard API keys are not sufficient.
  - Only a Compliance access key, created by an Anthropic organization administrator or Enterprise Primary Owner, can retrieve conversation content, files, and artifacts.
- **Retention and deleted data**
  - Relativity collects deleted data only if Anthropic still retains the content.
  - Anthropic does not keep the content of deleted conversations, but it may keep records that the conversation occurred.
  - Your organization sets the retention policy. For more information on retention policies, see Anthropic's documentation.
  - Collection completeness is dependent on Anthropic retention policies and data availability at run time.
- **Collection behavior**
  - If you have multiple Claude organizations, you must configure a separate data source for each organization.
  - We recommend clearly naming each data source.
  - Relativity automatically converts collected conversation prompts and responses to Relativity's short message format (RSMF). For more information, see the Relativity Short Message Format guide.
  - Relativity collects Claude metadata. For more information, see Collected metadata on the next page.
- **Defensibility**
  - Access is read-only.
  - Collect does not modify or delete Claude data.
  - Data is retrieved directly via Anthropic's Compliance APIs.

10.2 Prerequisites

Before configuring your data source in Collect, you must enable the Compliance API on Anthropic's side to obtain an API key.

For more information about the Compliance API, see Anthropic's documentation.

Once you enabled the Compliance API, you can begin creating the data source.

10.3 Collected data

When configured with a valid Compliance access key, Collect can retrieve the following data from Claude Enterprise:

- **Conversations**—user prompts and Claude responses, collected in chronological order.
- **Artifacts**—AI-generated outputs such as documents or code artifacts.

- **Files**—user-uploaded and assistant-generated files associated with conversations.
- **Metadata**—custodian, user, timestamps, and conversation identifiers.

To make data review-ready in Collect,

- Collected conversations are ingested as parent documents.
- Artifacts and files linked as child documents or attachments.

10.3.1 Collected metadata

Relativity collects metadata from Anthropic's Compliance API as part of activity logs. For each action, like sending a prompt, getting a response, or uploading a file, Relativity collects all related metadata.

As of the current integration with Anthropic's Compliance API, Relativity captures the following metadata fields in collections:

Metadata	Collected
Conversation ID	Always
Conversation title	Always
User ID	Always
User name	Always
User email	Always
Timestamp of prompt	Always
Timestamp of response	Always
Prompt text	Always
Response text	Always
Edit history	Captures updates when a user edits and re-runs a prompt.
Attachments	Claude generated files, and user uploaded files submitted by users during the conversation.

10.3.2 Retention expectations and data availability

Collect retrieves only the Claude data that is retained and accessible at the time of collection.

Collections reflect the current retained state of Claude data and are not a historical reconstruction of all past activity.

Key considerations:

- Claude Enterprise retains conversation content by default, but customers may configure shorter retention periods.
- Conversations or artifacts deleted by users or retention policies cannot be collected.
- Collect cannot reconstruct historical data that no longer exists in Anthropic systems.

10.4 Creating the data source

Use the following procedure to connect the Claude data source to Collect.

In Relativity aiR:

1. Navigate to **Collection Admin**.
2. Click the **New Collection Source Instance** button.
3. Complete the following fields:
    - **Name**—enter a unique name for the data source.
    - **Type**—select the Claude data source.
    - **Settings**—enter the required information in the Settings fields. For more information, see Settings fields.
4. Click **Save**.

After clicking Save, Relativity verifies the parameters and connectivity to the data source instance.

- When verification is successful, Relativity saves the data source.
- When the connection fails, Relativity displays a message indicating that the connection failed.
    - When verification fails, verify that the values are correct.
    - Relativity can only save the data source when the values are correct and verified.

The data source displays on the Collection Admin page.

10.5 Settings fields

To connect Relativity to an Claude workspace, you need to gather and enter the information for the following fields:

- **API Key**—enter the API key that Anthropic provided to your organization. You can use the same API key when configuring multiple Claude data sources from which you want to collect.
- **Organization ID**—enter the Claude Organization ID.

10.6 Configuring the data source

Each data source used in Collect has different search criteria on the Collection Details step when creating a collection job. The criteria needs to be configured in this step.

Relativity collects Claude chat data in Relativity's short message format (RSMF). For more information, the Relativity Short Message Format guide.

Add search criteria to collect specific data. To configure the data source, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source. You must set a Start Date to complete the Data Sources step.
- **Operator**—choose an operator. For example, equals or greater than.
- **Value**—enter a value to find in the selected field.

The following table lists the filter criteria supported for Claude collections:

All dates are in Coordinated Universal Time (UTC).

Criteria	Operators	Description	Example
Created Date	Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Created Date property in a query, the search returns prompts and responses that exist the day of and after the entered date.	When you search a Created Date of 1/1/2026 to 12/31/2026, Relativity collects all prompts and responses from that date to the end of 2026.
Updated Date	Greater Than, Greater Than or Equals, Less than or Equals	When you use the Updated Date property in a query, the search returns prompts and responses that exist the day of and after the entered date.	When you search a Updated Date of 1/1/2026 to 12/31/2026, Relativity collects all prompts and responses from that date to the end of 2026.

11 Google

Before you collect from a Google data source, Workspace or Gemini, you must complete the following tasks:

Instance	Process	Procedure
Google Workspace	Google above	1. Create a Google Cloud project on the next page 2. Enable required APIs for the project on the next page 3. Set up OAuth2 consent screen on page 45 4. Add scopes on page 45 5. Create credentials on page 46 6. Set reauthentication policy on page 48
	Google Workspace user account setup on page 48	1. Create admin role for Vault API on page 48 2. Create admin role for the user accounts listing on page 49 3. Create admin role for the groups listing on page 49 4. Enable required privileges on page 49
	Restricting collections to the selected user accounts on page 50	1. Create an organizational unit on page 50 2. Add users to the organization unit on page 50 3. Scope user privileges to the organizational unit on page 51
Relativity aiR	Google Workspace data source on page 51	1. Create the data source on page 63 2. Configure the data source in Collect on page 54

Instance	Process	Procedure
	Google Gemini data source on page 61	1. Create the data source on page 63 2. Configure the data source in Collect on page 64

The procedure is the same for any Google Workspace data source and Google Gemini.

11.1 Google Workspace account setup

Connecting your Google Workspace to Collect takes some setup in Google and Relativity. Begin with the credential setup in Google.

11.1.1 Create a Google Cloud project

Create a Google Cloud project to create, enable, and use all Google Cloud services. You will use this account to manage APIs.

To create a Google Cloud project:

1. Open the Cloud Resource Manage page (https://console.cloud.google.com/cloud-resource-manager).
2. Click **Create Project**.
3. Enter information into the fields:
   - **Project name**—enter a memorable name for your project.
   - **Organization**—enter the name of your organization.
   - **Location**—enter the parent organization or folder.
4. Click **Create**.

11.1.2 Enable required APIs for the project

Continuing in this process, you now need to enable the required Google Cloud Console APIs and associate them to a new project.

To start enabling APIs in the Google Cloud Console:

1. In the Google Cloud Console (https://console.cloud.google.com/), select the newly created project.
2. Enter *Google Vault API* in the search bar and search.
3. Click the **Google Vault API** option.
4. Click **Enable**.
   You will then see the Google Vault API/Service Details page.
5. Enter *Admin SDK API* in the search bar and search.
6. Click the **Admin SDK API** option.
7. Click **Enable**.
   You will then see the Admin SDK API/Service Details page.
8. Enter *Cloud Storage API* in the search bar and search.

9. Click the **Cloud Storage API** option.

   Note: Be sure to choose Cloud Storage API. Cloud Storage API is different than Cloud Storage.

10. Click **Enable** if the API is not already enabled by default.

11.1.3 Set up OAuth2 consent screen

Follow the steps to create a OAuth2 consent screen in Google Cloud Console.

1. In the Google Cloud Console (https://console.cloud.google.com/) and select newly created project.
2. Select **APIs & Services>OAuth consent screen**.
3. Click **Get started**.
4. Enter the **App information**.
   - **App name**—enter a name for the Collect app you're using. For example, *Relativity Collect*.
   - **User support email**—select the email address for users to contact you with questions about their consent.
5. Click **Next**.
6. Select **Internal** audience type and click **Next**.
7. Enter an email address in the **Contact Information** field.
   Google uses this email address to notify you about any changes to your project.
8. Click **Next**.
9. Complete the **Finish** step by selecting the check box and click **Continue**.
10. Click **Create**.

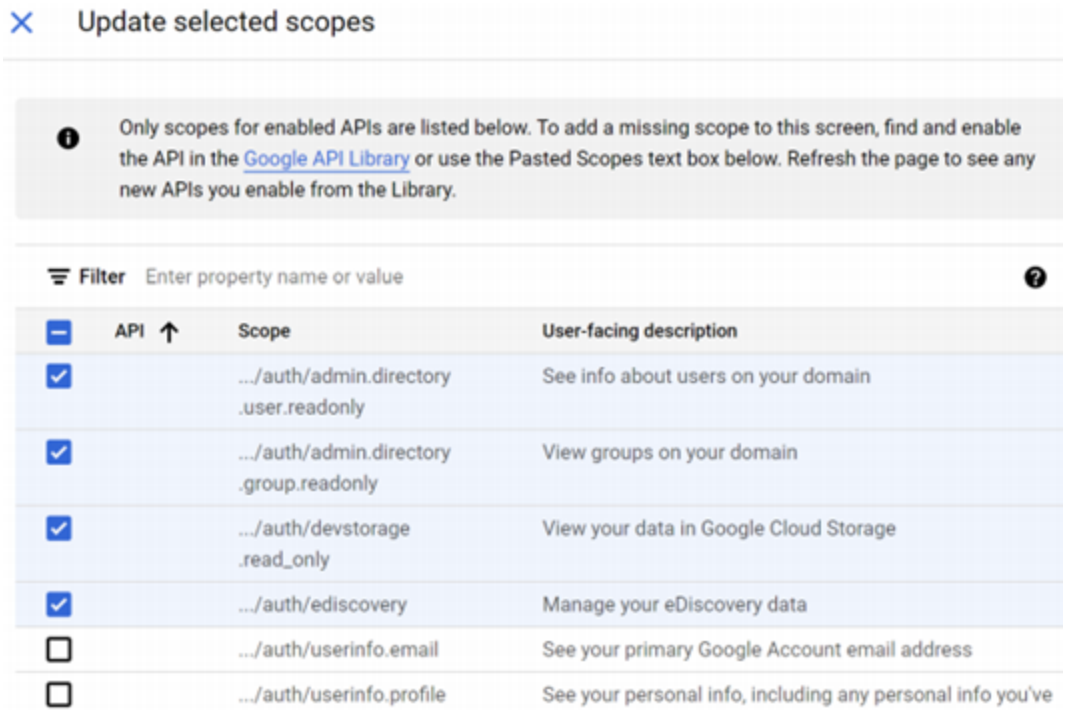
Your Oauth configuration has been created.

11.1.4 Add scopes

Next, you must add scopes.

1. In the Google Cloud Console (https://console.cloud.google.com/), navigate to **Data Access**.
2. Click **Add or remove scopes**.
3. Enter filter and select required scopes one at a time, or enter them in a text box.
   The scopes are:
   - **https://www.googleapis.com/auth/ediscovery**
     Google Vault API | .../auth/ediscovery | Manage your eDiscovery data
   - **https://www.googleapis.com/auth/devstorage.read_only**
     BigQuery API | .../auth/devstorage.read_only | View your data in Google Cloud Storage
   - **https://www.googleapis.com/auth/admin.directory.user.readonly**
     Admin SDK API | .../auth/admin.directory.user.readonly | See info about users on your domain

- **https://www.googleapis.com/auth/admin.directory.group.readonly**
  Admin SDK API | .../auth/admin.directory.group.readonly | View groups on your domain



4. Click **Update**.
5. Click **Save**.

Your data access changes are then saved.

11.1.5 Create credentials

Next, create credentials.

1. In the Google Cloud Console (https://console.cloud.google.com/), navigate to **APIs & Services > Credentials**.
2. Click **Create Credentials**.
3. Click **OAuth Client ID** credentials.
4. Enter the following information in the fields:
   - **Application type**—select Web application.
   - **Name**—enter a name for the credentials.
   - **Authorized redirect URIs**—enter the URI (Uniform Resource Identifier) based on the Relativity aiR Data Center Geo you intend to run collections from.

Note: When copying and pasting the URI, please ensure there are no whitespaces or typos in the address, as they will cause a connection failure with Google.

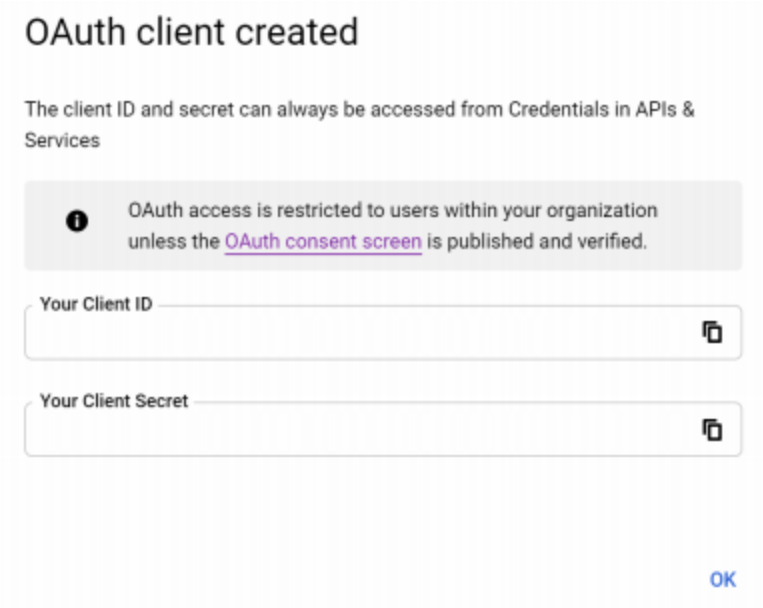
Relativity aiR Data Center Geo URIs

- **Asia (East)**—https://services.esas.relativity.one/collect-oauth-authorization/index.html
- **Asia (Southeast)**—https://services.seas.relativity.one/collect-oauth-authorization/index.html
- **Australia**—https://services.auea.relativity.one/collect-oauth-authorization/index.html

- **Brazil (South)**—https://services.brso.relativity.one/collect-oauth-authorization/index.html
- **Canada (Central)**—https://services.cact.relativity.one/collect-oauth-authorization/index.html
- **Europe (North)**—https://services.noeu.relativity.one/collect-oauth-authorization/index.html
- **Europe (West)**—https://services.wseu.relativity.one/collect-oauth-authorization/index.html
- **Germany (West Central)**—https://services.dect.relativity.one/collect-oauth-authorization/index.html
- **India (Central)**—https://services.inct.relativity.one/collect-oauth-authorization/index.html
- **Japan**—https://services.jpes.relativity.one/collect-oauth-authorization/index.html
- **Korea (Central)**—https://services.krct.relativity.one/collect-oauth-authorization/index.html
- **Switzerland**—https://services.chno.relativity.one/collect-oauth-authorization/index.html
- **United Arab Emirates**—https://services.aeno.relativity.one/collect-oauth-authorization/index.html
- **United Kingdom (South)**—https://services.ukso.relativity.one/collect-oauth-authorization/index.html
- **United States (Central)**—https://services.ctus.relativity.one/collect-oauth-authorization/index.html
- **United States (East)**—the United States (East) geo has six URIs associated to the pod to which your Relativity aiR tenant is assigned. Contact Relativity Support to confirm which URI to use.
    - **Relativity aiR pod esus025000**—
        - https://services.esus.relativity.one/collect-oauth-authorization/index.html
    - **Relativity aiR pod esus025064**—
        - https://services-02.esus.relativity.one/collect-oauth-authorization/index.html
    - **Relativity aiR pod esus025128**—
        - https://services-03.esus.relativity.one/collect-oauth-authorization/index.html
    - **Relativity aiR pod esus025192**—
        - https://services-04.esus.relativity.one/collect-oauth-authorization/index.html
    - **Relativity aiR pod esus008064**—
        - https://services-05.esus.relativity.one/collect-oauth-authorization/index.html
    - **Relativity aiR pod esus022064**—
        - https://services-06.esus.relativity.one/collect-oauth-authorization/index.html
    - **United States (Government)**—
        - https://services.vaus.relativityone.us/collect-oauth-authorization/index.html

5. Click **Create**.

After clicking Create, you will have your Client ID and Client Secret. Copy both of them, because you will need them later when creating the Google data source in Collect.



11.1.6 Set reauthentication policy

In this required step, you must configure Google's reauthentication policy as follows:

1. Open the Google Cloud console (https://admin.google.com/ac/home).
2. Select the newly created project.
3. Click on the Navigation menu.
4. Select **Security > Access and data control > Google Cloud session control**.
5. On the Google Cloud session control, select a reauthentication policy.
    - **Never require reauthentication**
    - **Require reauthentication**. If you select Require authentication, you must also select **Exempt Trust apps**.
6. Click **Save**.

For more information on setting reauthentication policy and the options, see Google's documentation.

11.2 Google Workspace user account setup

Collections require user account on which behalf Relativity exports data. This can be a dedicated or an existing user account.

11.2.1 Create admin role for Vault API

To create the admin role for the Vault API:

1. Open the Google Admin page (https://admin.google.com/ac/home).
2. Click **Account>Admin roles** to open the up the page.
3. Click **Create New Role**.
4. Enter the role name. We recommend *Relativity Collect*.
5. Click **Continue** to select privileges.

6. Select the following privileges:
    - Services - Google Vault > Manage Matters
    - Services - Google Vault > Manage Searches
    - Services - Google Vault > Manage Exports
7. Click **Continue**.
8. Click **Create Role**.

11.2.2 Create admin role for the user accounts listing

To create the admin role for the users accounts listing:

1. Open the Google Admin page (https://admin.google.com/ac/home).
2. Click **Account>Admin roles** to open the up the page.
3. Click **Create New Role**.
4. Enter the role name.
   We recommend *Users Reader for Collect*.
5. Click **Continue**.
6. Select the **Admin API privileges - Users > Read** privilege.
7. Click **Continue**.
8. Click **Create Role**.

11.2.3 Create admin role for the groups listing

To create the admin role for groups listing:

1. Open the Google Admin page (https://admin.google.com/ac/home).
2. Click **Account>Admin roles** to open the up the page.
3. Click **Create New Role**.
4. Enter the role name.
   We recommend *Groups Reader for Collect*.
5. Click **Continue**.
6. Select the **Admin API privileges - Groups > Read** privilege.
7. Click **Continue**.
8. Click **Create Role**.

11.2.4 Enable required privileges

To enable required privileges:

1. Open the Google Admin page (https://admin.google.com/ac/home).
2. Navigate to **Directory > Users** to open the list of users.
3. Select or create the user you want to use.
4. Click the **Admin roles and privileges** pane.

5. In the Roles section, click the **edit pencil icon**, or anywhere in the Roles tables.
6. Assign the following roles to the user in All organizational units scope.
    - Relativity Collect
    - Users Reader for Collect
    - Groups Reader for Collect

11.3 Restricting collections to the selected user accounts

You can restrict collections to the selected group of users by leveraging admin role scoping to organizational units.

To limit collections, you will need to create an organizational unit and add the users to the unit. Once created, Collect will only collect data from the users within the organizational unit.

This configuration step is for Google Workspace data sources only and is optional.

11.3.1 Create an organizational unit

An organization unit restricts Relativity aiR's collections only to the selected custodians. Create an organization unit and add selected custodians to the unit so only their information is collected.

To create an organizational unit, open Google Admin Console and follow the steps below:

1. Open the Google Admin page (https://admin.google.com/ac/home).
2. Navigate to **Directory > Organizational Units**.
3. On the *Manage organizational units* page, click **Create organization unit**.
4. In the *Create new organizational unit* pop-up menu, enter the **Name of organizational unit**.
5. (Optional) Enter description of the organizational unit.
6. Select the **Parent Organization Unit (POU)**.
   If this field is not populated, add a POU. To create a POU, follow the steps in Google's documentation.
7. Click **Create**.

Once the organizational unit is created, the next step is to add targeted users you want to collect from to the unit.

11.3.2 Add users to the organization unit

To add users to the organizational unit, follow the steps below:

1. Click the navigation menu.
2. Navigate to **Directory > Users**.
3. Select the users who should have collections restricted
4. Click the **More options** drop-down menu.
5. Click **Change organizational unit.**
6. In the Change organizational unit pop-up menu, select appropriate organizational unit.
7. Click **Continue**.
8. Click **Confirm**.

You can upload a .csv file to bulk update users. For more information, see Google's documentation.

11.3.3 Scope user privileges to the organizational unit

To update the scope of the user's role:

1. Open the Google Admin page (https://admin.google.com/ac/home).
2. Navigate to **Directory > Users**.
3. Select or create a user account.
4. Select and expand the **Admin roles and privileges** pane.
5. Click the pencil icon.
6. Select a **Role name** to update.
7. Edit the scope of the role to the appropriate organization unit.
8. Click **Save**.

Groups Reader privilege can only be scoped to *All organizational units*. This privilege is only required to enable collections from Google Workspace Groups and it can be omitted. Doing so will disable Groups collections on behalf of this user account.

11.4 Google data sources

Once you complete setting up a Google admin and user account, you can configure Google data sources in Relativity aiR.

Once in Relativity aiR, you can connect the following Google data sources:

- **Workspace**—this includes Google Chats, Drive, Gmail, and Groups. For more information, see Google Workspace data source below.
- **Gemini**—this is Google's generative AI tool. For more information see Google Gemini data source on page 61.

12 Google Workspace data source

This topic provides details on how to capture Google Chats, Drive, Groups, and emails with Collect. Relativity collects Google Drive data using the Vault API.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

12.1 Considerations

Consider the following items about this data source:

- This connector requires a Google Workspace Enterprise Plus license with Vault enabled.
- Each user account you collect from must also have a Google Vault license assigned.
- Collection of Calendar is currently unsupported.

- Google allows a maximum of 20 simultaneous Vault exports per organization.
  - Running more than 20 target collections at the same time can lead to export failures on Google's end.
  - For more details, refer to Manage exports.
- Google does not have a date range limitation.
  - We recommend limiting the date range of the collection.
  - Extended date ranges can increase collection time and potentially create issues.

12.1.1 Grouped collection

Google Chat data is collected into grouped collections. Chat conversations often include multiple custodians in the same message threads or channels. Relativity collects this data as a single grouped data set rather than splitting messages by individual custodian.

For more information on grouped collections, see Grouped collections on page 167.

12.2 Collection size

Google Workspace collections can be large. When collection jobs become too large, performance decreases.

12.2.1 Chat

Chat collections grow quickly due to conversational density, especially in active organizations.

Category	Details
Hard limits (enforced)	30 custodians per job
Planning thresholds (guidance)	Long chat histories become large quickly
When to split	Long date ranges in active orgs
Notes	Collected as RSMF

Limit date ranges for active tenants to prevent rapid growth in job size.

12.2.2 Drive

Drive performance depends more on folder structure than raw data size.

Category	Details
Hard limits (enforced)	30 custodians per job
Planning thresholds (guidance)	Deep folder trees scale poorly
When to split	Large or complex folder structures
Notes	Data shape > raw size

Prioritize simplifying folder scope. Complex hierarchies should be split or targeted.

12.2.3 Gmail

Gmail collections are heavily influenced by Vault export behavior, particularly for long historical ranges.

Category	Details
Hard limits (enforced)	30 custodians per job
Planning thresholds (guidance)	Greater than 15 custodians and greater than 3 years commonly slows exports
When to split	Multi-year collections
Notes	Vault export behavior dominates

Expect slower exports for large historical scopes. Split primarily by time range.

12.2.4 Groups

Groups behave similarly to chat-based sources, especially in high-traffic environments.

Category	Details
Hard limits (enforced)	30 custodians per job
Planning thresholds (guidance)	High-traffic groups over long periods
When to split	Long time windows
Notes	Similar to chat-style sources

Split collections based on traffic volume and duration to control size.

12.3 Create the data source in Collect

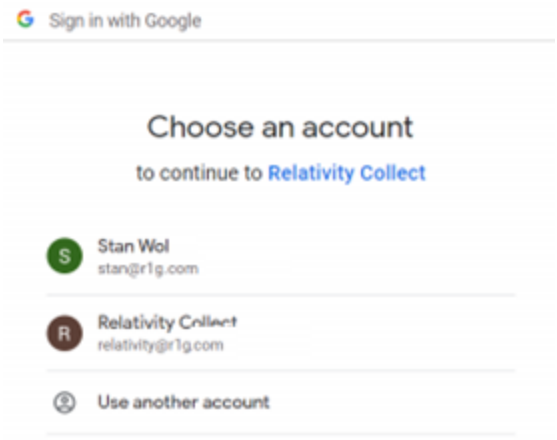
After completing the steps covered above for Google Workspace account setup and user account setup, you can then configure your first Google data source in the Relativity aiR Collect application.

Caution: After generating the Refresh Token in Step 10 below for the first Google data source, be sure to save the token value in a secure location, as it will be needed to set up additional Google data sources. Google only allows **one** refresh token to be generated. If you attempt to generate another refresh token, it will **invalidate** the original token, and you will **not** receive a new one, which will break the data source connection to Google. When setting up additional Google data sources in the Collection application, paste the refresh token value that you saved in a secure location into the refresh token field and click Save.

To add the Google Workspace data source, follow the steps below in Relativity aiR:

1. Navigate to **Collection Admin** within Collect Admin of Set Up.
2. Click the **New Collection Source Instance** button.
3. In the Data Source Information pane, do the following:
   - **Name**—enter in a unique name for the data source.
   - **Type**—select a **Google Workspace** data source. Chat, Drive, Gmail, or Groups.
4. In the Settings pane, enter the **Client Id** and **Client Secret** copied from Google's OAuth2 credentials page. For more information, see Google Workspace data source on page 51.
5. Click **Generate Code**.

6. Select or sign into Google's account on which behalf collections will be performed.



7. Click **Copy Temporary Code** to copy to your clipboard.
8. Once copied, you can close that window and return back to Relativity aiR.
9. In Collect, paste the code in the **Temporary Code** field.
10. Click **Generate Refresh Token**.
    The access token will be generated and populated in the **Refresh Token** field. Refer to the Caution above regarding Refresh Tokens.
11. Click **Save**.

12.4 Configure the data source in Collect

Add criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.
- **Operator**—choose an operator such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

After selecting field options, you must click **Add Criteria**.

Details to know about criteria:

- Each criteria is then separated by an AND operator.
- Leave the data source criteria empty to collect all data from the sources.

Filter a data source's data that you want to collect by adding criteria. This section covers the different criteria for each data source. It also includes what can be searched within each data source. The criteria options change based on the selected data source.

- Google Groups on the next page
- Gmail on page 56
- Google Drive on page 59
- Google Chat on page 60

All dates are in Coordinated Universal Time (UTC).

12.4.1 Google Groups

Setting criteria for Google Groups is not required. For more information on Advanced examples, see Google Workspace documentation.

The following table lists the filter criteria support for Google Workspace Groups collections. Setting criteria for Google Workspace Groups is not required. For more information on Advanced examples, see Google Workspace documentation.

Groups criteria

Criteria	Operators	Description	Example
Advanced	Equals	When you use the Advanced property in a query, specific Google Workspace search criteria become available in Collect. For more information, see Google Workspace documentation.	For more information on Advanced examples, see Google Workspace documentation.
Email BCC	Contains	When you use the Email From property in a query, the search returns all messages that contain the text in the Email BCC field.	If you search "@example.com," your results include all blind carbon copied messages received by people with the @example.com in their email address.
Email CC	Contains	When you use the Email From property in a query, the search returns all messages that contain the text in the Email CC field.	If you search "@example.com," your results include all carbon copied messages received by people with the @example.com in their email address.
Email From	Contains	When you use the Email From property in a query, the search returns all messages that contain the text in the Email From field.	If you search "@example.com," your results include all messages sent by people with the @example.com in their email address.
Email Received Date	Equals, Does Not Equal, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Email Received Date property in a query, the search returns all messages that equal/-doesn't equal, greater/less than the date entered.	If you search "Less Than 1/1/2021," your results include all emails received before January 1, 2021.
Email Sent Date	Equals, Does Not Equal, Greater Than, Greater Than or Equals, Less Than, Less Than or	When you use the Email Sent Date property in a query, the search returns all messages that equal/-doesn't equal, greater/less than the date entered.	If you search "Greater Than 1/1/2001," your results include all emails sent after January 1, 2001.

Criteria	Operators	Description	Example
	Equals		
Email To	Contains	When you use the Email To property in a query, the search returns all messages that contain the text in the Email To field.	If you search “@example.com,” your results include all messages sent to people with the @example.com in their email address.
Has Attachments	Equals, Does Not Equal	When you use the Has Attachments property, the search returns emails with or without attachments based on the Value setting.	If you mark toggle the Value setting On, your results include all messages that include an attachment.
Is Draft	Equals	Indicates whether or not messages are written and not sent. Use the values true or false.	If you mark toggle the Value setting On, your results include all emails that are in the drafted state.
Keyword Search	Search In	When you use the Keyword Search property in a query, the search returns all messages that contain the text you are searching for.	If you search “Dear John,” your results include all messages that contain the text in email body. Note that this is not the same as searching for “Dear” OR “John”. In order to do that you need to enter keywords in separate lines.
Label	Equals	When you use the Label property, the search returns all messages that contains the search word or phrase in the emails' label.	If you search "Important," your results include all emails that are marked with the "Important" label.
Subject	Contains	When you use the Subject property, the search returns all messages that contains the search word or phrase in the email's title.	If you use the Subject property in a query, the search returns all messages which the subject line contains the text you’re searching for. In other words, the query doesn’t return only those messages that have an exact match. For example, if you search for subject “Quarterly Financials,” your results include messages with the subject “Quarterly Financials 2018.”

Included in the Google Workspace Groups Criteria is one toggle:

- **Collect all email with attachments regardless of criteria**—enable the toggle to collect emails and attachments. Disable to collect only emails that match the criteria.

12.4.2 Gmail

Setting criteria for Gmail is not required. For more information on Advanced examples, see Google Workspace documentation.

The following table lists the filter criteria support for Google Workspace Gmail collections. Setting criteria for Google Workspace Gmail is not required. For more information on Advanced examples, see Google Workspace documentation.

Gmail criteria

Criteria	Operators	Description	Example
Advanced	Equals	When you use the Advanced property in a query, specific Google Workspace search criteria become available in Collect. For more information, see Google Workspace documentation.	For more information on Advanced examples, see Google Workspace documentation.
Email BCC	Contains	When you use the Email From property in a query, the search returns all messages that contain the text in the Email BCC field.	If you search "@example.com," your results include all blind carbon copied messages received by people with the @example.com in their email address.
Email CC	Contains	When you use the Email From property in a query, the search returns all messages that contain the text in the Email CC field.	If you search "@example.com," your results include all carbon copied messages received by people with the @example.com in their email address.
Email From	Contains	When you use the Email From property in a query, the search returns all messages that contain the text in the Email From field.	If you search "@example.com," your results include all messages sent by people with the @example.com in their email address.
Email Received Date	Equals, Does Not Equal, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Email Received Date property in a query, the search returns all messages that equal/-doesn't equal, greater/less than the date entered.	If you search "Less Than 1/1/2021," your results include all emails received before January 1, 2021.
Email Sent Date	Equals, Does Not Equal, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Email Sent Date property in a query, the search returns all messages that equal/-doesn't equal, greater/less than the date entered.	If you search "Greater Than 1/1/2001," your results include all emails sent after January 1, 2001.
Email To	Contains	When you use the Email To property in a query, the search returns all messages that contain the text in the Email To field.	If you search "@example.com," your results include all messages sent to people with the @example.com in their email address.
Has Attachments	Equals, Does Not Equal	When you use the Has Attachments property, the	If you mark toggle the Value setting On, your results include all messages that include an attachment.

Criteria	Operators	Description	Example
		search returns emails with or without attachments based on the Value setting.	
Is Draft	Equals	Indicates whether or not messages are written and not sent. Use the values true or false.	If you mark toggle the Value setting On, your results include all emails that are in the drafted state.
Keyword Search	Search In	When you use the Keyword Search property in a query, the search returns all messages that contain the text you're searching for.	If you search "Dear John," your results include all messages that contain the text in email body. Note that this is not the same as searching for "Dear" OR "John". In order to do that you need to enter keywords in separate lines.
Label	Equals	When you use the Label property, the search returns all messages that contains the search word or phrase in the emails' label.	If you search "Important," your results include all emails that are marked with the "Important" label.
Subject	Contains	When you use the Subject property, the search returns all messages that contains the search word or phrase in the email's title.	If you use the Subject property in a query, the search returns all messages which the subject line contains the text you're searching for. In other words, the query doesn't return only those messages that have an exact match. For example, if you search for subject "Quarterly Financials," your results include messages with the subject "Quarterly Financials 2018."

Included in the Google Workspace Gmail Criteria is one toggle:

- **Collect all email with attachments regardless of criteria**—enable the toggle to collect emails and attachments. Disable to collect only emails that match the criteria.
  - If you are using keyword search criteria, we recommend enabling the toggle, regardless of keyword search results.
  - Use the *Collect all emails with attachments regardless of criteria* to collect all emails with attachments, including ones that do not match the selected keyword search criteria.
    - **Enabled**—toggle on to collect emails that match the keyword search criteria, emails that match other criteria such as date range, and all emails with attachments regardless of keyword search criteria.
      For example, if you add a date range and keywords, Collect pulls the following:
      - Emails with keywords in the body.
      - Emails within the specified date range.
      - Emails with attachments within the date range.
    - **Disabled**—toggle off to collect only emails that match the search criteria.
  - Other filter criteria still applies to the collection. For example, if you specify a date range along with keywords, Collect does not return any emails outside the date range. It returns the emails within the date range that are either responsive to the keywords or have an attachment.

- **Collect Linked Files**—enable the toggle to collect linked files related to Gmail emails in the mailbox export. Linked files can be, for example, PDF file, picture file, PowerPoint file, and so forth, that is linked from Google. Disable to exclude linked files related to Gmail emails in the mailbox export.

12.4.3 Google Drive

Setting criteria for Google Drive is not required. For more information on Advanced examples, see Google Workspace documentation.

Note: Google Vault API usage limits do not permit more than 20 exports to be in progress simultaneously across your *entire* organization. If you have very large matters and need the maximum to be increased, contact Google for assistance. For more information, refer to Google Vault documentation on usage limits and usage quota increases.

The following table lists the filter criteria support for Google Workspace Drive collections. Setting criteria for Google Workspace Drive is not required. For more information on Advanced examples, see Google Workspace documentation.

Drive criteria

Criteria	Operators	Description	Example
Advanced	Equals	When you use the Advanced property in a query, specific Google Workspace search criteria become available in Collect. For more information, see Google Workspace documentation.	For more information on Advanced examples, see Google Workspace documentation.
File Type	Equals	When you use the File Type property in a query, the search returns all files that equals what is entered.	If you select "Google Sheets" as your value, your results include Google Sheet files.
Filename	Contains	When you use the Filename property in a query, the search returns all files that contain the value entered.	If you search "Important_Document," your results include all files with "Important_ Document" in the filename.
Keyword Search	Search In	When you use the Keyword Search property in a query, the search returns all files that contain the text you're searching for.	If you search "Dear John," your results include all messages that contain the text in the file. Note that this is not the same as searching for "Dear" OR "John". In order to do that you need to enter keywords in separate lines.
Modification Date	Equals, Does Not Equal, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Modification Date property in a query, the search returns all files that equal/doesn't equal, greater/less than the selected date.	If you search "Less Than 1/1/2021," your results include all files received before January 1, 2021.
Owner	Contains	When you use the Owner property in a query, the search returns all messages that contain the text in the Owner field.	If you search "Iscovery," your results include all files sent by people with the "Iscovery" in their name, such as "Ed Iscovery."
Shared By	Contains	When you use the	If you search "ExampleUser1," your results include all filed shared by people with the

Criteria	Operators	Description	Example
		Shared By property in a query, the search returns all files that contain the text in the Shared By field.	UserExample1 in their name.
Shared With	Contains	When you use the Shared With property in a query, the search returns all files that contain the text in the Shared With field.	If you search “UserExample1,” your results include all files shared with people with the UserExample1 in their name.
Version Date	Equals	When you use the Version Date property in a query, the search returns the version of files on the selected date.	If you search 1/1/2021, your results include only the version of the files on 1/1/2021. The results won't include earlier or later versions of the file.

Included in the Google Workspace Drive Criteria is one toggle:

- **Collect files from shared drives**—enable the toggle to retrieve data from shared drives, along with personal drives, that match the criteria. Disable to collect only data from personal drives that match the criteria.

12.4.4 Google Chat

Setting criteria for Google Workspace Chat is not required. For more information on Advanced examples, see Google Workspace documentation.

The following table lists the filter criteria support for Google Workspace Chat collections. Google Workspace Chat data is collected in RSMF.

Chat criteria

Criteria	Operators	Description	Example
Advanced	Equals	When you use the Advanced property in a query, specific Google Workspace search criteria become available in Collect. For more information, see Google Workspace documentation.	For more information on Advanced examples, see Google Workspace documentation.
Content Type	Equals	When you used the Content Type property in a query, the search returns messages with specific file types.	If you search with the value set to Google Docs, your results include all Google Docs sent as messages.
Keyword Search	Equals	When you use the Keyword Search property in a query, the search returns all messages that contain the text you’re searching for.	If you search “Dear John,” your results include all messages that contain the text in email body. Note that this is not the same as searching for “Dear” OR “John”. In order to do that you need to enter keywords in separate lines.
Message Source	Equals	When you use the Message Source property in a query, the search returns all direct messages or all messages in rooms.	If you search with the value set to "Messages in Rooms," your results include only messages sent in a group chat and no direct messages will be included.
Sent/Updated Date	Greater Than or Equals,	When you use the Sent/Updated property in a query, the search	If you search “Greater Than 1/1/2001,” your results include all messages sent after Janu-

Criteria	Operators	Description	Example
	Less Than, Less Than or Equals	returns all messages that equal/-doesn't equal, greater/less than the date entered.	ary 1, 2001.
Slice Interval in Hours	Equals	When you use The Slice Interval in Hours property, the search returns all messages in a specific time range or defaults the slice interval to 24 hours.	If you search with a slice interval set to one hour and a conversation spans five hours, you will end up with five RSMFs after processing.
User At	Contains	When you use the User At property in a query, the search returns all messages that contain the text in the User At field.	If you search "UserExample1" your results include all messages sent to people with the UserExample1 in their email address.
User From	Contains	When you use the User From property in a query, the search returns all messages that contain the text in the User From field.	If you search "ExampleUser1," your results include all messages sent by people with the UserExample1 in their email address.

Included in the Google Workspace Chat Criteria are two toggles:

- **Include results from Spaces**—enable this toggle to include all messages in spaces, along with direct messages, that match your query. Disable to collect only direct messages that match your query.
- **Disable RSMF conversion**—enable this toggle to keep data in its original format by preventing Relativity from converting the files into Relativity's short message format (RSMF) files.

  Note: Relativity provides you win .json files when running collections with this toggle enabled.

12.5 Troubleshooting

This table includes troubleshooting for Google's data sources.

Error	Cause	Resolution
The token is invalid. You must remove access and generate a new refresh token.	Your token is invalid. This could be due to changing the account owner.	While signed in with your account, navigate to https://myaccount.google.com/u/0/permissions. In the page, click **Remove Access**. Then generate a new refresh token. For more information on generating a refresh token, see Google Workspace data source on page 51

13 Google Gemini data source

This topic provides details on how to capture Google Gemini chat data with Collect.

Relativity aiR collects Gemini Chat data and automatically converted to Relativity's short message format (RSMF).

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

13.1 Considerations

Note the following considerations about this data source:

- This connector requires a Google Workspace Enterprise Plus license with Vault enabled.
- Each user account you collect from must also have a Google Vault license assigned.
- Gemini conversations are retained and made accessible based on your organization's Vault retention policies.
- This connector collects Google Chat messages, including Gemini-enhanced threads, through the Google Vault API.
- Google allows a maximum of 20 simultaneous Vault exports per organization. Running more than 20 target collections at the same time can lead to export failures on Google's end. For more details, refer to Manage exports.
- If your organization uses multiple Google Workspace domains or organizational units, you must configure a separate data source for each in the Collect application. We recommend that you clearly name each data source to identify the workspace it is connecting to.
- Relativity supports both persistent and ephemeral conversations, provided they fall within the configured retention window in Vault.
    - Ephemeral conversations are those where messages are not retained in the user's chat history but are accessible with the Vault API.
    - These are returned in Collect if Vault retention is enabled and search filters align with message dates.

13.2 Advanced Gemini features

Several advanced Gemini features are not currently included in Vault exports. This means they will not be seen in our RSMF output.

These limitations are inherent to Google's current export behavior and not Collect-specific.

Currently, in some cases, Google Vault exports may include placeholder links, or immersive chips, for these features.

- When the immersive chips are available, Relativity inserts a Gemini Content Description based on the accompanying summary text provided by Google.
- This content description offers limit context and does not include full visual or interactive content.

Google has indicated that there will be support for these features in the future.

The advanced features include:

- Canvas
- Deep Research responses
- Uploaded images
- Citations
- Custom assistant names
- Annotation metadata

13.3 Prerequisites

You must set up and configure a Google Cloud project before creating the data source in Relativity aiR. For more information, see Google on page 43.

Complete the following before setting up a Google Gemini data source in Relativity:

- Set up a Google Cloud project and enable the following APIs:
  - Google Vault API
  - Admin SDK API
  - Generate OAuth 2.0 credentials:
  - Client ID and Client Secret
- Grant the required access scopes during OAuth configuration:
  - https://www.googleapis.com/auth/admin.directory.user.readonly
  - https://www.googleapis.com/auth/ediscovery
- Confirm that target user accounts and chat spaces are covered by an active Vault retention policy.

For detailed steps, see Google on page 43.

Once you complete the prerequisites, you can begin creating the data source.

13.4 Collection size

Gemini is a newer source with evolving performance patterns, particularly for long interaction histories.

Category	Details
Hard limits (enforced)	No explicit hard cap published
Planning thresholds (guidance)	High interaction volume over long periods
When to split	Long-running interaction history
Notes	Newer source with evolving behavior

Use conservative scoping until performance characteristics are better established.

13.5 Create the data source

Use the following procedure to connect the Google Gemini data source to Collect.

In Relativity aiR:

1. Navigate to **Collection Admin**.
2. Click the New Collection Source Instance button.
   1. **Name**—enter a unique name for the data source.
   2. **Type**—select the Google Workspace data source.
   3. **Settings**—enter the required information in the Settings fields. For more information, see Settings fields on the next page.
3. Click **Save**.

The data source displays on the Collection Admin page.

13.5.1 Settings fields

To connect Relativity to a Google Gemini workspace, you need to gather and enter the information for the following fields.

- **OAuth Client ID**—enter the client ID created in your Google Cloud project.
- **OAuth Client Secret**—enter the client secret linked to the above client ID.
- **Super Admin Email**—enter the email address of a super admin account in your Google Workspace domain. This enables user impersonation for Vault access.

Note: You must complete OAuth app setup in your Google Cloud console and approve domain-wide delegation before using these credentials.

13.6 Configure the data source in Collect

Add criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.
- **Operator**—choose an operator such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

After selecting field options, you must click **Add Criteria**.

All dates are in Coordinated Universal Time (UTC).

Criteria	Operators	Description	Example
Start Date	Greater Than or Equals	When you use the Start Date property in a query, the search returns messages that exist the day of and after the entered date.	When you search a Start Date of 1/1/2024, Relativity collects all messages from that date to today.
End Date	Less Than or Equals	When you use the End Date property in a query, the search returns messages that exist the day of and before the entered date.	When you search an End Date of 1/31/2024, Relativity collects messages from the beginning of time through that date.
Custodian Email	Equals	Filters for messages involving the specified user's email address.	Messages sent or received by user-@company.com are included.
Conversation ID	Equals	Filters for a specific conversation or message thread in Gemini Chat.	Collects messages associated with conversation ID 17:abc123xyz456....
Workspace ID	Equals	Filters messages within a specific Google Chat space, room or group chat.	Collects from the space with ID spaces/AAAAB3NzaC1yc2....
Keyword	Contains	Filters for messages containing one or more specified search terms or phrases.	"project launch" OR "contract signed"

Note: Temporary, or ephemeral, chats will also be returned if they occurred within the Vault retention window and meet your search criteria.

14 iManage data source

This topic provides details on how to capture data from iManage cloud instances with Collect.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

Your iManage account needs to have an iManage support account. To get an iManage support account, please refer to iManage's documentation. You must also connect it to Collect using the steps below.

14.1 Considerations

Consider the following before collecting from the iManage data source:

- iManage Control Center must be configured for Password authentication and not SSO. Collect application authentication relies on password authentication and is not compatible with SSO.
- This data source connector only works with cloud versions of iManage. We cannot collect from on-premise instances of iManage.
- If you are a Relativity aiR Government customer and are using iManage Cloud, you do not need to take different steps to authenticate or to collect data.
- Custodial-only support. Collecting iManage data without a custodian, non-custodial collection, is not supported.
    - Collect currently supports custodial collections only for the iManage data source.
    - Collections require selecting one or more custodians, and collection scope is based on user access.

14.2 Prerequisites

Complete the following before collecting from the iManage data source:

- Before configuring the Collect application in your iManage tenant, you need to submit an email to appregistration@imanage.com.
    - The sender's email address must be associated with a valid iManage Help Center account.
    - In the email, request to add the Collect application to your iManage tenant.
    - The request should include:
        - The following statement: *This is for the Relativity Collect application.*
        - Your organization or company name.
        - Your iManage tenant ID.
- If you have IP restrictions in your environment, you must add a Relativity aiR IP address in the iManage Control Center. For more information, log into the Community site to viewthe Relativity aiR - Firewall Outbound IP Addresses file.
- If you are using iManage Cloud Classic, you must add your tenant-specific iManage API endpoint URL to the allowlist in Relativity aiR Government before running collections.

- This is because in Cloud Classic, the endpoints are unique for each iManage customer.
- You will need to work with the Relativity aiR implementation team to add your API endpoint URL to the allowlist.

14.3 Collection size

iManage performance depends on repository size and backend configuration.

Category	Details
Hard limits (enforced)	No global hard cap
Planning thresholds (guidance)	Large repositories slow down
When to split	Very large workspaces
Notes	Backend configuration matters

Tailor job size to repository scale and environment configuration.

14.4 Task checklist

The table lists the order to perform the necessary tasks for setting up the data source for Collect.

Order	Application	Task
1	iManage	Setting up Relativity Collect in iManage below
2	Collect	Creating the data source in Collect on the next page
3	Collect	Configuring the data source in Collect on page 68

14.5 Setting up Relativity Collect in iManage

To set up Collect in iManage, you need to have the App Management role permission in iManage. For more information, see iManage documentation on adding an application package. Then, use the following procedure to configure the application.

Note: iManage Control Center must be configured for Password authentication and not SSO. Collect application authentication relies on password authentication and is not compatible with SSO.

1. In the iManage Control Center, navigate to the **Settings > Applications** pane.
2. Click **Add Application**.
3. In the available applications list, search for and select the **Relativity Collect** application.
4. Click **Authentication** to configure the OAuth settings.
5. In the OAuth settings, leave the default options:

   Note: Collect uses a service account's username and password stored in the data source. This allows Collect to automatically re-authenticate and request a new access token when the previous one expires, without requiring a user to log in every 30 minutes.

- **Allow Refresh Token**—No
- **Refresh Token Expiry**—default, 365 days
- **Access Token Expiry**—default, 30 minutes

6. Click **Access** to configure which service account can access the Relativity Collect application in iManage.
7. Set **Allow Access** to *Custom* to give access to specific users or groups to use the application.
8. Search for and select the service account you want to provide access to use the application. Collect requires this account and the associated password when setting up the iManage data source connection in Relativity aiR.
9. Select **Review** to view your changes.
10. Click **Finish**.

Once you have completed setting up the Collect application in iManage, do the following:

1. Click on the application in the Applications Explorer.
2. Click **View**.
   The Client ID displays in the application view, but the Client Secret does not. iManage will provide it to you.

Notes:

- You need the Client ID and Client Secret later when setting up your iManage data source connection in the Collect application so be sure to make note of them.
- Relativity bases permissions off the account you selected for granting application access to. The scope of what is visible for collections will be dependent on the permissions of that user account.

14.5.1 Permissions

Collect bases the permissions off the account you use to authenticate with the iManage API. Ensure the service account has enough permissions to view any files or folders you want to collect.

14.5.2 Throttling

Collect handles throttling by reading the response headers for each API call Relativity makes for the header *x-ratelimit-remaining*. When that header value returns 0, Relativity looks for another header value called *x-ratelimit-reset*. The x-ratelimit-reset value specifies the amount of time in seconds to wait until Collect no longer needs to. After the wait, the module will retry the throttled API call.

14.6 Creating the data source in Collect

In Relativity aiR, use the following procedure to connect the iManage data source to Collect.

1. Navigate to **Collection Admin** within Collect Admin of Set Up.
2. Click the **New Collection Source Instance** button.
3. Do the following:
   - **Name**—enter in a unique name for the data source.
   - **Type**—select the **iManage** data source.
   - **Settings**—enter the required information in the Settings fields. For more information, see Settings fields on the next page.

4. Click **Save**.

For more information, see Creating a collect data source on page 22.

14.7 Settings fields

To connect Relativity to an iManage data source, you need to gather and enter the information for the following fields:

- **Client ID**—enter the Client ID for the application.
- **Client secret**—enter the Client Secret for the application.
- **Username**—enter the iManage user name.
- **Password**—enter the iManage password.
- **Library ID**—enter the name of the iManage database.
- **iManage Base address**—enter the base address that points to the domain or sub-domain of your iManage Cloud instance. For example, https://cloudimanage.com, https://CustomSubdomain.cloudimanage.com or https://example.goimanage.com, https://CustomSubDomain.goimanage.com. If the URL contains cloud-imanage.com, Collect targets the Cloud. If it does not contain that, then Collect targets Classic Cloud.

14.7.1 Data source details

Each data source details page includes an Actions console. The options available will be different for each data source.

You can click **Validate Connection** to validate to validate the client ID, certificate, and other credentials with iManage.

14.8 Configuring the data source in Collect

Configure the data sources chosen in the Collection Details step. If you select multiple data sources in the first step, you'll configure all sources in the step. Switch between each source by clicking the name of the data source in the left navigation menu. Clicking **Next** and **Previous** also moves you through the data sources. Select individual data sources by clicking on the checkbox and then using the right arrows to select them. After selecting the data sources to configure, fill out the criteria. Each data source has different criteria to enter.

Add search criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.
- **Operator**—choose an operator, such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

The following table lists the filter criteria supported for iManage collections. Setting criteria for iManage is not required. If you have not selected criteria, Relativity collects all results by default.

All dates are in Coordinated Universal Time (UTC).

The Less Than operator is only supported when used in conjunction with Greater Than or Equals.

Criteria	Operators	Description	Example
Creation Date	Greater than or equals; Less than or	When you use the Creation Date property in a query, the search returns	If you search “Greater than or equals 1/1/2001,” your results include all emails sent on and after January 1, 2001.

Criteria	Operators	Description	Example
	equals	all data that equals greater/less than the date entered.	
Document Class	Equals	When you use the Document Class property, the search returns data with the entered document class	If you search for a document class that equals one of your custom-defined class categories, your results will include documents only in that class.
Document Subclass	Equals	When you use the Document Subclass property, the search returns data with the entered document subclass	If you search for a document subclass that equals one of your custom-defined subclass categories, your results will include documents only in that class.
Edit Date	Greater than or equals; Less than or equals	When you use the Edit Date property in a query, the search returns all data that equals greater/less than the date entered.	If you search “Greater Than 1/1/2001,” your results include all documents edited after January 1, 2001
File Extension Exclusion	Equals	When you use the File Extension Exclusion property, the search returns data without the entered file extension.	If enter .csv, your results include all data that does not include .csv files.
File Extension Inclusion	Equals	When you use the File Extension Inclusion property, the search returns data with the entered file extension.	If enter .csv, your results include all data that does include .csv files.
iManage Custom1-16 value	Equals	When you use the iManage Custom1-16 Value properties in a query, the search returns all data that equals the entered value in its Custom 1 Property within iManage.	If you search for an iManage Custom1-16 value, your results will include documents that match your custom value between 1 and 16. For more information, see iManage custom fields documentation.
iManage Custom21-24 Value	Greater than or equals; Less than or equals	When you use the Edit Date property in a query, the search returns all data that equals greater/less than the date entered.	If you search for an iManage Custom21-24 value, your results will include documents that match your custom value between 1 and 16. For more information, see iManage custom fields documentation.
iManage Custom25-28 Value	Equals, Does Not Equal	When you use the iManage Custom25 Value property in a query, the search returns all data that matches the entered value in its Custom 25 Property	If you search for an iManage Custom25 value, your results will include documents that match your custom value 25. For more information, see iManage custom fields documentation.

Criteria	Operators	Description	Example
		within iManage.	
iManage Custom29-30 Value	Equals	When you use the iManage Custom29-30 Value property in a query, the search returns all data that equals the entered value in its Custom 29-30 Property within iManage.	If you search for an iManage Custom29-30 value, your results will include documents that match your custom value between 29-30. For more information, see iManage custom fields documentation.
iManage Workspace Name	Equals	When you use the iManage Workspace name property, the search returns all data within the workspaces that equals the search word or phrase in the workspace's name.	If you use the iManage Workspace Name property in a query, the search returns all data that the workspace name equals the text you're searching. In other words, the query doesn't return only the data from channels that have an exact match. For example, if you search for "finance_team," your results include data from workspaces like "finance_team_project."
Received Date	Greater than or equals; Less than or equals	When you use the Received Date property in a query, the search returns all messages that equals, greater/less than the date entered.	If you search "Less than or equals 1/1/2023," your results include all data received on and before January 1, 2021.
Recipient SMTP	Equals	When you use the Recipient SMTP property in a query, the search returns all data that matches the text in the Recipient SMTP field.	If you search "iManage," your results include all messages sent to iManage SMTPs.
Search Term - Anywhere	Equals	When you use the Anywhere Search Term property in a query, the search returns all data because iManage does not support this search criteria.	iManage does not support this search criteria.
Search Term - Body	Equals	When you use the Body Search Term property in a query, the search returns all data that matches the text you are searching.	If you search "Dear John," your results include all data that contains the text in body. Note that this is not the same as searching for "Dear" OR "John". In order to do that you need to enter keywords in separate lines.
Search Term - Subject	Equals	When you use the Subject Search Term property, the search returns all messages that contains the search word or phrase in the data's subject.	If you use the Subject Search Term property in a query, the search returns all data that the subject line contains the text you're searching. In other words, the query doesn't return only those messages that have an exact match. For example, if you search for subject "Quarterly Financials," your results includes data with the subject "Quarterly Financials 2023."

Criteria	Operators	Description	Example
Sender SMTP	Equals	When you use the Sender SMTP property in a query, the search returns all data that matches the text in the Sender SMTP field.	If you search “iManage,” your results include all messages sent from iManage SMTPs.
Sent Date	Greater than or equals; Less than or equals	When you use the Sent Date property in a query, the search returns all data that is greater than or equals or less than or equals the date entered.	If you search “Greater than or equals 1/1/2001,” your results include all data sent on or after January 1, 2001.

15 Microsoft 365 - Inactive mailboxes data source

This topic provides details on how to capture Microsoft 365 Inactive mailboxes with Collect.

Outlook mailboxes become inactive mailboxes when an account is deleted while under a preservation hold.

- When deleted, Microsoft does not throw the mailbox away.
- Microsoft keeps it in inactive state until the related preservation or retention hold is over.

After all retention policies or holds are removed in Microsoft, the inactive mailbox changes to a soft-deleted mailbox. The 30-day deletion period starts only after the mailbox reaches the soft-deleted state.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

15.1 Considerations

Consider the following about Microsoft 365 Inactive mailboxes data sources:

- The inactive mailbox connector uses Microsoft's Purview API.
- Purview Cases will be created in your Microsoft Purview instance to facilitate the search and export of inactive mailboxes.
- Relativity collects all available files including preserved files.
  - You do not need to take extra steps to collect preserved files as they are automatically included in the collection.
  - For more information on preserving data, see the Legal Hold guide.
- Inactive mailbox export requires an account with the eDiscovery Manager role and an Azure AD app registration that has the required delegated permissions.
- Microsoft APIs do not support verifying that an inactive mailbox exists prior to collection. You will see failed collections in cases where the mailbox no longer exists.
- Relativity collects inactive mailboxes as .pst files.

- If the password changes on the account used to generate the refresh token, all existing refresh tokens are invalidated. To continue collecting, go to Collect Admin, select the data source, click Edit, and generate a new refresh token.

15.2 Collection size

Microsoft 365 collections can be large. When collection jobs become too large, performance decreases.

Large collections	Best practices
200 GB per search	Reduce search size
Multi-TB exports	Limit the number of custodians per job. Collect max 30 custodians per job.
Long date ranges with many mailboxes	Using smaller date ranges.

15.2.1 Export duration for large mailboxes

Export duration is determined primarily by mailbox size and whether or not date range criteria are being used, as well as the current load on Microsoft's services. Purview eDiscovery runs on shared, multi-tenant Microsoft 365 infrastructure, and Microsoft does not provide a service-level agreement or guaranteed throughput for export operations.

Exports occur in two phases, and each contributes to the overall duration:

- **Phase 1**—export preparation on the Microsoft side. Microsoft packages the mailbox data before transferring any documents.
  - While this phase is in progress, the document counter on the Collect monitoring page remains at zero, which is normal.
  - The counter reflects documents received by Collect. Nothing is transferred until preparation finishes.
  - For large mailboxes, this phase alone can take several hours or longer.
- **Phase 2**—data transfer. When preparation completes, documents begin transferring to Collect and the counter starts incrementing.
  - Microsoft throttles transfer throughput. Throughput is typically around 2 GB per hour per mailbox.
  - Completion of the preparation phase does not mean the collection is nearly finished.
  - A 25 GB mailbox may require 12 or more hours of transfer time after preparation completes.

A mailbox larger than 25 GB may take several hours to more than 24 hours to fully collect.

Do not cancel or restart a collection solely because progress appears slow. Doing so restarts the export preparation from the beginning.

If a large mailbox collection shows zero documents for more than 48 hours, contact Relativity Support.

15.3 Task checklist

The table lists the order to perform the necessary tasks for setting up the data source for Collect.

Note: Separate Microsoft data sources inside Collect can use the same Microsoft Azure app registration. This means you only need to create one Microsoft Graph application and provide one Client ID and one Client Secret. You can then enter that same set of credentials for Microsoft data sources within Collect.

Order	Application	Task
1	Azure	Registering the Collect application below
2	Azure	Obtaining a client secret on the next page
3	Azure	Setting API permissions on the next page
4	Azure	Adding a redirect URI on page 75
5	Collect	Creating the data source in Collect on page 77
6	Collect	Configuring the data source in Collect on page 78

15.4 Accessing Microsoft 365 tenants

Register the Collect application to access Microsoft 365.

When registering the application, the Microsoft 365 administrator creates a Microsoft Application ID and secret. Relativity uses this ID and secret to configure data sources in Collect and provides access to the Microsoft 365 tenants.

You can register the application through Azure Portal or by registering the delegated permissions through the Microsoft App Registration Portal. After registering the application, request administrator consent. From there, it is possible to revoke application access.

Depending on your Relativity aiR license, commercial or government, and your Microsoft tenant, Microsoft 365 or Microsoft 365 Government, you will be able to collect from either Microsoft 365 or both Microsoft 365 and Microsoft 365 Government data sources. Commercial users can only collect from Microsoft 365 tenants. Government users can collect from Microsoft 365 and Government 365 tenants. These data sources act the same, but have different icons within Collect.

15.4.1 Registering the Collect application

Start with registering your application in the Azure portal by following the steps below.

Caution: The listed permissions and roles are required and supported by Relativity.

- Relativity does not support substitutions or reduced permissions.
- You can submit requests for alternative or reduced permissions as product feedback.

For more information on registering an application in the Azure portal, refer to documentation on Microsoft's site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Click **App registrations**.
4. Click **New Registration** to display the Register an application page.
5. Enter an application name in the **Name** field.
6. Accept the default setting, **Accounts in this organizational directory only**, as the supported account type.
7. Click **Register**.
8. Once the application is registered, make note of the **Application (client) ID** and **Directory (tenant) ID** for use later when configuring the data source in Relativity aiR Collect.

15.4.2 Obtaining a client secret

Next, obtain the client secret for the registered application in the Azure portal. For more information, see relevant Microsoft documentation on the Microsoft site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **Certificates & secrets** option in the left navigation bar.
2. Click the **Client secrets** tab.
3. Click **New client secret**.
4. Enter a description for the client secret in the **Description** text box.
5. Select **730 days (24 months)** from the Expires list. The client secret will expire after this time frame.
    - Once the client secret expires, you must create a new client secret in the Azure portal as described in these steps.
    - Then you must update your Microsoft 365 Collect data sources with it. For more information, see Expired Azure client secrets below.
    - For any additional assistance with client secrets, please contact the Azure Admin in your organization.
6. Click **Add** to create a new secret.

    Caution: Microsoft will only show the secret value this one time. There is no way to recover a secret.

7. Click the copy icon to copy the **Secret Value** to the clipboard.
    - Paste it to a safe location.
    - You will use the Secret Value later when creating the data source in Collect.
    - Confirm you copy the *Secret Value* and not the Secret ID.
8. Give your Relativity Admin the Application ID and the Client Secret for setup of Collect.
    - This application secret is also needed for setting up a Microsoft Entra ID integration point.
    - For more information, see the Integration Points guide.

15.4.2.1 Expired Azure client secrets

If your Azure client secret expires, follow these steps:

1. Get a new secret as outlined in the steps above.
2. Go to **Collect Admin** in Relativity aiR.
3. Select the desired data source that has expired, and click **Edit**.
4. Input the new client secret value in the **Application Secret** field.
5. Click **Save**.

You must repeat these steps for all Microsoft data sources that you have set up.

15.4.3 Setting API permissions

Each data source has its own set of permissions necessary to allow access to the tenants. To add the correct permissions based on your selected Microsoft 365 data source, follow the steps below.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **Manage > API permissions** option in the left navigation bar.

   Note: The *User.Read* permission is automatically added by default.

2. Click **Add a permission**.
3. Click **Graph API**.
4. Select **Delegated Permissions**.
5. Select the **eDiscovery.ReadWrite.All** permission from the Permission list.
6. Click **Add permissions**.
7. Click **Grant Permission**.
   The window will show all permissions granted.
   - Make a note of the application ID that Microsoft assigned to the app registration.
   - This ID is also required for setup of data sources in Collect.
8. Click **Add a permission**.
9. Select **APIs my organization uses**.
10. Search for **MicrosoftPurviewEDiscovery**.
    - If *MicrosoftPurviewEDiscovery* does not appear in the APIs my organization uses list, you must first register the app in Microsoft Entra ID.
    - For more information, see Microsoft's Register the MicrosoftPurviewEDiscovery app in Microsoft Entra ID documentation.
11. Select **Application Permissions**.
12. Select the **eDiscovery.Download.Read** permission from the Permission list.
13. Click **Add permissions**.
14. Click **Grant Permission**.
    The window will show all permissions granted.
    - Make a note of the application ID that Microsoft assigned to the app registration.
    - This ID is also required for setup of data sources in Collect.
15. Verify that all permissions have been granted.
16. Click **Add permissions**.
17. Click **Grant Permission**.
18. Click **Accept** to grant the permissions.

All API permissions have been granted and you can start creating the data source in Relativity aiR.

15.5 Adding a redirect URI

After setting up API permissions, you must add a Redirect URI to the Azure Application Registration. Add the Redirect URI with the following steps:

1. In the left-side menu console, click **Authentication**.

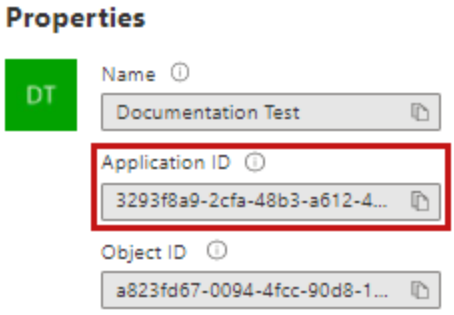
   Note: It may appear as **Authentication (Preview)**.

2. Click **Add Redirect URI**.
3. Click **Web**.
4. Enter your Redirect URI.
   - Your Redirect URI is your Relativity aiR tenant domain URL plus */collect-services/api/v1/Authentication/ms-auth-response*.
   - For example, *https://acme.corp.relativity.one/collect-services/api/v1/Authentication/ms-auth-response*

15.6 Finding Azure credentials

If an application is already created and you need to find the application information to complete the Source Connection step, follow the steps below in the Azure Portal. For more information, see relevant Microsoft documentation on the Microsoft site.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Navigate to **Enterprise applications**.
4. In the list of applications, locate and click on your application.The application page displays.
5. Navigate to **Properties**.
6. Click the **copy icon** next to the **Application ID**. The ID is copied to your clipboard to use as needed.



15.7 Limiting application registration access to accounts

Limit the access of Collect to specific Microsoft user accounts and mailboxes by using *New-ServicePrincipal -AppId <Client Application ID in AAD> -ObjectId <Service principal object ID in AAD> -DisplayName <name>*. For more information, see Microsoft documentation.

15.8 Revoking application access

Revoke the application from the Azure portal or by using a PowerShell script. For more information, see Microsoft's documentation.

15.8.1 Revoking access via Azure Portal

To revoke access from the Azure portal:

1. Open your Azure Portal.
2. Navigate to **Enterprise Application**.
3. Under **All applications**, search for your application and click its link.
4. Under **Manage > Properties**, click **Delete**.

Collect no longer has access.

15.8.2 Revoking access via Powershell

Revoke access in Powershell using the Remove-MsolServicePrincipal script. See the Powershell example below of retrieving and deleting an application registration.

```
Get-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602

  ExtensionData : System.Runtime.Serialization.ExtensionDataObject
AccountEnabled : True
 Addresses : {}
AppPrincipalId : 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
 DisplayName : Relativity-Development-Application
ObjectId : 51798fb3-e72c-4373-8c63-6e7d0dd63ad7
ServicePrincipalNames : {19ab8a2e-ccce-4fa8-a9ee-eb16e220d602}
 TrustedForDelegation : False

Remove-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
```

15.9 Creating the data source in Collect

The Collection Admin tab is where you create, edit, and remove data sources from your workspace.

- You need to setup each data source once.
- You must create your data sources prior to setting up your custodian targets.

In Relativity aiR, navigate to **Collect**.

1. Click the **New Collection Source Instance** button.
2. Enter in a unique name for the data source.
3. Select a **Microsoft 365 Inactive Mailbox** data source.

   Note: Collect automatically collects any data that is preserved due to an in-place hold or litigation hold. Data on a hold is stored in a preservation library and separate folders. For more information, see Microsoft Retention Policies.
4. Enter the required information in Settings. For more information, see Settings fields on the next page
5. Click **Save**.

After clicking Save, Relativity verifies the parameters and connectivity to the Microsoft 365 data source.

- If successful, Relativity saves the data source.
- If the connection fails, a message appears indicating that the connection failed.
    - If verification fails, verify that the values are correct.
    - The data source will save when it is corrected and is verified.

Once the set up is complete, the data source information on the Collect Admin page.

15.10 Settings fields

To connect Relativity to a Microsoft Outlook data source, you need to gather and enter the information for the following fields:

- **Tenant ID**—enter the Tenant ID or Primary domain of the Microsoft 365 tenant the collection is intended for.
    - The domain name usually ends with .onmicrosoft.com.
    - To locate the tenant ID or primary domain name, see Microsoft documentation.
- **Application Id**—enter the Application ID created during registering the Collect application in Microsoft 365.
- **Application secret**—enter the Application secret created during registering the Collect application in Microsoft 365. For more information, see Accessing Microsoft 365 tenants on page 73.
- **Refresh token**—after entering in the three pieces of information, click **Generate Refresh Token**.
    - An authentication window appears.
    - In the authentication window, you must get a refresh token from a Microsoft account with the Microsoft eDiscovery Manager role assigned.

15.10.1 Data source details

Each data source details page includes an Action console. Each data source has different actions.

On the Microsoft Teams data source page, click **Validate Connection** in the Actions console to validate the client ID, certificate, and other credentials with Microsoft 365.

15.11 Configuring the data source in Collect

In Relativity aiR, configure the data sources chosen in the Collection Details step.

15.11.1 Data source criteria

Add criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.

    Note: You must add start and end dates when you are configuring the Outlook Calendar data source to complete the Data Sources step.

- **Operator**—choose an operator, such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

After selecting field options, you must click **Add Criteria**.

Details to know about criteria:

- Each criteria is then separated by an AND operator.
- Leave the data source criteria empty to collect all data from the sources.

15.11.2 Criteria

Filter a data source's data that you want to collect by adding criteria.

This section covers the different criteria for each data source. It also includes what can be searched within each data source.

15.11.2.1 Inactive mailbox criteria

The following table lists the filter criteria supported for mailbox collections.

Note: You must register Relativity in Microsoft 365 before using this data source. For information on registering Relativity in Microsoft 365, see Accessing Microsoft 365 tenants on page 73.

The following table lists the filter criteria supported for mailbox collections.

All dates are in Coordinated Universal Time (UTC).

Criteria	Operators	Description	Example
Email Received Date	Does Not Equal, Equals, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Email Received Date property in a query, the search returns all messages that equal or does not equal, greater or less than the date entered.	If you search “Less Than 1/1/2020,” your results include all emails received before January 1, 2020.
Email Sent Date	Does Not Equal, Equals, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Email Sent Date property in a query, the search returns all messages that equal or does not equal, greater or less than the date entered.	If you search “Greater Than 1/1/2001,” your results include all emails sent after January 1, 2001.

16 Microsoft 365 - Inactive OneDrive data source

The Microsoft 365 Inactive OneDrive data source enables Collect to retrieve OneDrive content belonging to custodian accounts that have been deactivated or removed. This provides a direct and defensible alternative to manual exports and re-ingestion workflows.

OneDrive data becomes inactive, or inaccessible, to users when a user account is deleted, even if a preservation hold exists. Microsoft does not permanently delete the OneDrive content while a retention policy or hold is in place.

After all retention policies or holds are removed, the OneDrive continues through its standard deletion lifecycle and is permanently deleted according to the configured retention period.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

This topic provides details on how to capture Microsoft 365 inactive OneDrive data with Collect.

16.1 Considerations

Note the following considerations about Microsoft 365 inactive OneDrive data sources:

- The inactive OneDrive connector uses Microsoft's Purview API.
- Purview Cases will be created in your Microsoft Purview instance to facilitate the search and export of inactive OneDrive.
- Relativity collects all available files including preserved files.
    - You do not need to take extra steps to collect preserved files as they are automatically included in the collection.
    - For more information on preserving data, see the Legal Hold guide.
- Delegated permissions are mandatory.
    - App-only authentication is not supported for inactive OneDrive collections.
    - Inactive OneDrive exports require an account with the *eDiscovery Manager* role and an Azure AD app registration that has the required delegated permissions.
- Microsoft APIs do not support verifying that an inactive OneDrive exists prior to collection. You will see failed collections in cases where the OneDrive no longer exists.
- Relativity collects inactive OneDrive data as .zip files.
- If the Azure Application Registration secret changes or expires, update all Microsoft data sources that use that registration. Go to *Collect Admin*, select each affected data source, click *Edit*, enter the new secret in the Application Secret field, and click *Save*.

16.2 Collection size

Microsoft 365 collections can be large. When collection jobs become too large, performance decreases.

Large collections	Best practices
200 GB per search	Reduce search size
Multi-TB exports	Limit the number of custodians per job. Collect max 30 custodians per job.
Long date ranges with many OneDrivees	Using smaller date ranges.

16.3 Inactive OneDrive data

Inactive OneDrive collections differ from active Microsoft 365 data sources:

- Content is exported from Microsoft Purview eDiscovery, not Microsoft Graph file APIs.
- A temporary Purview hold is applied to the OneDrive site during export to prevent deletion.
- OneDrive content is exported as ZIP packages, then downloaded and ingested into Relativity aiR.
- Temporary holds and export artifacts are removed after collection completes.

These behaviors are specific to OneDrive and do not mirror inactive mailbox collection behavior.

16.4 Task checklist

The table lists the order to perform the necessary tasks for setting up the data source for Collect.

Note: Separate Microsoft data sources inside Collect can use the same Microsoft Azure app registration. This means you only need to create one Microsoft Graph application and provide one Client ID and one Client Secret. You can then enter that same set of credentials for Microsoft data sources within Collect.

Order	Application	Task
1	Azure	Registering the Collect application below
2	Azure	Obtaining a client secret on the next page
3	Azure	Setting API permissions on page 83
4	Azure	Adding a redirect URI on page 83
5	Collect	Creating the data source in Collect on page 85
6	Collect	Configuring the data source in Collect on page 86

16.5 Accessing Microsoft 365 tenants

Register the Collect application to access Microsoft 365.

When registering the application, the Microsoft 365 administrator creates a Microsoft Application ID and secret. Relativity uses this ID and secret to configure data sources in Collect and provides access to the Microsoft 365 tenants.

You can register the application through Azure Portal or by registering the delegated permissions through the Microsoft App Registration Portal. After registering the application, request administrator consent. From there, it is possible to revoke application access.

Depending on your Relativity aiR license, commercial or government, and your Microsoft tenant, Microsoft 365 or Microsoft 365 Government, you will be able to collect from either Microsoft 365 or both Microsoft 365 and Microsoft 365 Government data sources. Commercial users can only collect from Microsoft 365 tenants. Government users can collect from Microsoft 365 and Government 365 tenants. These data sources act the same, but have different icons within Collect.

16.5.1 Registering the Collect application

Start with registering your application in the Azure portal by following the steps below.

Caution: The listed permissions and roles are required and supported by Relativity.

- Relativity does not support substitutions or reduced permissions.
- You can submit requests for alternative or reduced permissions as product feedback.

For more information on registering an application in the Azure portal, refer to documentation on Microsoft's site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Click **App registrations**.
4. Click **New Registration** to display the Register an application page.
5. Enter an application name in the **Name** field.
6. Accept the default setting, **Accounts in this organizational directory only**, as the supported account type.

7. Click **Register**.
8. Once the application is registered, make note of the **Application (client) ID** and **Directory (tenant) ID** for use later when configuring the data source in Relativity aiR Collect.

16.5.2 Obtaining a client secret

Next, obtain the client secret for the registered application in the Azure portal. For more information, see relevant Microsoft documentation on the Microsoft site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **Certificates & secrets** option in the left navigation bar.
2. Click the **Client secrets** tab.
3. Click **New client secret**.
4. Enter a description for the client secret in the **Description** text box.
5. Select **730 days (24 months)** from the Expires list. The client secret will expire after this time frame.
    - Once the client secret expires, you must create a new client secret in the Azure portal as described in these steps.
    - Then you must update your Microsoft 365 Collect data sources with it. For more information, see Expired Azure client secrets below.
    - For any additional assistance with client secrets, please contact the Azure Admin in your organization.
6. Click **Add** to create a new secret.

    Caution: Microsoft will only show the secret value this one time. There is no way to recover a secret.

7. Click the copy icon to copy the **Secret Value** to the clipboard.
    - Paste it to a safe location.
    - You will use the Secret Value later when creating the data source in Collect.
    - Confirm you copy the *Secret Value* and not the Secret ID.
8. Give your Relativity Admin the Application ID and the Client Secret for setup of Collect.
    - This application secret is also needed for setting up a Microsoft Entra ID integration point.
    - For more information, see the Integration Points guide.

16.5.2.1 Expired Azure client secrets

If your Azure client secret expires, follow these steps:

1. Get a new secret as outlined in the steps above.
2. Go to **Collect Admin** in Relativity aiR.
3. Select the desired data source that has expired, and click **Edit**.
4. Input the new client secret value in the **Application Secret** field.
5. Click **Save**.

You must repeat these steps for all Microsoft data sources that you have set up.

16.5.3 Setting API permissions

Each data source has its own set of permissions necessary to allow access to the tenants.

To add the correct permissions based on your selected Microsoft 365 data source, follow the steps below.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **Manage > API permissions** option in the left navigation bar.

   Note: The *User.Read* permission is automatically added by default.

2. Click **Add a permission**.
3. Click **Graph API**.
4. Select **Delegated Permissions**.
5. Select the **eDiscovery.ReadWrite.All** permission from the Permission list.
6. Click **Add permissions**.
7. Click **Grant Permission**.
   The window will show all permissions granted.
   - Make a note of the application ID that Microsoft assigned to the app registration.
   - This ID is also required for setup of data sources in Collect.
8. Click **Add a permission**.
9. Select **APIs my organization uses**.
10. Search for **MicrosoftPurviewEDiscovery**.
11. Select **Application Permissions**.
12. Select the **eDiscovery.Download.Read** permission from the Permission list.
13. Click **Add permissions**.
14. Click **Grant Permission**.
    The window will show all permissions granted.
    - Make a note of the application ID that Microsoft assigned to the app registration.
    - This ID is also required for setup of data sources in Collect.
15. Verify that all permissions have been granted.
16. Click **Add permissions**.
17. Click **Grant Permission**.
18. Click **Accept** to grant the permissions.

All API permissions have been granted and you can start creating the data source in Relativity aiR.

16.6 Adding a redirect URI

After setting up API permissions, you must add a Redirect URI to the Azure Application Registration. Add the Redirect URI with the following steps:

1. In the left-side menu console, click **Authentication**.

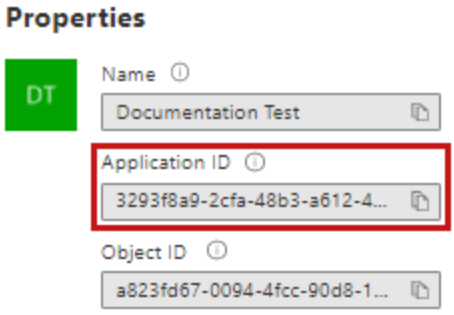
   Note: It may appear as **Authentication (Preview)**.

2. Click **Add Redirect URI**.
3. Click **Web**.
4. Enter your Redirect URI.
   - Your Redirect URI is your Relativity aiR tenant domain URL plus */collect-services/api/v1/Authentication/ms-auth-response*.
   - For example, *https://acme.corp.relativity.one/collect-services/api/v1/Authentication/ms-auth-response*

16.7 Finding Azure credentials

If an application is already created and you need to find the application information to complete the Source Connection step, follow the steps below in the Azure Portal. For more information, see relevant Microsoft documentation on the Microsoft site.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Navigate to **Enterprise applications**.
4. In the list of applications, locate and click on your application.The application page displays.
5. Navigate to **Properties**.
6. Click the **copy icon** next to the **Application ID**. The ID is copied to your clipboard to use as needed.



16.8 Limiting application registration access to accounts

Limit the access of Collect to specific Microsoft user accounts and mailboxes by using *New-ServicePrincipal -AppId <Client Application ID in AAD> -ObjectId <Service principal object ID in AAD> -DisplayName <name>*. For more information, see Microsoft documentation.

16.9 Revoking application access

Revoke the application from the Azure portal or by using a PowerShell script. For more information, see Microsoft's documentation.

16.9.1 Revoking access via Azure Portal

To revoke access from the Azure portal:

1. Open your Azure Portal.
2. Navigate to **Enterprise Application**.
3. Under **All applications**, search for your application and click its link.
4. Under **Manage > Properties**, click **Delete**.

Collect no longer has access.

16.9.2 Revoking access via Powershell

Revoke access in Powershell using the Remove-MsolServicePrincipal script. See the Powershell example below of retrieving and deleting an application registration.

```
Get-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602

  ExtensionData : System.Runtime.Serialization.ExtensionDataObject
AccountEnabled : True
 Addresses : {}
AppPrincipalId : 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
 DisplayName : Relativity-Development-Application
ObjectId : 51798fb3-e72c-4373-8c63-6e7d0dd63ad7
ServicePrincipalNames : {19ab8a2e-ccce-4fa8-a9ee-eb16e220d602}
 TrustedForDelegation : False

Remove-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
```

16.10 Creating the data source in Collect

The Collection Admin tab is where you create, edit, and remove data sources from your workspace. You need to setup each data source once. You must create your data sources prior to setting up your custodian targets.

In Relativity aiR, navigate to **Collect**.

1. Click the **New Collection Source Instance** button.
2. Enter in a unique name for the data source.
3. Select a **Microsoft 365 Inactive OneDrive** data source.

   Note: Collect automatically collects any data that is preserved due to an in-place hold or litigation hold. Data on a hold is stored in a preservation library and separate folders. For more information, see Microsoft Retention Policies.
4. Enter the required information in Settings. For more information, see Settings fields on the next page
5. Click **Save**.

After clicking Save, Relativity verifies the parameters and connectivity to the Microsoft 365 data source.

If successful, Relativity saves the data source. If the connection fails, a message appears indicating that the connection failed. If verification fails, verify that the values are correct. The data source will save when it is corrected and is verified.

Once the set up is complete, the data source information on the Collect Admin page.

16.11 Settings fields

To connect Relativity to the Inactive OneDrive data source, you need to gather and enter the information for the following fields:

- **Tenant ID**—enter the Tenant ID or Primary domain of the Microsoft 365 tenant the collection is intended for. The domain name usually ends with .onmicrosoft.com. To locate the tenant ID or primary domain name, see Microsoft documentation.
- **Application Id**—enter the Application ID created during registering the Collect application in Microsoft 365.
- **Application secret**—enter the Application secret created during registering the Collect application in Microsoft 365. For more information, see Accessing Microsoft 365 tenants on page 81.
- **Refresh token**—after entering in the three pieces of information, click **Generate Refresh Token**.
  - An authentication window appears.
  - In the authentication window, you must get a refresh token from a Microsoft account with the Microsoft eDiscovery Manager role assigned.
  - For long-running export jobs, the refresh token may be rotated. Monitor job logs and be prepared to re-authenticate if a token expiration error occurs.

16.11.1 Data source details

Each data source details page includes an Action console. Each data source has different actions.

On the Microsoft Inactive OneDrive data source page, click **Validate Connection** in the Actions console to validate the client ID, certificate, and other credentials with Microsoft 365.

16.12 Configuring the data source in Collect

In Relativity aiR, configure the data sources chosen in the Collection Details step.

16.12.1 Data source criteria

Add criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.
- **Operator**—choose an operator, such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

After selecting field options, you must click **Add Criteria**.

Details to know about criteria:

- Each criteria is then separated by an AND operator.
- Leave the data source criteria empty to collect all data from the sources.

16.12.2 Criteria

Filter a data source's data that you want to collect by adding criteria. It also includes what can be searched within each data source.

16.12.2.1 Inactive OneDrive criteria

The following table lists the filter criteria supported for inactive OneDrive collections.

Note: You must register Relativity in Microsoft 365 before using this data source. For information on registering Relativity in Microsoft 365, see Accessing Microsoft 365 tenants on page 81.

The following table lists the filter criteria support for Inactive OneDrive collections.

Note: You must register Relativity in Microsoft 365 before using this data source. For information on registering Relativity in Microsoft 365, see Microsoft 365 - Inactive OneDrive data source on page 79.

When using search criteria to filter for Microsoft 365 inactive OneDrive, different operators can return different results. Knowing the search operators is crucial.

The keyword search criteria uses the Search In operator. When using the Search In operator:

- Search for a phrase by entering the phrase without any OR operators into the Value text box.
  Example: acme corp contract
- Search for individual keywords by entering the keywords and separating them with an OR in the Value text box.
  Example: cat OR dog OR mouse

  Notes: Enter the OR operator with all capital letters. You should add keywords and phrases in lower case only.

- Keywords hit on matches and if a word is prefixed with a keyword.
  Example: "Work" will return "workday" and "workplace"

Note: Inactive OneDrive filtering is file-based. Email-specific criteria such as sender, recipient, or message headers are not applicable to this data source.

All dates are in Coordinated Universal Time (UTC).

Criteria	Operators	Description	Example
Creation Date	Equals, Does Not Equal, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Creation Date property in a query, the search returns all messages that equal/doesn't equal, greater/less than the date entered.	If you search "Greater Than 1/1/2001," your results include all messages created after January 1, 2001.
File Extension	Equal, Does Not Equal, Contains	When you use the File Extension property in a query, the search returns all files that contain the entered file extension.	If you search "Contains docx," your results include all Microsoft Word files saved with that extension.
File Name	Equal, Does Not Equal, Contains	When you use the File Name property in a query, the search returns all files that equals/does not equal or contain the value entered.	If you search "Equals Important_ Document," your results include all files with that text in the filename.
File Path	Equal, Does Not Equal, Contains	When you use the File Path property in a query, the search returns all messages equals/does not equal or contain the folder path entered.	If you search "Contains documents/Relativity," your results include all files within the listed folder and any folder beyond the file path entered.

Criteria	Operators	Description	Example
Keyword Search	Search In	When you use the Keyword Search property in a query, the search returns all files containing the searched text.	If you search “Relativity,” your results include all files that contain the searched text in the file.
Modification Date	Equals, Does Not Equal, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Modification Date property in a query, the search returns all updated files that equal/-doesn’t equal, greater/less than the date entered.	If you search “Less Than 1/1/2020,” your results include all files modified before January 1, 2020.

16.13 Troubleshooting

Common issues during inactive OneDrive collections include:

- Refresh token expiration during long-running exports.
- Partial success where some files export successfully and others fail.
- Cleanup issues, such as temporary holds not being removed.
- File-level errors rather than custodian-level failures.

Job results and logs should be reviewed to identify which files were successfully collected and which encountered errors.

17 Microsoft 365 - Mailboxes data source

This topic provides details on how to capture Microsoft 365 mailbox data with Collect.

The Mailboxes connector uses Microsoft's Purview API to collect standard mailboxes, archived online mailboxes, and inactive mailboxes for a custodian in a single collection job.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

17.1 Considerations

Consider the following about the Microsoft 365 Mailboxes data source:

17.1.1 API and connector

- This connector uses Microsoft's Purview API.
- By default, Collect retrieves all mailbox types that the Purview API supports for a custodian. This includes:
  - The primary mailbox
  - The archived online mailbox, if enabled
  - Any inactive mailboxes associated with the custodian.

- You do not need to configure each mailbox type separately. For more information on how the Purview API handles each mailbox type, see Data sources in eDiscovery and Learn about inactive mailboxes.

17.1.2 Purview case

- Relativity creates a case in Microsoft Purview, adds the custodian, runs the search, and exports the results to Collect.
- You can view this case at any time in the Microsoft Purview portal.
- Purview cases are created in your Microsoft Purview instance to support the search and export of mailbox data.

17.1.3 Preserved files

- Relativity collects all available data, including preserved files.
- You do not need to take extra steps to collect preserved files. They are automatically included in the collection.
- For more information on preserving data, see the Preservation in-place guide.

17.1.4 Requirements and limitations

- Export requires an account with the eDiscovery Manager role and an Azure AD app registration with the required delegated permissions.
- Microsoft APIs do not support verifying that an inactive mailbox exists before collection. You will see failed collections when a mailbox no longer exists.
- Relativity collects mailbox data as .pst files.
- If the password changes on the account used to generate the refresh token, all existing refresh tokens are invalidated. To continue collecting, go to Collect Admin, select the data source, click Edit, and generate a new refresh token.

17.2 Collection size

Microsoft 365 collections can be large. When collection jobs become too large, performance decreases.

Large collections	Best practices
200 GB per search	Reduce search size
Multi-TB exports	Limit the number of custodians per job. Collect supports a maximum of 30 custodians per job.
Long date ranges with many mailboxes	Use smaller date ranges.
Large mailboxes	Plan for 2 GB per hour per mailbox transfer throughput. For mailboxes larger than 25 GB, collection may take more than 24 hours.

17.2.1 Export duration for large mailboxes

Export duration is determined primarily by mailbox size and whether or not date range criteria are being used, as well as the current load on Microsoft's services. Purview eDiscovery runs on shared, multi-tenant Microsoft 365 infrastructure, and Microsoft does not provide a service-level agreement or guaranteed throughput for export operations.

Exports occur in two phases, and each contributes to the overall duration.

17.2.1.1 Phase 1: Export preparation in Microsoft

Microsoft packages the mailbox data before transferring any documents.

- While this phase is in progress, the document counter on the Collect monitoring page remains at zero, which is normal.
- The counter reflects documents received by Collect. Nothing is transferred until preparation finishes.
- For large mailboxes, this phase alone can take several hours or longer.

17.2.2 Phase 2: Data transfer

When preparation completes, documents begin transferring to Collect and the counter starts incrementing.

- Microsoft throttles transfer throughput. Throughput is typically around 2 GB per hour per mailbox.
- Completion of the preparation phase does not mean the collection is nearly finished.
- A 25 GB mailbox may require 12 or more hours of transfer time after preparation completes. A mailbox larger than 25 GB may take several hours to more than 24 hours to fully collect.

Do not cancel or restart a collection solely because progress appears slow. Doing so restarts the export preparation from the beginning.

If a large mailbox collection shows zero documents for more than 48 hours, contact Relativity Support.

17.3 Accessing Microsoft 365 tenants

Register the Collect application to access Microsoft 365.

When registering the application, the Microsoft 365 administrator creates a Microsoft Application ID and secret. Relativity uses this ID and secret to configure data sources in Collect and provides access to the Microsoft 365 tenants.

You can register the application through Azure Portal or by registering the delegated permissions through the Microsoft App Registration Portal. After registering the application, request administrator consent. From there, it is possible to revoke application access.

Depending on your Relativity aiR license, commercial or government, and your Microsoft tenant, Microsoft 365 or Microsoft 365 Government, you will be able to collect from either Microsoft 365 or both Microsoft 365 and Microsoft 365 Government data sources. Commercial users can only collect from Microsoft 365 tenants. Government users can collect from Microsoft 365 and Government 365 tenants. These data sources act the same, but have different icons within Collect.

17.3.1 Registering the Collect application

Start with registering your application in the Azure portal by following the steps below.

Caution: The listed permissions and roles are required and supported by Relativity.

- Relativity does not support substitutions or reduced permissions.
- You can submit requests for alternative or reduced permissions as product feedback.

For more information on registering an application in the Azure portal, refer to documentation on Microsoft's site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Click **App registrations**.
4. Click **New Registration** to display the Register an application page.
5. Enter an application name in the **Name** field.
6. Accept the default setting, **Accounts in this organizational directory only**, as the supported account type.
7. Click **Register**.
8. Once the application is registered, make note of the **Application (client) ID** and **Directory (tenant) ID** for use later when configuring the data source in Relativity aiR Collect.

17.3.2 Obtaining a client secret

Next, obtain the client secret for the registered application in the Azure portal. For more information, see relevant Microsoft documentation on the Microsoft site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **Certificates & secrets** option in the left navigation bar.
2. Click the **Client secrets** tab.
3. Click **New client secret**.
4. Enter a description for the client secret in the **Description** text box.
5. Select **730 days (24 months)** from the Expires list. The client secret will expire after this time frame.
    - Once the client secret expires, you must create a new client secret in the Azure portal as described in these steps.
    - Then you must update your Microsoft 365 Collect data sources with it. For more information, see Expired Azure client secrets below.
    - For any additional assistance with client secrets, please contact the Azure Admin in your organization.
6. Click **Add** to create a new secret.

    Caution: Microsoft will only show the secret value this one time. There is no way to recover a secret.

7. Click the copy icon to copy the **Secret Value** to the clipboard.
    - Paste it to a safe location.
    - You will use the Secret Value later when creating the data source in Collect.
    - Confirm you copy the *Secret Value* and not the Secret ID.
8. Give your Relativity Admin the Application ID and the Client Secret for setup of Collect.
    - This application secret is also needed for setting up a Microsoft Entra ID integration point.
    - For more information, see the Integration Points guide.

17.3.2.1 Expired Azure client secrets

If your Azure client secret expires, follow these steps:

1. Get a new secret as outlined in the steps above.
2. Go to **Collect Admin** in Relativity aiR.
3. Select the desired data source that has expired, and click **Edit**.
4. Input the new client secret value in the **Application Secret** field.
5. Click **Save**.

You must repeat these steps for all Microsoft data sources that you have set up.

17.3.3 Setting API permissions

Each data source has its own set of permissions necessary to allow access to the tenants. To add the correct permissions based on your selected Microsoft 365 data source, follow the steps below.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **Manage > API permissions** option in the left navigation bar.

   Note: The *User.Read* permission is automatically added by default.
2. Click **Add a permission**.
3. Click **Graph API**.
4. Select **Delegated Permissions**.
5. Select the **eDiscovery.ReadWrite.All** permission from the Permission list.
6. Click **Add permissions**.
7. Click **Grant Permission**.
   The window will show all permissions granted.
   - Make a note of the application ID that Microsoft assigned to the app registration.
   - This ID is also required for setup of data sources in Collect.
8. Click **Add a permission**.
9. Select **APIs my organization uses**.
10. Search for **MicrosoftPurviewEDiscovery**.
    - If *MicrosoftPurviewEDiscovery* does not appear in the APIs my organization uses list, you must first register the app in Microsoft Entra ID.
    - For more information, see Microsoft's Register the MicrosoftPurviewEDiscovery app in Microsoft Entra ID documentation.
11. Select **Application Permissions**.
12. Select the **eDiscovery.Download.Read** permission from the Permission list.
13. Click **Add permissions**.
14. Click **Grant Permission**.
    The window will show all permissions granted.
    - Make a note of the application ID that Microsoft assigned to the app registration.
    - This ID is also required for setup of data sources in Collect.

15. Verify that all permissions have been granted.
16. Click **Add permissions**.
17. Click **Grant Permission**.
18. Click **Accept** to grant the permissions.

All API permissions have been granted and you can start creating the data source in Relativity aiR.

17.4 Adding a redirect URI

After setting up API permissions, you must add a Redirect URI to the Azure Application Registration. Add the Redirect URI with the following steps:

1. In the left-side menu console, click **Authentication**.

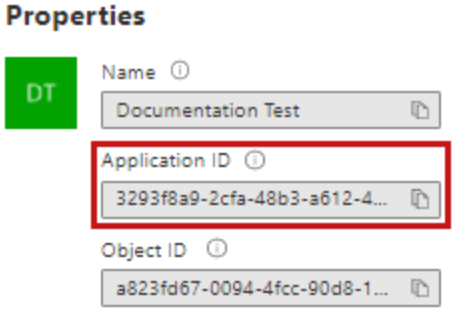
   Note: It may appear as **Authentication (Preview)**.

2. Click **Add Redirect URI**.
3. Click **Web**.
4. Enter your Redirect URI.
   - Your Redirect URI is your Relativity aiR tenant domain URL plus */collect-services/api/v1/Authentication/ms-auth-response*.
   - For example, *https://acme.corp.relativity.one/collect-services/api/v1/Authentication/ms-auth-response*

17.5 Finding Azure credentials

If an application is already created and you need to find the application information to complete the Source Connection step, follow the steps below in the Azure Portal. For more information, see relevant Microsoft documentation on the Microsoft site.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Navigate to **Enterprise applications**.
4. In the list of applications, locate and click on your application.The application page displays.
5. Navigate to **Properties**.
6. Click the **copy icon** next to the **Application ID**. The ID is copied to your clipboard to use as needed.



17.6 Limiting application registration access to accounts

Limit the access of Collect to specific Microsoft user accounts and mailboxes by using *New-ServicePrincipal -AppId <Client Application ID in AAD> -ObjectId <Service principal object ID in AAD> -DisplayName <name>*. For more information, see Microsoft documentation.

17.7 Revoking application access

Revoke the application from the Azure portal or by using a PowerShell script. For more information, see Microsoft's documentation.

17.7.1 Revoking access via Azure Portal

To revoke access from the Azure portal:

1. Open your Azure Portal.
2. Navigate to **Enterprise Application**.
3. Under **All applications**, search for your application and click its link.
4. Under **Manage > Properties**, click **Delete**.

Collect no longer has access.

17.7.2 Revoking access via Powershell

Revoke access in Powershell using the Remove-MsolServicePrincipal script. See the Powershell example below of retrieving and deleting an application registration.

Revoking access via Powershell

```
Get-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602


     ExtensionData         : System.Runtime.Serialization.ExtensionDataObject
       AccountEnabled        : True
    Addresses             : {}
       AppPrincipalId        : 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
      DisplayName           : Relativity-Development-Application
       ObjectId              : 51798fb3-e72c-4373-8c63-6e7d0dd63ad7
       ServicePrincipalNames : {19ab8a2e-ccce-4fa8-a9ee-eb16e220d602}
      TrustedForDelegation  : False


      Remove-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
```

17.8 Creating the data source in Collect

The Collection Admin tab is where you create, edit, and remove data sources from your workspace.

- You need to setup each data source once.
- You must create your data sources prior to setting up your custodian targets.

In Relativity aiR, navigate to **Collect**.

1. Click the **New Collection Source Instance** button.
2. Enter in a unique name for the data source.
3. Select a **Microsoft 365 Inactive Mailbox** data source.

   Note: Collect automatically collects any data that is preserved due to an in-place hold or litigation hold. Data on a hold is stored in a preservation library and separate folders. For more information, see Microsoft Retention Policies.
4. Enter the required information in Settings. For more information, see Settings fields below
5. Click **Save**.

After clicking Save, Relativity verifies the parameters and connectivity to the Microsoft 365 data source.

- If successful, Relativity saves the data source.
- If the connection fails, a message appears indicating that the connection failed.
  - If verification fails, verify that the values are correct.
  - The data source will save when it is corrected and is verified.

Once the set up is complete, the data source information on the Collect Admin page.

Settings fields

To connect Relativity to a Microsoft Outlook data source, you need to gather and enter the information for the following fields:

- **Tenant ID**—enter the Tenant ID or Primary domain of the Microsoft 365 tenant the collection is intended for.
  - The domain name usually ends with .onmicrosoft.com.
  - To locate the tenant ID or primary domain name, see Microsoft documentation.
- **Application Id**—enter the Application ID created during registering the Collect application in Microsoft 365.
- **Application secret**—enter the Application secret created during registering the Collect application in Microsoft 365. For more information, see Accessing Microsoft 365 tenants on page 90.
- **Refresh token**—after entering in the three pieces of information, click **Generate Refresh Token**.
  - An authentication window appears.
  - In the authentication window, you must get a refresh token from a Microsoft account with the Microsoft eDiscovery Manager role assigned.

17.8.1 Data source details

Each data source details page includes an Action console. Each data source has different actions.

On the Microsoft Teams data source page, click **Validate Connection** in the Actions console to validate the client ID, certificate, and other credentials with Microsoft 365.

17.9 Configuring the data source in Collect

In Relativity aiR, configure the data sources chosen in the Collection Details step.

17.9.1 Data source criteria

Add criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.

  Note: You must add start and end dates when you are configuring the Outlook Calendar data source to complete the Data Sources step.

- **Operator**—choose an operator, such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

After selecting field options, you must click **Add Criteria**.

Details to know about criteria:

- Each criteria is then separated by an AND operator.
- Leave the data source criteria empty to collect all data from the sources.

17.9.2 Criteria

Filter a data source's data that you want to collect by adding criteria.

This section covers the different criteria for each data source. It also includes what can be searched within each data source.

17.9.2.1 Inactive mailbox criteria

The following table lists the filter criteria supported for mailbox collections.

Note: You must register Relativity in Microsoft 365 before using this data source. For information on registering Relativity in Microsoft 365, see Accessing Microsoft 365 tenants on page 90.

The following table lists the filter criteria supported for mailbox collections.

All dates are in Coordinated Universal Time (UTC).

Criteria	Operators	Description	Example
Email Received Date	Does Not Equal, Equals, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Email Received Date property in a query, the search returns all messages that equal or does not equal, greater or less than the date entered.	If you search “Less Than 1/1/2020,” your results include all emails received before January 1, 2020.
Email Sent Date	Does Not Equal, Equals, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Email Sent Date property in a query, the search returns all messages that equal or does not equal, greater or less than the date entered.	If you search “Greater Than 1/1/2001,” your results include all emails sent after January 1, 2001.

18 Microsoft 365 - OneDrive data source

This topic provides details on how to capture Microsoft 365 OneDrive with Collect.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

18.1 Considerations

Consider the following when using the OneDrive data source:

- Relativity cannot collect shared, or public, OneDrive folders.
- It also cannot collect OneDrive data for inactive user accounts.
- Collect retrieves the latest version of the document, even when versioning is enabled in Microsoft.
- When a user is under a preservation hold, multiple numbered versions of edited files may exist in the preservation library. Collect retrieves all versions of files residing in the preservation library.
- If the Azure Application Registration secret changes or expires, update all Microsoft data sources that use that registration. Go to *Collect Admin*, select each affected data source, click *Edit*, enter the new secret in the Application Secret field, and click *Save*.

After taking everything under consideration, you can begin the task checklist.

18.2 Collection size

OneDrive collections depend heavily on the size and structure of personal drives. Large drives benefit from targeted scoping.

Category	Details
Hard limits (enforced)	30 targets per job
Planning thresholds (guidance)	2 GB/hour per account (avg) Large personal drives benefit from scoping
When to split	Large drives across many custodians
Notes	Throughput higher than Teams, lower than email

Focus on limiting scope for large drives. Splitting by custodian groups or folders helps maintain predictable performance.

18.3 Task checklist

The table lists the order to perform the necessary tasks for setting up the data source for Collect.

Note: Separate Microsoft data sources inside Collect can use the same Microsoft Azure app registration. This means you only need to create one Microsoft Graph application and provide one Client ID and one Client Secret. You can then enter that same set of credentials for Microsoft data sources within Collect.

Order	Application	Task
1	Azure	Registering the Collect application below
2	Azure	Obtaining a client secret on the next page
3	Azure	Setting API permissions on the next page
4	Collect	Creating the data source in Collect on page 103
5	Collect	Configuring the data source in Collect on page 103

18.4 Accessing Microsoft 365 tenants

Register the Collect application to access Microsoft 365.

When registering the application, the Microsoft 365 administrator creates a Microsoft Application ID and secret. You will use this ID and secret to configure data sources in Collect and provide access to the Office 365 tenants.

You can register the application through Azure Portal or by registering the application permissions through the Microsoft App Registration Portal. After registering the application, request administrator consent. From there, it is possible to revoke application access.

Depending on your Relativity aiR license, commercial or government, and your Microsoft tenant, Microsoft 365 or Microsoft 365 Government, you will be able to collect from either Microsoft 365 or both Microsoft 365 and Microsoft 365 Government data sources. Commercial users can only collect from Microsoft 365 tenants. Government users can collect from Microsoft 365 and Government 365 tenants. These data sources act the same, but have different icons within Collect.

18.4.1 Registering the Collect application

Register your application permissions through Azure Portal to access tenants.

Start with registering your application in the Azure portal by following the steps below.

Caution: The listed permissions and roles are required and supported by Relativity.

- Relativity does not support substitutions or reduced permissions.
- You can submit requests for alternative or reduced permissions as product feedback.

For more information on registering an application in the Azure portal, refer to documentation on Microsoft's site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Click **App registrations**.
4. Click **New Registration** to display the Register an application page.
5. Enter an application name in the **Name** field.
6. Accept the default setting, **Accounts in this organizational directory only**, as the supported account type.
7. Click **Register**.
8. Once the application is registered, make note of the **Application (client) ID** and **Directory (tenant) ID** for use later when configuring the data source in Relativity aiR Collect.

18.4.2 Obtaining a client secret

Next, obtain the client secret for the registered application in the Azure portal. For more information, see relevant Microsoft documentation on the Microsoft site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **Certificates & secrets** option in the left navigation bar.
2. Click the **Client secrets** tab.
3. Click **New client secret**.
4. Enter a description for the client secret in the **Description** text box.
5. Select **730 days (24 months)** from the Expires list. The client secret will expire after this time frame.
    - Once the client secret expires, you must create a new client secret in the Azure portal as described in these steps.
    - Then you must update your Microsoft 365 Collect data sources with it. For more information, see Expired Azure client secrets below.
    - For any additional assistance with client secrets, please contact the Azure Admin in your organization.
6. Click **Add** to create a new secret.

    Caution: Microsoft will only show the secret value this one time. There is no way to recover a secret.

7. Click the copy icon to copy the **Secret Value** to the clipboard.
    - Paste it to a safe location.
    - You will use the Secret Value later when creating the data source in Collect.
    - Confirm you copy the *Secret Value* and not the Secret ID.
8. Give your Relativity Admin the Application ID and the Client Secret for setup of Collect.
    - This application secret is also needed for setting up a Microsoft Entra ID integration point.
    - For more information, see the Integration Points guide.

18.4.2.1 Expired Azure client secrets

If your Azure client secret expires, follow these steps:

1. Get a new secret as outlined in the steps above.
2. Go to **Collect Admin** in Relativity aiR.
3. Select the desired data source that has expired, and click **Edit**.
4. Input the new client secret value in the **Application Secret** field.
5. Click **Save**.

You must repeat these steps for all Microsoft data sources that you have set up.

18.4.3 Setting API permissions

Each data source has its own set of permissions necessary to allow access to the tenants. To add the correct permissions based on your selected Microsoft 365 data source, follow the steps below.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **API permissions** option in the left navigation bar. The User-.Read permission is automatically added by default.
2. Click **Add a permission**.
3. Click **Microsoft Graph**.
4. Select **Application Permissions**.
5. Select the following permissions from the Permission list. Refer to *Azure Application Registration Permissions for Collect* below for more information about these permissions.
    - Files.Read.All
    - Sites.Read.All
    - User.Read.All
6. Click **Add permissions**.
7. Click **Grant Permission**.
8. Make a note of the application ID that Microsoft assigned to the app registration. This ID is also required for setup of data sources in Collect.
9. The window will show all permissions granted. Verify that all permissions have been granted.
10. Click **Accept** to grant the permissions.

18.4.3.1 Azure Application Registration Permissions for Collect

The Collect application in Relativity aiR is a tool designed to streamline the data collection process for eDiscovery. Its primary purpose is to gather data from various sources, such as cloud-based applications and other data repositories, in a manner that is secure, defensible, and efficient. Collect aims to reduce the time and effort involved in data collection, ensuring that the data is accurate and complete, while maintaining chain of custody and compliance with legal and regulatory requirements.

Due to the architecture of the Collect application, Delegated permission can't be used and are not supported. The Collect application requires the use of Microsoft Graph API Azure Application permissions to facilitate the collection of data that occurs in processes running in the background.

The Collect application requires specific Graph API Application permissions be granted to an Azure Application Registration to facilitate efficient and comprehensive data collection for e-discovery and compliance purposes.

Following is an explanation of each Azure application Graph API permission required and why it is needed to support collections of M365 data. For a PDF of this information, see Azure Application Registration Permissions for Collect.

Required Azure Application Graph API Permissions:

1. **Calendars.Read**—this permission allows Relativity to access calendar events. For e-discovery, it's important to capture calendar data as it can provide crucial context, timelines, and evidence related to the case or investigation.
2. **ChannelMember.Read.All**—this permission provides access to the membership information of all Teams channels. It allows Relativity to see who is part of each channel, which can be important for understanding who had access to certain communications and information during an investigation.
3. **ChannelMessage.Read.All**—this permission provides access to all messages in Microsoft Teams channels. It allows Relativity to capture and review conversations and discussions that take place in Teams channels, which may contain pertinent information for legal or compliance purposes.
4. **Chat.Read.All**—this permission enables Relativity to read all chat messages in Microsoft Teams. This includes private chats between users. Access to these messages is essential for gathering complete communication records and ensuring that no relevant information is overlooked in an investigation.

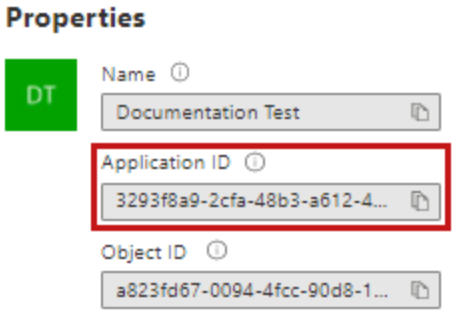
5. **Contacts.Read**—this permission allows access to contacts and is necessary to gather information about communications and relationships between individuals, which can be critical in understanding the full scope of interactions and connections in an investigation.
6. **eDiscovery.Download.Read**—this permission allows Relativity to download export packages and item reports from Microsoft Purview eDiscovery. These exports can contain documents, emails, Teams messages, and other collected data that are relevant to a legal matter or compliance review. This permission is required to retrieve exported data from Microsoft Purview for processing and review.
7. **eDiscovery.ReadWrite.All**—this permission allows Relativity to read and manage Microsoft Purview eDiscovery objects, including cases, custodians, holds, searches, review sets, and exports. It enables Relativity to create and manage e-discovery workflows programmatically, helping organizations automate the identification, preservation, collection, and review of potentially relevant information for legal and compliance matters.
8. **Files.Read.All**—this permission enables Relativity to access all files in OneDrive and SharePoint. It is essential for collecting documents, spreadsheets, presentations, and other files that might contain relevant information for a legal matter or compliance review. This permission is also required to support collection of linked OneDrive and SharePoint files in Outlook emails and Teams chats.
9. **Full_access_as_app Permission**—the Microsoft Graph API does not support accessing Outlook Online Archives (Archived Mailboxes). We utilize Microsoft's Exchange Web Services (EWS) API to collect Archived Mailboxes.
10. **Group.Read.All**—this permission allows Relativity to read all groups in the directory, including their properties and memberships. It helps in understanding the structure and membership of various groups within the organization, which can be important for context in e-discovery and compliance scenarios.
11. **Mail.Read**—this permission allows access to emails, which is one of the core components of e-discovery. This permission allows Relativity to read email messages in users' mailboxes to identify, preserve, and analyze communications that are pertinent to the case.
12. **Sites.Read.All**—this permission allows Relativity to access all SharePoint sites, including content and metadata. It ensures that any relevant information stored in SharePoint sites can be collected and reviewed.
13. **Team.ReadBasic.All**—this permission allows Relativity to read basic properties of all Teams. It helps in identifying and understanding the different Teams within the organization, their purposes, and their memberships, which can be relevant for investigations and compliance checks.
14. **TeamsTab.Read.All**—this permission allows Relativity to read the properties of all tabs in Microsoft Teams. Tabs can contain important resources, documents, and tools that users interact with. Access to this information can provide additional context and insights into the work and communications of users.
15. **User.Read.All**—this permission provides access to read the properties and membership of users. It is useful for identifying and understanding the roles, permissions, and activities of different users within the organization, which can be relevant for investigations and compliance checks.

18.5 Finding Azure credentials

If an application is already created and you need to find the application information to complete the Source Connection step, follow the steps below in the Azure Portal. For more information, see relevant Microsoft documentation on the Microsoft site.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Navigate to **Enterprise applications**.

4. In the list of applications, locate and click on your application.The application page displays.
5. Navigate to **Properties**.
6. Click the **copy icon** next to the **Application ID**. The ID is copied to your clipboard to use as needed.



18.6 Revoking application access

Revoke the application from the Azure portal or by using a PowerShell script. For more information, see Microsoft's documentation.

18.6.1 Revoking access via Azure Portal

To revoke access from the Azure portal:

1. Open your Azure Portal.
2. Navigate to **Enterprise Application**.
3. Under **All applications**, search for your application and click its link.
4. Under **Manage > Properties**, click **Delete**.

Collect no longer has access.

18.6.2 Revoking access via Powershell

Revoke access in Powershell using the Remove-MsolServicePrincipal script. See the Powershell example below of retrieving and deleting an application registration.

```
Get-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602

  ExtensionData : System.Runtime.Serialization.ExtensionDataObject
AccountEnabled : True
 Addresses : {}
AppPrincipalId : 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
 DisplayName : Relativity-Development-Application
ObjectId : 51798fb3-e72c-4373-8c63-6e7d0dd63ad7
ServicePrincipalNames : {19ab8a2e-ccce-4fa8-a9ee-eb16e220d602}
 TrustedForDelegation : False

Remove-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
```

18.7 Creating the data source in Collect

The Collection Admin tab is where you create, edit, and remove data sources from your workspace. Setup only needs to be done once for each data source. You must create your data sources prior to setting up your custodian targets.

In Relativity aiR, navigate to **Collect**.

1. Click the **New Collection Source Instance** button.
2. Enter a unique name for the data source.
3. Select **M365 - OneDrive** or **G365 - OneDrive**.

   Note: Collect automatically collects any preserved data that has an in-place hold or litigation hold. Microsoft stored data on a hold in a preservation library and separate folders. For more information, see Microsoft Retention Policies.
4. Enter the required information in Settings. For more information, see Settings fields below.
5. Click **Save**.

After clicking Save, Relativity verifies the parameters and connectivity to the Microsoft 365 data source. If successful, Relativity saves the data source. If the connection fails, a message appears indicating that the connection failed. If verification fails, verify that the values are correct. Relativity will save the data source when you correct it and it's verified.

Once the set up is complete, the data source information on the Collect Admin page.

18.8 Settings fields

To connect Relativity to a Microsoft OneDrive data source, you need to gather and enter the information for the following fields:

- **Domain**—enter the Tenant ID or Primary domain (domain name usually ends with .onmicrosoft.com) of the Microsoft 365 tenant the collection is intended for. To locate the tenant ID or primary domain name, see Microsoft documentation.
- **Application Id**—enter the Application ID created during registering the Collect application in Microsoft 365.
- **Application secret**—enter the Application Secret created during registering the Collect application in Microsoft 365.

Depending on your Relativity aiR license, commercial or government, and your Microsoft tenant, Microsoft 365 or Microsoft 365 Government, you will be able to collect from either Microsoft 365 or both Microsoft 365 and Microsoft 365 Government data sources. Commercial users can only collect from Microsoft 365 tenants. Government users can collect from Microsoft 365 and Government 365 tenants. These data sources act the same, but have different icons within Collect.

18.8.1 Data source details

Each data source details page includes an Action console. Each data source has different actions.

On the Microsoft Teams data source page, click **Validate Connection** in the Actions console to validate the client ID, certificate, and other credentials with Microsoft 365.

18.9 Configuring the data source in Collect

In Relativity aiR, configure the data sources chosen in the Collection Details step.

18.9.1 Data source criteria

Add criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.
- **Operator**—choose an operator such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

After selecting field options, you must click **Add Criteria**.

Details to know about criteria:

- Each criteria is then separated by an AND operator.
- Leave the data source criteria empty to collect all data from the sources.

18.9.1.1 Criteria

Filter a data source's data that you want to collect by adding criteria. This section covers the different criteria for each data source. It also includes what you can search within each data source. The criteria options change based on the Microsoft 365 Archived mailbox data source.

The following table lists the filter criteria support for OneDrive collections.

Note: You must register Relativity in Microsoft 365 before using this data source. For information on registering Relativity in Microsoft 365, see Accessing Microsoft 365 tenants on page 98.

When using search criteria to filter for Microsoft 365 OneDrive, different operators can return different results. Knowing the search operators is crucial.

The keyword search criteria uses the Search In operator. When using the Search In operator:

- Search for a phrase by entering the phrase without any OR operators into the Value text box.
  Example: acme corp contract
- Search for individual keywords by entering the keywords and separating them with an OR in the Value text box.
  Example: cat OR dog OR mouse

  Notes: Enter the OR operator with all capital letters. You should add keywords and phrases in lower case only.
- Keywords hit on matches and if a word is prefixed with a keyword.
  Example: "Work" will return "workday" and "workplace"

All dates are in Coordinated Universal Time (UTC).

Criteria	Operators	Description	Example
File Extension	Equal, Does Not Equal, Contains	When you use the File Extension property in a query, the search returns all files that contain the entered file extension.	If you search “Contains docx,” your results include all Microsoft Word files saved with that extension.
File Path	Equal, Does Not Equal, Contains	When you use the File Path property in a query, the search returns all messages equals/does not equal or contain the folder path entered.	If you search “Contains documents/Relativity,” your results include all files within the listed folder and any folder beyond the

Criteria	Operators	Description	Example
			file path entered.
File Name	Equal, Does Not Equal, Contains	When you use the File Name property in a query, the search returns all files that equals/does not equal or contain the value entered.	If you search “Equals Important_ Document,” your results include all files with that text in the filename.
Creation Date	Equals, Does Not Equal, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Creation Date property in a query, the search returns all messages that equal/doesn’t equal, greater/less than the date entered.	If you search “Greater Than 1/1/2001,” your results include all messages created after January 1, 2001.
Modification Date	Equals, Does Not Equal, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Modification Date property in a query, the search returns all updated files that equal/-doesn’t equal, greater/less than the date entered.	If you search “Less Than 1/1/2020,” your results include all files modified before January 1, 2020.
Keyword Search	Search In	When you use the Keyword Search property in a query, the search returns all files containing the searched text.	If you search “Relativity,” your results include all files that contain the searched text in the file.

18.9.2 Collecting preserved files

When running a collection with Microsoft OneDrive, Relativity collects all available files, including preserved files. You do not need to take extra steps to collect preserved files as they are automatically included in the collection.For more information on preserving data, see the Legal Hold guide.

When a user account is placed under a preservation hold, Microsoft creates a preservation library for OneDrive. The contents of the preservation library are automatically included in collections.

When files are on a preservation hold in Microsoft 365, Microsoft preserves original copies of any deleted or modified items. Microsoft stores preserved files in the Preservation Library. Collect automatically collects from these file locations.

Relativity collects all versions of the document available in the preservation library. Collecting all versions of a document means that Relativity collects multiple versions of the same file with the corresponding SHA-256 hashes for each version of the data. If there were changes in the file version, the hash should be unique. For more information on hash identifiers, see Hash identifier - SHA-256 on page 173.

19 Microsoft 365 - Outlook data source

Microsoft is deprecating the Exchange Web Services (EWS) API on October 1, 2026. The Microsoft 365 Outlook connector uses EWS to collect archived mailboxes and will no longer support archived mailbox collection after that date. After this date, you can use the *Microsoft 365 - Mailboxes* data source. The *M365 - Mailboxes* connector uses the Microsoft Purview API and supports primary, archived, and inactive mailboxes in a single collection job.
Fore more information, see Microsoft 365 - Mailboxes data source on page 88.

This topic provides details on how to capture Microsoft 365 Outlook mailbox, calendars, contacts, and archive mailboxes with Collect.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

19.1 Considerations

Note the following considerations about Microsoft 365 Outlook data sources:

19.1.1 Mailbox types and required permissions

Relativity supports collection from both standard and archived mailboxes. These mailbox types are treated as separate data sources and require specific configuration.

- Relativity can collect standard mailboxes and archived mailboxes, which are treated as two distinct data sources.
- Each mailbox type requires specific permissions to be configured in the Azure application registration.
- Standard Outlook mailboxes do not collect the contents of any shared mailboxes custodians have access to.
    - Shared mailboxes have to be collected separately using the email address of the shared mailbox.
    - This avoids collecting duplicate emails across relevant custodians that share a mailbox.
- Collecting online archived mailboxes requires modern authentication.
- For archived mailbox collection using modern authentication, the Azure app registration must include the Exchange Web Services *full_access_as_app* permission, along with the required Tenant ID, Client ID, and Client Secret.

19.1.2 Search and pre-collection filtering

Microsoft limits the filtering capabilities available before collection. As a result, search behavior may differ from other Microsoft and Relativity tools.

- Pre-collection filtering is limited by Microsoft.
- Search does not mimic search capabilities in either Microsoft Purview or Relativity dtSearch.
- Purview export results may not match the Collect job details if the filters or scope are different. When the settings don't match, the results will be different.
- Differences in supported operators and scope can cause confusion about what data is included in a collection.

19.1.3 Data source capabilities and limits

Different Microsoft data sources support different content types and scenarios.

- The Outlook data source supports collection of linked, or modern, attachments.
- The Outlook data source does not support collection of private, one-on-one Microsoft Teams chats.
- You must use the Teams data source to collect private one-on-one Teams chats
- If the Azure Application Registration secret changes or expires, update all Microsoft data sources that use that registration. Go to *Collect Admin*, select each affected data source, click *Edit*, enter the new secret in the Application Secret field, and click *Save*.
- For more information, see Microsoft 365 - Teams data source on page 134.

19.1.4 Government cloud and environment considerations

Government cloud environments require specific connector selection and may have additional network requirements.

- If you have a GCC High tenant, you must use the GCC High connector when setting up a data source. For more information, see Microsoft's GCC High endpoints documentation.
- If you are using GCC, non-High, you can use the standard Microsoft 365 commercial connector.
- Government 365 collections include archived mailboxes.
- If you are using the Government 365 version of a Microsoft connector where the tenant URL ends in *.us*, you must add Relativity aiR Collect outbound IP addresses to the SharePoint allow-list. For more information, see Control access based on network location.
- To obtain the current list of outbound IP addresses, contact the Cloud Services team by submitting a Product Support request through the Contact Support page.

19.1.5 Network access and IP restrictions

Network controls may impact Collect connectivity and should be configured carefully.

- Restricting Microsoft access based solely on IP addresses may prevent Collect from working as expected.
- Certain outbound IP addresses must be allowed by your IT or network team to enable required communication between your Relativity instance and Microsoft services.
- For current outbound IP allow-listing guidance, see the Relativity Community.

19.2 Collection size

Calendar data is typically smaller than email but can still grow significantly with long historical ranges across multiple custodians.

19.2.1 Mailbox

Use this guidance to plan Outlook email collections. Email collections scale quickly with both mailbox size and time range, so careful scoping is critical to avoid long-running jobs.

Category	Details
Hard limits (enforced)	30 targets per job
Planning thresholds (guidance)	Multi-year calendars across many custodians slow down
When to split	Multi-year ranges
Notes	Typically smaller than email but scales with history

Email is a fast-moving data sources but also is sensitive to scale. Split jobs early when combining large custodians and long time frames.

19.2.2 Calendar

Calendar data is typically smaller than email but can still grow significantly with long historical ranges across multiple custodians.

Category	Details
Hard limits (enforced)	30 targets per job
Planning thresholds (guidance)	Multi-year calendars across many custodians slow down
When to split	Multi-year ranges
Notes	Typically smaller than email but scales with history

Calendar collections are usually lightweight, but multi-year, multi-custodian jobs should still be segmented.

19.3 Task checklist

The table lists the order to perform the necessary tasks for setting up the data source for Collect.

Note: Separate Microsoft data sources inside Collect can use the same Microsoft Azure app registration. This means you only need to create one Microsoft Graph application and provide one Client ID and one Client Secret. You can then enter that same set of credentials for Microsoft data sources within Collect.

Order	Application	Task
1	Azure	Registering the Collect application below
2	Azure	Obtaining a client secret on the next page
3	Azure	Setting API permissions on page 110
4	Collect	Creating the data source in Collect on page 114
5	Collect	Configuring the data source in Collect on page 115

19.4 Accessing Microsoft 365 tenants

Register the Collect application to access Microsoft 365. When registering the application, the Microsoft 365 administrator creates a Microsoft Application ID and secret.

Relativity uses this ID and secret to configure data sources in Collect and provides access to the Microsoft 365 tenants. You can register the application through Azure Portal or by registering the application permissions through the Microsoft App Registration Portal. After registering the application, request administrator consent. From there, it is possible to revoke application access.

Depending on your Relativity aiR license, commercial or government, and your Microsoft tenant, Microsoft 365 or Microsoft 365 Government, you will be able to collect from either Microsoft 365 or both Microsoft 365 and Microsoft 365 Government data sources. Commercial users can only collect from Microsoft 365 tenants. Government users can collect from Microsoft 365 and Government 365 tenants. These data sources act the same, but have different icons within Collect.

19.4.1 Registering the Collect application

Start with registering your application in the Azure portal by following the steps below.

Caution: The listed permissions and roles are required and supported by Relativity.

- Relativity does not support substitutions or reduced permissions.
- You can submit requests for alternative or reduced permissions as product feedback.

For more information on registering an application in the Azure portal, refer to documentation on Microsoft's site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Click **App registrations**.
4. Click **New Registration** to display the Register an application page.
5. Enter an application name in the **Name** field.
6. Accept the default setting, **Accounts in this organizational directory only**, as the supported account type.
7. Click **Register**.
8. Once the application is registered, make note of the **Application (client) ID** and **Directory (tenant) ID** for use later when configuring the data source in Relativity aiR Collect.

19.4.2 Obtaining a client secret

Next, obtain the client secret for the registered application in the Azure portal. For more information, see relevant Microsoft documentation on the Microsoft site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **Certificates & secrets** option in the left navigation bar.
2. Click the **Client secrets** tab.
3. Click **New client secret**.
4. Enter a description for the client secret in the **Description** text box.
5. Select **730 days (24 months)** from the Expires list. The client secret will expire after this time frame.
    - Once the client secret expires, you must create a new client secret in the Azure portal as described in these steps.
    - Then you must update your Microsoft 365 Collect data sources with it. For more information, see Expired Azure client secrets below.
    - For any additional assistance with client secrets, please contact the Azure Admin in your organization.
6. Click **Add** to create a new secret.

    Caution: Microsoft will only show the secret value this one time. There is no way to recover a secret.

7. Click the copy icon to copy the **Secret Value** to the clipboard.
    - Paste it to a safe location.
    - You will use the Secret Value later when creating the data source in Collect.
    - Confirm you copy the *Secret Value* and not the Secret ID.
8. Give your Relativity Admin the Application ID and the Client Secret for setup of Collect.
    - This application secret is also needed for setting up a Microsoft Entra ID integration point.
    - For more information, see the Integration Points guide.

19.4.2.1 Expired Azure client secrets

If your Azure client secret expires, follow these steps:

1. Get a new secret as outlined in the steps above.
2. Go to **Collect Admin** in Relativity aiR.
3. Select the desired data source that has expired, and click **Edit**.
4. Input the new client secret value in the **Application Secret** field.
5. Click **Save**.

You must repeat these steps for all Microsoft data sources that you have set up.

19.4.3 Setting API permissions

Each data source has its own set of permissions necessary to allow access to the tenants. To add the correct permissions based on your selected Microsoft 365 data source, take the following steps:

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **Manage > API permissions** option in the left navigation bar. The User.Read permission is automatically added by default.
2. Click **Add a permission**.
3. Click **Microsoft Graph**.
4. Select **Application Permissions**.
5. Select the following permissions from the Permission list.
   Refer to *Azure Application Registration Permissions for Collect* below for more information about these permissions.
   - Calendars.Read
   - Contacts.Read
   - Files.Read.All
   - Mail.Read
   - Sites.Read.All
   - User.Read.All
6. Click **Add permissions**.
7. Click **Grant Permission**.
   The window will show all permissions granted.
   - Make a note of the application ID that Microsoft assigned to the app registration.
   - This ID is also required for setup of data sources in Collect.
8. Verify that all permissions have been granted.
9. Click **Accept** to grant the permissions.

To add permissions for Microsoft 365 online archived mailboxes:

1. Click **Add a permission**.
2. Click the **APIs my organization use**.
3. Select **Office 365 Exchange Online**.
4. Select **Application Permissions**.

5. Select the **full_access_as_app** permission from the Permission list.
6. Click **Add permissions**.
7. Click **Grant Permission**.
   The window will show all permissions granted.
8. Verify that all permissions have been granted.
9. Click **Accept** to grant the permissions.

All API permissions have been granted and you can start creating the data source in Relativity aiR.

19.4.3.1 Azure Application Registration Permissions for Collect

The Collect application in Relativity aiR is a tool designed to streamline the data collection process for eDiscovery. Its primary purpose is to gather data from various sources, such as cloud-based applications and other data repositories, in a manner that is secure, defensible, and efficient. Collect aims to reduce the time and effort involved in data collection, ensuring that the data is accurate and complete, while maintaining chain of custody and compliance with legal and regulatory requirements.

Due to the architecture of the Collect application, Delegated permission can't be used and are not supported. The Collect application requires the use of Microsoft Graph API Azure Application permissions to facilitate the collection of data that occurs in processes running in the background.

The Collect application requires specific Graph API Application permissions be granted to an Azure Application Registration to facilitate efficient and comprehensive data collection for e-discovery and compliance purposes.

Following is an explanation of each Azure application Graph API permission required and why it is needed to support collections of M365 data. For a PDF of this information, see Azure Application Registration Permissions for Collect.

Required Azure Application Graph API Permissions:

1. **Calendars.Read**—this permission allows Relativity to access calendar events. For e-discovery, it's important to capture calendar data as it can provide crucial context, timelines, and evidence related to the case or investigation.
2. **ChannelMember.Read.All**—this permission provides access to the membership information of all Teams channels. It allows Relativity to see who is part of each channel, which can be important for understanding who had access to certain communications and information during an investigation.
3. **ChannelMessage.Read.All**—this permission provides access to all messages in Microsoft Teams channels. It allows Relativity to capture and review conversations and discussions that take place in Teams channels, which may contain pertinent information for legal or compliance purposes.
4. **Chat.Read.All**—this permission enables Relativity to read all chat messages in Microsoft Teams. This includes private chats between users. Access to these messages is essential for gathering complete communication records and ensuring that no relevant information is overlooked in an investigation.
5. **Contacts.Read**—this permission allows access to contacts and is necessary to gather information about communications and relationships between individuals, which can be critical in understanding the full scope of interactions and connections in an investigation.
6. **eDiscovery.Download.Read**—this permission allows Relativity to download export packages and item reports from Microsoft Purview eDiscovery. These exports can contain documents, emails, Teams messages, and other collected data that are relevant to a legal matter or compliance review. This permission is required to retrieve exported data from Microsoft Purview for processing and review.
7. **eDiscovery.ReadWrite.All**—this permission allows Relativity to read and manage Microsoft Purview eDiscovery objects, including cases, custodians, holds, searches, review sets, and exports. It enables Relativity to create and manage e-discovery workflows programmatically, helping organizations automate the identification, preservation, collection, and review of potentially relevant information for legal and compliance matters.

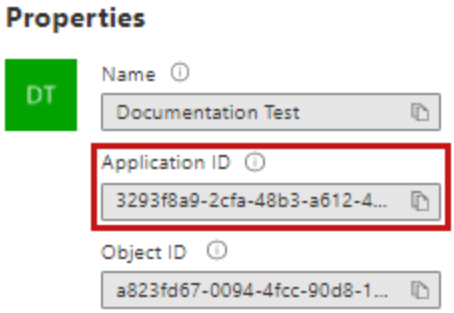
8. **Files.Read.All**—this permission enables Relativity to access all files in OneDrive and SharePoint. It is essential for collecting documents, spreadsheets, presentations, and other files that might contain relevant information for a legal matter or compliance review. This permission is also required to support collection of linked OneDrive and SharePoint files in Outlook emails and Teams chats.
9. **Full_access_as_app Permission**—the Microsoft Graph API does not support accessing Outlook Online Archives (Archived Mailboxes). We utilize Microsoft's Exchange Web Services (EWS) API to collect Archived Mailboxes.
10. **Group.Read.All**—this permission allows Relativity to read all groups in the directory, including their properties and memberships. It helps in understanding the structure and membership of various groups within the organization, which can be important for context in e-discovery and compliance scenarios.
11. **Mail.Read**—this permission allows access to emails, which is one of the core components of e-discovery. This permission allows Relativity to read email messages in users' mailboxes to identify, preserve, and analyze communications that are pertinent to the case.
12. **Sites.Read.All**—this permission allows Relativity to access all SharePoint sites, including content and metadata. It ensures that any relevant information stored in SharePoint sites can be collected and reviewed.
13. **Team.ReadBasic.All**—this permission allows Relativity to read basic properties of all Teams. It helps in identifying and understanding the different Teams within the organization, their purposes, and their memberships, which can be relevant for investigations and compliance checks.
14. **TeamsTab.Read.All**—this permission allows Relativity to read the properties of all tabs in Microsoft Teams. Tabs can contain important resources, documents, and tools that users interact with. Access to this information can provide additional context and insights into the work and communications of users.
15. **User.Read.All**—this permission provides access to read the properties and membership of users. It is useful for identifying and understanding the roles, permissions, and activities of different users within the organization, which can be relevant for investigations and compliance checks.

19.5 Finding Azure credentials

If an application is already created and you need to find the application information to complete the Source Connection step, follow the steps below in the Azure Portal. For more information, see relevant Microsoft documentation on the Microsoft site.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Navigate to **Enterprise applications**.
4. In the list of applications, locate and click on your application.The application page displays.
5. Navigate to **Properties**.

6. Click the **copy icon** next to the **Application ID**. The ID is copied to your clipboard to use as needed.



19.6 Limiting application registration access to accounts

Limit the access of Collect to specific Microsoft user accounts and mailboxes by using *New-ServicePrincipal -AppId <Client Application ID in AAD> -ObjectId <Service principal object ID in AAD> -DisplayName <name>*. For more information, see Microsoft documentation.

19.7 Revoking application access

Revoke the application from the Azure portal or by using a PowerShell script. For more information, see Microsoft's documentation.

19.7.1 Revoking access via Azure Portal

To revoke access from the Azure portal:

1. Open your Azure Portal.
2. Navigate to **Enterprise Application**.
3. Under **All applications**, search for your application and click its link.
4. Under **Manage > Properties**, click **Delete**.

Collect no longer has access.

19.7.2 Revoking access via Powershell

Revoke access in Powershell using the Remove-MsolServicePrincipal script. See the Powershell example below of retrieving and deleting an application registration.

```
Get-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602

  ExtensionData : System.Runtime.Serialization.ExtensionDataObject
AccountEnabled : True
 Addresses : {}
AppPrincipalId : 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
 DisplayName : Relativity-Development-Application
ObjectId : 51798fb3-e72c-4373-8c63-6e7d0dd63ad7
ServicePrincipalNames : {19ab8a2e-ccce-4fa8-a9ee-eb16e220d602}
 TrustedForDelegation : False

Remove-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
```

19.8 Creating the data source in Collect

The Collection Admin tab is where you create, edit, and remove data sources from your workspace. You need to setup each data source once. You must create your data sources prior to setting up your custodian targets.

In Relativity aiR, navigate to **Collect**.

1. Click the **New Collection Source Instance** button.
2. Enter in a unique name for the data source.
3. Select a **Microsoft 365 Outlook** data source.

   Note: Collect automatically collects any data that is preserved due to an in-place hold or litigation hold. Data on a hold is stored in a preservation library and separate folders. For more information, see Microsoft Retention Policies.
4. Enter the required information in Settings. For more information, see Settings fields below
5. Click **Save**.

After clicking Save, Relativity verifies the parameters and connectivity to the Microsoft 365 data source.

- If successful, Relativity saves the data source.
- If the connection fails, a message appears indicating that the connection failed.
  - If verification fails, verify that the values are correct.
  - The data source will save when it is corrected and is verified.

Once the set up is complete, the data source information on the Collect Admin page.

19.9 Settings fields

To connect Relativity to a Microsoft Outlook data source, you need to gather and enter the information for the following fields:

- **Domain**—enter the Tenant ID or Primary domain, domain name usually ends with .onmicrosoft.com, of the Microsoft 365 tenant the collection is intended for. To locate the tenant ID or primary domain name, see Microsoft documentation.
- **Application Id**—enter the Application ID created during registering the Collect application in Microsoft 365.
- **Application secret**—enter the Application secret created during registering the Collect application in Microsoft 365. For more information, see Accessing Microsoft 365 tenants on page 108.

Depending on your Relativity aiR license, commercial or government, and your Microsoft tenant, Microsoft 365 or Microsoft 365 Government, you will be able to collect from either Microsoft 365 or both Microsoft 365 and Microsoft 365 Government data sources. Commercial users can only collect from Microsoft 365 tenants. Government users can collect from Microsoft 365 and Government 365 tenants. These data sources act the same, but have different icons within Collect.

19.9.1 Data source details

Each data source details page includes an Action console. Each data source has different actions.

On the Microsoft Teams data source page, click **Validate Connection** in the Actions console to validate the client ID, certificate, and other credentials with Microsoft 365.

19.10 Configuring the data source in Collect

In Relativity aiR, configure the data sources chosen in the Collection Details step.

19.10.1 Data source criteria

Add criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.

  Note: You must add start and end dates when you are configuring the Outlook Calendar data source to complete the Data Sources step.

- **Operator**—choose an operator, such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

After selecting field options, you must click **Add Criteria**.

Details to know about criteria:

- Each criteria is then separated by an AND operator.
- Leave the data source criteria empty to collect all data from the sources.

19.10.2 Criteria

Filter a data source's data that you want to collect by adding criteria. This section covers the different criteria for each data source. It also includes what can be searched within each data source. The criteria options change based on the Microsoft 365 Outlook data source.

19.10.2.1 Microsoft 365 Outlook mailbox

Relativity collects all items in visible folders within Outlook's inbox and custom folders. Relativity collects hidden folders that exist under the Top of Information Store.

Note: The Microsoft 365 Outlook mailbox data source does not include soft deleted mailboxes, archived mailboxes, conversation history, notes, or tasks in the collections. To collect archived Outlook mailbox data, see Microsoft 365 archive mailboxes on page 119.

Another difference is the separation of calendar items and outlook contacts. Microsoft combines those two items with the Outlook mailbox. Relativity separates them into different data sources. For more information, see Microsoft 365 Outlook contacts on page 118 and Microsoft 365 Outlook calendar on page 118.

The following list is a list of file classes included in Outlook mailbox collections.

Collected file classes

- IPM.Activity
- IPM.Document
- IPM.OLE.Class
- IPM
- IPM.Post
- IPM.StickyNote
- IPM.Recall.Report

- IPM.Remote
- IPM.Report
- IPM.Resend
- IPM.Schedule
- IPM.TaskRequest

All dates are in Coordinated Universal Time (UTC).

Collect all emails with attachments regardless of criteria

This data source also includes the *Collect all emails with attachments regardless of criteria* toggle. If you are using keyword search criteria, we recommend enabling the toggle, regardless of keyword search results, because searching email attachments is not supported through the Microsoft Graph API.

Use the *Collect all emails with attachments regardless of criteria* to collect all emails with attachments, including ones that do not match the selected keyword search criteria.

- **Enabled**—toggle on to collect emails that match the keyword search criteria, emails that match other criteria such as date range, and all emails with attachments regardless of keyword search criteria.
  For example, if you add a date range and keywords, Collect pulls the following:
  - Emails with keywords in the body.
  - Emails within the specified date range.
  - Emails with attachments within the date range.
- **Disabled**—toggle off to collect only emails that match the search criteria.

Other filter criteria still applies to the collection. For example, if you specify a date range along with keywords, Collect does not return any emails outside the date range. It returns the emails within the date range that are either responsive to the keywords or have an attachment.

Outlook mailbox criteria

The following table lists the filter criteria supported for mailbox collections.

Note: You must register Relativity in Microsoft 365 before using this data source. For information on registering Relativity in Microsoft 365, see Accessing Microsoft 365 tenants on page 108.

When using search criteria to filter for Outlook Mailbox, different operators can return different results. For example, the search criteria uses Search In and it does not use Contains. When using the Search In operator:

- Search for a phrase by entering the phrase without any OR operators into the Value text box.
  Example: acme corp contract
- Search for individual keywords by entering the keywords and separating them with an OR in the Value text box.
  Example: cat OR dog OR mouse>

  Notes: Enter the OR operator with all capital letters. You should add keywords and phrases lower case only.
- Keywords hit on matches and if a word is prefixed with a keyword.
  Example: "Work" will return "workday" and "workplace"

The following table lists the filter criteria supported for mailbox collections.

Criteria	Operators	Description	Example
Email BCC	Contains	When you use the Email From prop-	If you search “@example.com,” your results

Criteria	Operators	Description	Example
		erty in a query, the search returns all messages that contain the text in the Email BCC field.	include all blind carbon copied messages received by people with the @example.com in their email address.
Email CC	Contains	When you use the Email From property in a query, the search returns all messages that contain the text in the Email CC field.	If you search "@example.com," your results include all carbon copied messages received by people with the @example.com in their email address.
Email From	Equals, Contains	When you use the Email From property in a query, the search returns all messages that contain the text in the Email From field.	If you search "@example.com," your results include all messages sent by people with the @example.com in their email address.
Email Received Date	Does Not Equal, Equals, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Email Received Date property in a query, the search returns all messages that equal/-doesn't equal, greater/less than the date entered.	If you search "Less Than 1/1/2020," your results include all emails received before January 1, 2020.
Email Sent Date	Does Not Equal, Equals, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Email Sent Date property in a query, the search returns all messages that equal/doesn't equal, greater/less than the date entered.	If you search "Greater Than 1/1/2001," your results include all emails sent after January 1, 2001.
Email To	Contains	When you use the Email To property in a query, the search returns all messages that contain the text in the Email To field.	If you search "@example.com," your results include all messages sent to people with the @example.com in their email address.
Has Attachments	Does Not Equal, Equals	When you use the Has Attachments property, the search returns emails with or without attachments based on the True or False setting.	If you mark "True," your results include all messages that include an attachment.
Keyword Search - Email Body	Search In	When you use the Keyword Search – Email Body property in a query, the search returns all messages email message contains the text you're searching for.	If you search "Dear John," your results include all messages that contain the text in email body. Note that this is not the same as searching for "Dear" OR "John." In order to do that, you need to separate keyword by OR
Keyword Search -	Search In	When you use the Keyword Search	If you search kritter@example.com, your results include all messages that have the text in

Criteria	Operators	Description	Example
Email Metadata		– Email Metadata property in a query, the search returns all messages which the Email To, Email From, Email CC, or Email BCC fields contain the text you're searching for.	the Email To, Email From, Email CC, or Email BCC fields.
Parent Folder Name	Contains, Does Not Equal, Equals	When you use the Parent Folder Path property in a query, the search returns all messages in the folder that equal, does not equal, or contains the name entered. When using the Parent Folder Name criteria, listing a parent folder includes the child folders in the returned results.	If you search "RelativityOne," your results include all emails in the folder and all emails within the child folders listed under the "RelativityOne" parent folder.
Subject	Contains	When you use the Subject property, the search returns all messages that contains the search word or phrase in the email's title.	If you use the Subject property in a query, the search returns all messages that the subject line contains the text you're searching for. In other words, the query does not return only those messages that have an exact match. For example, if you search for subject "Quarterly Financials," your results include messages with the subject "Quarterly Financials 2018."

19.10.2.2 Microsoft 365 Outlook calendar

The following table lists the filter criteria supported for calendar collections. You're required to enter the start date and end data criteria for calendar collections. The maximum supported date range is five years. For example, it can be 1/1/2001 to 12/31/2006 but not 1/1/2000 to 12/31/2007.

Note: You must register Relativity in Microsoft 365 before using this data source. For information on registering Relativity in Microsoft 365, see Accessing Microsoft 365 tenants on page 108.

You're required to enter the start and end dates when using an Microsoft 365 Outlook Calendar data source.

The following table lists the filter criteria supported for Outlook calendar collections.

Criteria	Operators	Description	Example
Start Date	Equals	When you use the Start Date property in a query, the search returns calendar items that exist the day of and after the entered date.	When you search a Start Date of 1/1/2001 and an End Date of 1/1/2020, Collect returns all calendar items on and between the two dates.
End Date	Equals	When you use the End Date property in a query, the search returns all calendar items the day of and before the entered date.	When you search a Start Date of 1/1/2001 and an End Date of 1/1/2020, Collect returns all calendar items on and between the two dates.

19.10.2.3 Microsoft 365 Outlook contacts

These properties are available for users to configure contacts, also called personal contacts, located in the personal address book of a user's mailbox. Relativity collects all contacts and no filter criteria is necessary.

Microsoft collects cached contacts, which are not contacts the user implicitly creates in Outlook. These contacts are not collected by Relativity.

Note: You must register Relativity in Microsoft 365 before using this data source. For information on registering Relativity in Microsoft 365, see Accessing Microsoft 365 tenants on page 108.

19.10.2.4 Microsoft 365 archive mailboxes

The following table lists the filter criteria supported for archive mailbox collections. Setting criteria for Microsoft 365 Email Archives is not required.

The Less Than operator is only supported when used in conjunction with Greater Than or Equals.

The following table lists the filter criteria supported for Outlook archived mailbox collections.

Criteria	Operators	Description	Example
Email Sent Date	Equals, Greater Than, Less Than	When you use the Email Sent Date property in a query, the search returns all messages that are greater than or equal/-less than the date entered. Less then operator is only supported together with the greater than or equals.	If you search "Greater Than 1/1/2001," your results include all emails sent after January 1, 2001.

19.11 Collecting preserved files

When running a collection with Microsoft Outlook, Relativity collects all available files including preserved files. You do not need to take extra steps to collect preserved files as they are automatically included in the collection. .For more information on preserving data, see the Legal Hold guide.

When Microsoft places a data source on a preservation hold, Microsoft creates a *Recoverable Items* folder for Outlook. The contents of the Recoverable Items folder are automatically included in collections.

When emails and files are on a preservation hold in Microsoft 365, Microsoft preserves original copies of any deleted or modified items. Find preserved emails in the Recoverable Items folder. Collect automatically collects from these file locations.

Relativity collects all versions of the document available in the preservation library. Collecting all versions of a document means that Relativity collects multiple versions of the same file with the corresponding SHA-256 hashes for each version of the data. If there were changes in the file version, the hash should be unique. For more information on hash identifiers, see Hash identifier - SHA-256 on page 173

19.12 Viewing collected data

When Relativity collects the data, Relativity accepts the path names and file names that the source provides. On occasion, the collection source modifies the path name or file name.

19.12.1 File names for Outlook email

Relativity collects Microsoft 365 Outlook emails as individual .eml files. Collect maintains the original folder structure of the mailbox on disk. Each .eml resides in its respective mailbox folder.

19.12.2 Files names on a preservation hold

A randomly generated and unique ID is appended to the original file name of the document if someone moves a deleted document to the Preservation Hold library, . For example, there is a document with the file name of *FY2017Budget.xlsx*. If someone deletes that document and then moves it to the Preservation Hold library, the file name of the document is modified. For example, the file name becomes something like *FY2017Budget_DEAF727D-0478-4A7F-87DE-5487F033C81A2000-07-05T10-37-55.xlsx*.

When a document on a site that is on hold is modified and versioning for the document library in the site has been enabled, a copy of the file is automatically created in the Preservation Hold library. In this case, a randomly generated and unique ID is also appended to the file name of the document that is copied to the Preservation Hold library.

The reason why file names of moved or copied documents to the Preservation Hold library is to prevent conflicting file names. For more information about placing a hold on sites and the Preservation Hold library, see Overview of in-place hold in SharePoint Server 2016.

19.12.3 Email considerations

Emails containing double byte characters and illegal characters will be HTML encoded to allow writing to the file system.

19.13 Troubleshooting

This table includes troubleshooting for Microsoft's archived mailboxes.

Error	Cause	Resolution
The remote server returned an error: (403).	Permissions have not been applied properly to the service account or application registration when using basic authentication or OAuth 2.0 respectively.	Apply the permission defined in the requirements section depending on your authentication method.
The specified folder could not be found in the store.	The mailbox does not have an archive.	Remove the mailbox from the list of targets.
Mailbox '...' doesn't have a valid license.	The owner of the mailbox does not have a valid license applied to their account.	Review the requirements section of this document and check if this user has a valid license. You can then choose to remove this user from the list of targets or apply a valid license.
The mailbox database is temporarily unavailable.	This error occurs if the mailbox database is not reachable. This can happen because the database is corrupt, in the process of being migrated, updated, or is offline for any other reason.	Wait an hour and retry the job to resolve this issue. If the issue persists, open a ticket with Microsoft.
The ExchangePrincipal object contains outdated information. The mailbox may have been moved recently.	The mailbox databases are separated in a way that causes inconsistent mailbox connections.	Retry the collection at a later time.
The request failed. Unable to connect to the remote server. A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond to microsoft_ip:443.	This is generally caused by a networking configuration either blocking access to the Exchange Online IP addresses—https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide or Exchange Online blocking access to itself via an allow list.	Perform the necessary network, firewall, or allowed IP address configuration to allow the connector to access Exchange Online.

20 Role-based access control

Use role-based access control (RBAC) in Microsoft 365 Exchange Online to restrict your Azure Application Registration to access only specific mailboxes. This is important for workflows where your application needs mail access, and still want to limit that access to a defined set of custodians rather than all users in your organization.

20.1 Azure application permissions

Azure application permissions are always-on by default.

When an application token is generated, it carries all permissions assigned to the app, regardless of any user-level RBAC assignments. This means you must carefully manage which permissions are assigned directly to the application versus which are scoped with RBAC.

The approach in this guide deliberately splits permissions between these two methods to achieve mailbox-level restriction.

20.2 Prerequisites

Before you begin, ensure you have the following in place:

- An Azure Application Registration already created for your application.
- The *Application (Client) ID* and the *Service Principal Object ID* for your app.
    - Make sure you are copying the Object ID from the Service Principal entry when looking up your app in Azure.
        - Do not copy from the Application Registration entry.
        - These are different objects in Azure AD and have different Object IDs.
    - Using the wrong one will cause the PowerShell commands to fail silently or produce unexpected results.
- Exchange Online PowerShell module installed and connected with appropriate admin privileges.
- The email addresses of the custodian mailboxes you want to grant access to.

20.3 Permission architecture

RBAC in Exchange Online has fewer granular permission options than Azure AD directly. As a result, some permissions must be assigned directly to the application, while the sensitive mail-access permissions are controlled through RBAC scoping.

Exchange Online has fewer permission options than Azure AD. Because of this, some permissions must be given directly to the app, while sensitive email access is controlled using RBAC limits.

20.4 Permissions assigned directly to the Azure App

Assign only the following permissions directly to your Azure Application Registration. These are needed for general user/file access and cannot be scoped with RBAC:

Permission Name	Purpose
Files.Read.All	Read files across SharePoint and OneDrive
Sites.Read.All	Read SharePoint site content
User.Read.All	Read user profile information across the tenant

20.4.1 Permissions assigned with RBAC (Mailbox-Scoped)

The following permissions should not be assigned directly to the app. Instead, they will be granted to specific mailboxes only through the RBAC steps in this guide:

For standard Outlook mailboxes:

Permission Name	Purpose
Application Mail.Read	Read mail from scoped mailboxes only
Application Calendars.Read	Read calendar events from scoped mailboxes only
Application Contacts.Read	Read contacts from scoped mailboxes only

For archived mailboxes:

Permission Name	Purpose
Application EWS.AccessAsApp	Access archived mailbox data through Exchange Web Services

20.5 Configuration steps

The following five steps must be performed in order using Exchange Online PowerShell. Replace the example values, such as App IDs, email addresses, names, with your own.

To complete RBAC configurations, you must complete the following steps:

1. Connect to Exchange Online PowerShell below.
2. Create a Service Principal in Exchange Online on the next page.
3. Create a Management scope for custodians on page 124.
4. Assign permissions to custodians on page 124.
5. Verify the configuration on page 125.

20.5.1 Connect to Exchange Online PowerShell

Run all Exchange commands inside PowerShell. On macOS/Linux, you must start PowerShell (pwsh) first; running these commands in zsh/bash will fail.

macOS / Linux:

1. Start PowerShell:

```
pwsh
```

2. Import the module:

```
Import-Module ExchangeOnlineManagement
```

3. Connect using device authentication (recommended):

```
Connect-ExchangeOnline -Device
```

4. Complete sign-in at https://login.microsoft.com/device and then verify:

```
Get-OrganizationConfig
```

Windows

1. PowerShell and import the module (if needed):

```
Import-Module ExchangeOnlineManagement
```

2. Connect:

```
Connect-ExchangeOnline
```

20.5.2 Create a Service Principal in Exchange Online

Register your Azure application as a Service Principal within Exchange Online. This links your Azure app to Exchange so that RBAC assignments can be applied to it.

```
New-ServicePrincipal \

  -AppId <Your-Application-Client-ID> \

  -ObjectId <Your-Service-Principal-Object-ID> \

  -DisplayName <FriendlyNameForYourApp>
```

Example:

```
      New-ServicePrincipal
       -AppId 2609b7e1-3b41-4e57-aa12-03bccbed8534 \
       -ObjectId 57b270fd-8b3f-47c3-9a12-29083613dff1 \
       -DisplayName FilteredMailboxApp
```

Verify (recommended):

```
Get-ServicePrincipal | Where-Object AppId -eq "APP_ID"
```

If New-ServicePrincipal indicates the AppId/ObjectId is already used, the Exchange service principal already exists and you can proceed.

20.5.2.1 Find the AppID and Object ID values

Find these values in the Azure Portal:

1. Navigate to Azure Active Directory > Enterprise Applications > [your app].
2. The Object ID shown here is the Service Principal Object ID.
3. The Application (Client) ID is found under Azure Active Directory > App Registrations > [your app] > Overview.

20.5.3 Create a Management scope for custodians

A Management Scope defines which mailbox a permission applies to. You must create one scope per custodian (user). The scope Name you set here will be used as the CustomResourceScope in Step 4.

```
New-ManagementScope \
  -Name "<ScopeName>" \
  -RecipientRestrictionFilter "PrimarySmtpAddress -eq '<user@yourdomain.com>'"
```

Example. Repeat for each custodian:

```
New-ManagementScope -Name "Jane" -RecipientRestrictionFilter "PrimarySmtpAddress -eq
'jane.doe@contoso.com'"
       New-ManagementScope -Name "John" -RecipientRestrictionFilter "PrimarySmt-
pAddress -eq 'john.smith@contoso.com'"
```

20.5.4 Assign permissions to custodians

Now assign each required permission to each custodian by creating a Management Role Assignment.

Each permission requires a separate assignment entry, but all assignments for the same user should share the same CustomResourceScope name. The scope name from Create a Management scope for custodians above.

For archived mailbox access. One entry per custodian:

```
New-ManagementRoleAssignment \
       -Name "<UniqueAssignmentName>" \
        -Role "Application EWS.AccessAsApp" \
        -App <Your-Service-Principal-Object-ID> \
        -CustomResourceScope "<ScopeName>"
```

For standard Outlook mailbox access. Three entries per custodian, one per permission:

```
New-ManagementRoleAssignment -Name "<Name>_Mail" -Role "Application Mail.Read" -App
<ObjectId> -CustomResourceScope "<ScopeName>"
        New-ManagementRoleAssignment -Name "<Name>_Cal" -Role "Application Cal-
endars.Read" -App <ObjectId> -CustomResourceScope "<ScopeName>"
        New-ManagementRoleAssignment -Name "<Name>_Contacts" -Role "Application Contact-
s.Read" -App <ObjectId> -CustomResourceScope "<ScopeName>"
```

Example for two custodians with archived mailbox access:

```
New-ManagementRoleAssignment -Name "Jane_EWS" -Role "Application EWS.AccessAsApp" \
        -App 57b270fd-8b3f-47c3-9a12-29083613dff1 -CustomResourceScope "Jane"
        New-ManagementRoleAssignment -Name "John_EWS" -Role "Application EWS.Ac-
cessAsApp" \
        -App 57b270fd-8b3f-47c3-9a12-29083613dff1 -CustomResourceScope "John"
```

20.5.4.1 Naming tip

The *-Name* parameter must be unique across all role assignments.

The *-CustomResourceScope* must exactly match the -Name you used in New-ManagementScope for that user. For example, all of Jane's assignments should use -CustomResourceScope "Jane" regardless of how you name the individual assignments.

20.5.5 Verify the configuration

After completing the above steps, use the following command to verify that the correct permissions are applied to a specific mailbox:

```
Test-ServicePrincipalAuthorization \
        -Identity <FriendlyNameForYourApp> \
        -Resource <user@yourdomain.com> | Format-Table
```

Example:

```
Test-ServicePrincipalAuthorization -Identity FilteredMailboxApp -Resource jane.-
doe@contoso.com | Format-Table
```

The output will list the permissions that your application has been granted for that specific mailbox. If a permission does not appear, verify that the Management Scope name and CustomResourceScope match exactly, and that the Service Principal Object ID was used. Not the Application Object ID.

20.6 Troubleshooting

This section covers common issues you may encounter when configuring or validating mailbox access and RBAC scoping.

Use the scenarios below to quickly identify misconfigurations, permission assignment problems, or command-line errors before continuing with setup.

20.6.1 Application can still access unscoped mailboxes

Verify that the mail-access permissions (Mail.Read, Calendars.Read, Contacts.Read, EWS.AccessAsApp) are not assigned directly on the Azure Application Registration. Any permission assigned directly to the app bypasses RBAC scoping entirely.

20.6.2 Test-ServicePrincipalAuthorization shows no permissions

Confirm the -Identity value matches the DisplayName used in New-ServicePrincipal

Confirm the CustomResourceScope in New-ManagementRoleAssignment exactly matches the Name used in New-ManagementScope

Confirm you used the Service Principal Object ID from Enterprise Applications and not the Application Object ID from App Registrations.

20.6.3 PowerShell commands return an error or unexpected results

Ensure you are connected to Exchange Online PowerShell with a global admin or Exchange admin account

Re-run Get-ServicePrincipal to confirm the Service Principal was created successfully before proceeding to later steps

20.6.4 macOS: zsh: command not found

You are running commands in zsh instead of PowerShell. Start PowerShell with pwsh and run the cmdlets in the PS prompt.

21 Microsoft 365 - SharePoint data source

This topic provides details on how to capture Microsoft 365 SharePoint with Collect.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

21.1 Considerations

Note the following considerations about this data source:

- SharePoint collections are not custodian-centric. You select the SharePoint sites you want to collect from.
  - You do not need to configure custodians.
  - Collect gathers all files within the selected sites regardless of who created or edited them.
- You can only collect parent level sites. You cannot collect sub-sites without collecting the parent level sites.
- Web Forms are not collected.
- Some Teams attachments may exist on the SharePoint sites.
  - Teams chat data should live within the group mailbox of a Teams channel or the users mailbox for 1:1 chats.
  - For more information, see Microsoft 365 - Teams data source on page 134.
- This data source is available to Relativity aiR Government customers collecting from Microsoft GCC High tenants.
  - No new permissions are needed.
  - These data sources work the same way but have different icons within Collect.
- If the Azure Application Registration secret changes or expires, update all Microsoft data sources that use that registration. Go to *Collect Admin*, select each affected data source, click *Edit*, enter the new secret in the Application Secret field, and click *Save*.

21.2 Collection size

SharePoint collections operate at the site level and are sensitive to the number and size of sites included.

Category	Details
Hard limits (enforced)	30 targets per job
Planning thresholds (guidance)	Large sites or many subsites slow down
When to split	Many large sites in one job
Notes	Site-level targeting only

Avoid grouping many large sites in a single job. Break collections into smaller site sets to maintain throughput.

21.3 Task checklist

The table lists the order to perform the necessary tasks for setting up the data source for Collect.

Order	Application	Task
1	Azure	Registering the Collect application below
2	Azure	Obtaining a client secret on the next page
3	Azure	Setting API permissions on page 129
4	Collect	Creating the data source in Collect on page 132
5	Collect	Configuring the data source in Collect on page 133

21.4 Accessing Microsoft 365 tenants

Register the Collect application to access Microsoft 365. When registering the application, the Microsoft 365 administrator creates a Microsoft Application ID and secret.

You will use this ID and secret to configure data sources in Collect and provides access to the Microsoft 365 tenants. You can register the application through Azure Portal or by registering the application permissions through the Microsoft App Registration Portal.

After registering the application, request administrator consent. From there, it is possible to revoke application access.

Depending on your Relativity aiR license, commercial or government, and your Microsoft tenant, Microsoft 365 or Microsoft 365 Government, you will be able to collect from either Microsoft 365 or both Microsoft 365 and Microsoft 365 Government data sources. Commercial users can only collect from Microsoft 365 tenants. Government users can collect from Microsoft 365 and Government 365 tenants. These data sources act the same, but have different icons within Collect.

21.4.1 Registering the Collect application

Start with registering your application in the Azure portal by following the steps below.

Caution: The listed permissions and roles are required and supported by Relativity.

- Relativity does not support substitutions or reduced permissions.
- You can submit requests for alternative or reduced permissions as product feedback.

For more information on registering an application in the Azure portal, refer to documentation on Microsoft's site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Click **App registrations**.
4. Click **New Registration** to display the Register an application page.
5. Enter an application name in the **Name** field.
6. Accept the default setting, **Accounts in this organizational directory only**, as the supported account type.
7. Click **Register**.
8. Once the application is registered, make note of the **Application (client) ID** and **Directory (tenant) ID** for use later when configuring the data source in Relativity aiR Collect.

21.4.2 Obtaining a client secret

Next, obtain the client secret for the registered application in the Azure portal. For more information, see relevant Microsoft documentation on the Microsoft site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **Certificates & secrets** option in the left navigation bar.
2. Click the **Client secrets** tab.
3. Click **New client secret**.
4. Enter a description for the client secret in the **Description** text box.
5. Select **730 days (24 months)** from the Expires list. The client secret will expire after this time frame.
    - Once the client secret expires, you must create a new client secret in the Azure portal as described in these steps.
    - Then you must update your Microsoft 365 Collect data sources with it. For more information, see Expired Azure client secrets on the next page.
    - For any additional assistance with client secrets, please contact the Azure Admin in your organization.
6. Click **Add** to create a new secret.

    Caution: Microsoft will only show the secret value this one time. There is no way to recover a secret.

7. Click the copy icon to copy the **Secret Value** to the clipboard.
    - Paste it to a safe location.
    - You will use the Secret Value later when creating the data source in Collect.
    - Confirm you copy the *Secret Value* and not the Secret ID.
8. Give your Relativity Admin the Application ID and the Client Secret for setup of Collect.
    - This application secret is also needed for setting up a Microsoft Entra ID integration point.
    - For more information, see the Integration Points guide.

21.4.2.1 Expired Azure client secrets

If your Azure client secret expires, follow these steps:

1. Get a new secret as outlined in the steps above.
2. Go to **Collect Admin** in Relativity aiR.
3. Select the desired data source that has expired, and click **Edit**.
4. Input the new client secret value in the **Application Secret** field.
5. Click **Save**.

You must repeat these steps for all Microsoft data sources that you have set up.

21.4.3 Setting API permissions

Each data source has its own set of permissions necessary to allow access to the tenants. To add the correct permissions based on your selected Microsoft 365 data source, follow the steps below.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **API permissions** option in the left navigation bar. The User-.Read permission is automatically added by default.
2. Click **Add a permission**.
3. Click **Microsoft Graph**.
4. Select **Application Permissions**.
5. Select the following permissions from the Permission list. Refer to *Azure Application Registration Permissions for Collect* below for more information about these permissions.
    - Files.Read.All
    - Sites.Read.All
6. Click **Add permissions**.
7. Click **Grant Permission**.
8. Make a note of the application ID that Microsoft assigned to the app registration. This ID is also required for setup of data sources in Collect.
9. The window will show all permissions granted. Verify that all permissions have been granted..
10. Click **Accept** to grant the permissions.

21.4.3.1 Azure Application Registration Permissions for Collect

The Collect application in Relativity aiR is a tool designed to streamline the data collection process for eDiscovery. Its primary purpose is to gather data from various sources, such as cloud-based applications and other data repositories, in a manner that is secure, defensible, and efficient. Collect aims to reduce the time and effort involved in data collection, ensuring that the data is accurate and complete, while maintaining chain of custody and compliance with legal and regulatory requirements.

Due to the architecture of the Collect application, Delegated permission can't be used and are not supported. The Collect application requires the use of Microsoft Graph API Azure Application permissions to facilitate the collection of data that occurs in processes running in the background.

The Collect application requires specific Graph API Application permissions be granted to an Azure Application Registration to facilitate efficient and comprehensive data collection for e-discovery and compliance purposes.

Following is an explanation of each Azure application Graph API permission required and why it is needed to support collections of M365 data. For a PDF of this information, see Azure Application Registration Permissions for Collect.

Required Azure Application Graph API Permissions:

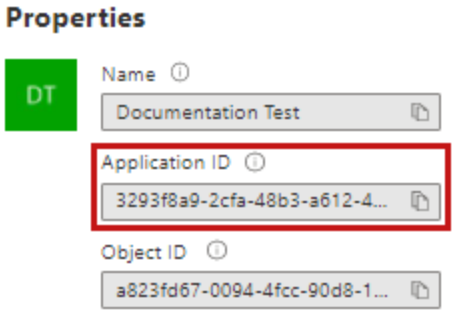
1. **Calendars.Read**—this permission allows Relativity to access calendar events. For e-discovery, it's important to capture calendar data as it can provide crucial context, timelines, and evidence related to the case or investigation.
2. **ChannelMember.Read.All**—this permission provides access to the membership information of all Teams channels. It allows Relativity to see who is part of each channel, which can be important for understanding who had access to certain communications and information during an investigation.
3. **ChannelMessage.Read.All**—this permission provides access to all messages in Microsoft Teams channels. It allows Relativity to capture and review conversations and discussions that take place in Teams channels, which may contain pertinent information for legal or compliance purposes.
4. **Chat.Read.All**—this permission enables Relativity to read all chat messages in Microsoft Teams. This includes private chats between users. Access to these messages is essential for gathering complete communication records and ensuring that no relevant information is overlooked in an investigation.
5. **Contacts.Read**—this permission allows access to contacts and is necessary to gather information about communications and relationships between individuals, which can be critical in understanding the full scope of interactions and connections in an investigation.
6. **eDiscovery.Download.Read**—this permission allows Relativity to download export packages and item reports from Microsoft Purview eDiscovery. These exports can contain documents, emails, Teams messages, and other collected data that are relevant to a legal matter or compliance review. This permission is required to retrieve exported data from Microsoft Purview for processing and review.
7. **eDiscovery.ReadWrite.All**—this permission allows Relativity to read and manage Microsoft Purview eDiscovery objects, including cases, custodians, holds, searches, review sets, and exports. It enables Relativity to create and manage e-discovery workflows programmatically, helping organizations automate the identification, preservation, collection, and review of potentially relevant information for legal and compliance matters.
8. **Files.Read.All**—this permission enables Relativity to access all files in OneDrive and SharePoint. It is essential for collecting documents, spreadsheets, presentations, and other files that might contain relevant information for a legal matter or compliance review. This permission is also required to support collection of linked OneDrive and SharePoint files in Outlook emails and Teams chats.
9. **Full_access_as_app Permission**—the Microsoft Graph API does not support accessing Outlook Online Archives (Archived Mailboxes). We utilize Microsoft's Exchange Web Services (EWS) API to collect Archived Mailboxes.
10. **Group.Read.All**—this permission allows Relativity to read all groups in the directory, including their properties and memberships. It helps in understanding the structure and membership of various groups within the organization, which can be important for context in e-discovery and compliance scenarios.
11. **Mail.Read**—this permission allows access to emails, which is one of the core components of e-discovery. This permission allows Relativity to read email messages in users' mailboxes to identify, preserve, and analyze communications that are pertinent to the case.
12. **Sites.Read.All**—this permission allows Relativity to access all SharePoint sites, including content and metadata. It ensures that any relevant information stored in SharePoint sites can be collected and reviewed.
13. **Team.ReadBasic.All**—this permission allows Relativity to read basic properties of all Teams. It helps in identifying and understanding the different Teams within the organization, their purposes, and their memberships, which can be relevant for investigations and compliance checks.

14. **TeamsTab.Read.All**—this permission allows Relativity to read the properties of all tabs in Microsoft Teams. Tabs can contain important resources, documents, and tools that users interact with. Access to this information can provide additional context and insights into the work and communications of users.
15. **User.Read.All**—this permission provides access to read the properties and membership of users. It is useful for identifying and understanding the roles, permissions, and activities of different users within the organization, which can be relevant for investigations and compliance checks.

21.5 Finding Azure credentials

If an application is already created and you need to find the application information to complete the Source Connection step, follow the steps below in the Azure Portal. For more information, see relevant Microsoft documentation on the Microsoft site.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Navigate to **Enterprise applications**.
4. In the list of applications, locate and click on your application.The application page displays.
5. Navigate to **Properties**.
6. Click the **copy icon** next to the **Application ID**. The ID is copied to your clipboard to use as needed.



21.6 Revoking application access

Revoke the application from the Azure portal or by using a PowerShell script. For more information, see Microsoft's documentation.

21.6.1 Revoking access via Azure Portal

To revoke access from the Azure portal:

1. Open your Azure Portal.
2. Navigate to **Enterprise Application**.
3. Under **All applications**, search for your application and click its link.
4. Under **Manage > Properties**, click **Delete**.

Collect no longer has access.

21.6.2 Revoking access via Powershell

Revoke access in Powershell using the Remove-MsolServicePrincipal script. See the Powershell example below of retrieving and deleting an application registration.

```
Get-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602

ExtensionData : System.Runtime.Serialization.ExtensionDataObject
AccountEnabled : True
Addresses : {}
AppPrincipalId : 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
DisplayName : Relativity-Development-Application
ObjectId : 51798fb3-e72c-4373-8c63-6e7d0dd63ad7
ServicePrincipalNames : {19ab8a2e-ccce-4fa8-a9ee-eb16e220d602}
TrustedForDelegation : False

Remove-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
```

21.7 Creating the data source in Collect

The Collection Admin tab is where you create, edit, and remove data sources from your workspace. You only need to complete setup once for each data source. You must create your data sources before setting up your targets.

In Relativity aiR, navigate to **Collect**.

1. Click the **New Collection Source Instance** button.
2. Enter in a unique name for the data source.
3. Select **M365 - SharePoint** or **G365 - SharePoint**.

   Note: Collect automatically collects any preserved data that has an in-place hold or litigation hold. Microsoft stored data on a hold in a preservation library and separate folders. For more information, see Microsoft Retention Policies.
4. Enter the required information in Settings. For more information, see Settings fields below.
5. Click **Save**.

After clicking Save, Relativity verifies the parameters and connectivity to the Microsoft 365 data source. If successful, Relativity saves the data source. If the connection fails, a message appears indicating the connection failed. If verification fails, verify that the values are correct. Relativity will save the data source when you correct it and it's verified.

Once the set up is complete, the data source information on the Collect Admin page.

21.7.1 Settings fields

To connect Relativity to a Microsoft SharePoint data source, you need to gather and enter the information for the following fields:

- **Domain**—enter the Tenant ID or Primary domain, domain name usually ends with .onmicrosoft.com, of the Microsoft 365 tenant the collection is intended for. To locate the tenant ID or primary domain name, see Microsoft documentation.
- **Application Id**—enter the Application ID created during registering the Collect application in Microsoft 365.

- **Application secret**—enter the Application Secret created during registering the Collect application in Microsoft 365.

Depending on your Relativity aiR license, commercial or government, and your Microsoft tenant, Microsoft 365 or Microsoft 365 Government, you will be able to collect from either Microsoft 365 or both Microsoft 365 and Microsoft 365 Government data sources. Commercial users can only collect from Microsoft 365 tenants. Government users can collect from Microsoft 365 and Government 365 tenants. These data sources act the same, but have different icons within Collect.

21.7.2 Data source details

Each data source details page includes an Action console. Each data source has different actions.

On the SharePoint data source page, you should see an Actions console with two options:

- **Refresh sites**—click to make Relativity check your SharePoint for disconnected or new sites.
- **Validate Connection**—click to validate the client ID, certificate, and other credentials with Microsoft 365.

21.8 Configuring the data source in Collect

In Relativity aiR, configure the data sources chosen in the Collection Details step.

21.8.1 Data source criteria

Add criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.
- **Operator**—choose an operator such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

After selecting field options, you must click **Add Criteria**.

Details to know about criteria:

- Each criteria is then separated by an AND operator.
- Leave the data source criteria empty to collect all data from the sources.

21.8.1.1 Criteria

Filter a data source's data that you want to collect by adding criteria. This section covers the different criteria for each data source. It also includes what you can search within each data source.

Relativity aiR only collects user created files that meet the filter criteria entered. Be aware that it does not collect Web Forms.

The following table lists the filter criteria support for SharePoint collections.

Note: You must register Relativity in Microsoft 365 before using this data source. For information on registering Relativity in Microsoft 365, see Accessing Microsoft 365 tenants on page 127.

When using search criteria to filter for Microsoft 365 SharePoint, different operators can return different results. Knowing the search operators is crucial.

All dates are in Coordinated Universal Time (UTC).

Criteria	Operators	Description	Example
Start Date	Equals	When you use the Start Date property in a query, the search returns calendar items that exist the day of and after the entered date.	When you search a Start Date of 1/1/2001 and an End Date of 1/1/2020, Collect returns all calendar items on and between the two dates.
End Date	Equals	When you use the End Date property in a query, the search returns all calendar items the day of and before the entered date.	When you search a Start Date of 1/1/2001 and an End Date of 1/1/2020, Collect returns all calendar items on and between the two dates.

21.8.2 Collecting preserved files

When you run a collection from SharePoint, Collect includes all available content, including any items that have been preserved. No additional configuration is required to ensure preserved SharePoint files are collected. For more information on preserving data, see the Legal Hold guide.

When a SharePoint site is placed under a preservation hold, Microsoft creates a *Preservation Hold Library* for the site. The contents of the Preservation Hold Library are automatically included in collections.

During collection, Collect automatically gathers content stored in the Preservation Hold Library. This ensures that both current files and preserved copies created as a result of the hold are included in the collected data set.

Relativity collects all versions of the document available in the preservation library. Collecting all versions of a document means that Relativity collects multiple versions of the same file with the corresponding SHA-256 hashes for each version of the data. If there were changes in the file version, the hash should be unique. For more information on hash identifiers, see Hash identifier - SHA-256 on page 173.

21.9 Troubleshooting

Job status	Error log	Cause	Resolution
InvalidLicense	Needs a valid license to access this API.	A target of the collection does not have the correct license.	See the section on Licenses for a list of valid license. You can find the list of unlicensed users in the errors.csv file included in the results of the collection.

22 Microsoft 365 - Teams data source

This topic provides details on how to capture Microsoft 365 Teams with Collect.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

22.1 Considerations

Note the following considerations about this data source:

- Requires enhanced licensing - E5 licensing. For more information, see Licensing requirements on page 136.
- Attachments have a 200MB limit for collections.

- We recommend limiting the date range of the collection.
  - Extended date ranges can increase collection time and potentially create issues.
  - For more information, see Collection size.
- Collect uses the Teams API endpoints.
  - The Teams export does not currently support access to preserved Teams chat messages.
  - This endpoint does not navigate to recoverable items folders. For example, the SubstrateHold folder.
- If the Azure Application Registration secret changes or expires, update all Microsoft data sources that use that registration. Go to *Collect Admin*, select each affected data source, click *Edit*, enter the new secret in the Application Secret field, and click *Save*.

22.1.1 Grouped collection

Teams data is collected into grouped collections. Chat conversations often include multiple custodians in the same message threads or channels. Relativity collects this data as a single grouped data set rather than splitting messages by individual custodian.

For more information on grouped collections, see Grouped collections on page 167.

22.1.2 Attachments and linked cloud files

Relativity includes files directly attached to conversations are included as children to the parent RSMF file that is generated during collection.

Relativity retrieves the linked cloud files residing in OneDrive and SharePoint during Teams collections. Currently, the most recent version of the file is retrieved. If the file no longer exists or is inaccessible, an item-level error is recorded in the errors report for the target collection. Relativity includes linked cloud files are included as children to the parent RSMF.

22.1.3 Collection size

Teams collections are slower relative to other Microsoft sources due to API constraints and high activity levels.

Category	Details
Hard limits (enforced)	30 custodians per job
Planning thresholds (guidance)	About 0.5 GB/hour per custodian (average) Active tenants slow even with short ranges
When to split	Active channels over long periods
Notes	Slower due to Teams Export API

Plan for slower throughput. Always segment long or highly active channel collections.

22.2 Task checklist

The table lists the order to perform the necessary tasks for setting up the data source for Collect.

Note: Separate Microsoft data sources inside Collect can use the same Microsoft Azure app registration. This means you only need to create one Microsoft Graph application and provide one Client ID and one Client Secret. You can then enter that same set of credentials for Microsoft data sources within Collect.

Order	Application	Task
1	Azure	Registering the Collect application below
2	Azure	Obtaining a client secret on the next page
3	Azure	Setting API permissions on page 138
4	Collect	Creating the data source in Collect on page 141
5	Collect	Configuring the data source in Collect on page 142

22.3 Accessing Microsoft 365 tenants

Register the Collect application in Azure to access Microsoft 365. When registering the application, the Microsoft 365 administrator creates a Microsoft Application ID and secret. You will use the ID and secret to configure data sources in Collect and they provide access to the Office 365 tenants. You can register the application through Azure Portal or by registering the application permissions through the Microsoft App Registration Portal. After registering the application, request administrator consent. From there, it is possible to revoke application access.

Depending on your Relativity aiR license, commercial or government, and your Microsoft tenant, Microsoft 365 or Microsoft 365 Government, you will be able to collect from either Microsoft 365 or both Microsoft 365 and Microsoft 365 Government data sources. Commercial users can only collect from Microsoft 365 tenants. Government users can collect from Microsoft 365 and Government 365 tenants. These data sources act the same, but have different icons within Collect.

22.3.1 Licensing requirements

With the Teams Export API, Relativity meets compliance when collecting data. To use the API and collect Teams chats, users must meet one of the following licensing requirements. This licensing applies to individual custodian accounts.

- Office 365 E5/A5/G5
- Microsoft 365 E5/A5/G5
- Microsoft 365 E5/A5/F5/G5 Compliance and Microsoft 365 F5 Security & Compliance
- Microsoft 365 E5/A5/F5/G5 Information Protection and Governance

For more information, see relevant Microsoft documentation on the Microsoft site:

- https://docs.microsoft.com/en-us/microsoftteams/export-teams-content
- https://docs.microsoft.com/en-us/graph/teams-licenses
- https://learn.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance#microsoft-graph-apis-for-teams-data-loss-prevention-dlp-and-for-teams-export

22.3.2 Registering the Collect application

Start with registering your application in the Azure portal by following the steps below.

Caution: The listed permissions and roles are required and supported by Relativity.

- Relativity does not support substitutions or reduced permissions.
- You can submit requests for alternative or reduced permissions as product feedback.

For more information on registering an application in the Azure portal, refer to documentation on Microsoft's site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Click **App registrations**.
4. Click **New Registration** to display the Register an application page.
5. Enter an application name in the **Name** field.
6. Accept the default setting, **Accounts in this organizational directory only**, as the supported account type.
7. Click **Register**.
8. Once the application is registered, make note of the **Application (client) ID** and **Directory (tenant) ID** for use later when configuring the data source in Relativity aiR Collect.

22.3.3 Obtaining a client secret

Next, obtain the client secret for the registered application in the Azure portal. For more information, see relevant Microsoft documentation on the Microsoft site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **Certificates & secrets** option in the left navigation bar.
2. Click the **Client secrets** tab.
3. Click **New client secret**.
4. Enter a description for the client secret in the **Description** text box.
5. Select **730 days (24 months)** from the Expires list. The client secret will expire after this time frame.
   - Once the client secret expires, you must create a new client secret in the Azure portal as described in these steps.
   - Then you must update your Microsoft 365 Collect data sources with it. For more information, see Expired Azure client secrets on the next page.
   - For any additional assistance with client secrets, please contact the Azure Admin in your organization.
6. Click **Add** to create a new secret.

   Caution: Microsoft will only show the secret value this one time. There is no way to recover a secret.

7. Click the copy icon to copy the **Secret Value** to the clipboard.
   - Paste it to a safe location.
   - You will use the Secret Value later when creating the data source in Collect.
   - Confirm you copy the *Secret Value* and not the Secret ID.

8. Give your Relativity Admin the Application ID and the Client Secret for setup of Collect.
    - This application secret is also needed for setting up a Microsoft Entra ID integration point.
    - For more information, see the Integration Points guide.

22.3.3.1 Expired Azure client secrets

If your Azure client secret expires, follow these steps:

1. Get a new secret as outlined in the steps above.
2. Go to **Collect Admin** in Relativity aiR.
3. Select the desired data source that has expired, and click **Edit**.
4. Input the new client secret value in the **Application Secret** field.
5. Click **Save**.

You must repeat these steps for all Microsoft data sources that you have set up.

22.3.4 Setting API permissions

Each data source has its own set of permissions necessary to allow access to the tenants. To add the correct permissions based on your selected Microsoft 365 data source, follow the steps below. For more information, see relevant Microsoft documentation on the Microsoft site.

Note: These steps must be completed by a Microsoft 365 administrator.

1. From the registered application's page, click the **API permissions** option in the left navigation bar. The User-.Read permission is automatically added by default.
2. Click **Add a permission**.
3. Click **Microsoft Graph**.
4. Select **Application Permissions**.
5. Select the following permissions from the Permission list. Refer to *Azure Application Registration Permissions for Collect* below for more information about these permissions.
    - User.Read.All
    - ChannelMessage.Read.All
    - Chat.Read.All
    - Files.Read.All
    - Group.Read.All
    - TeamsTab.Read.All
    - Team.ReadBasic.All
    - ChannelMember.Read.All
6. Click **Add permissions**.
7. Click **Grant Permission**.
8. Make a note of the application ID that Microsoft assigned to the app registration. This ID is also required for setup of data sources in Collect.

Notes:

- The window displays all permissions granted. Verify that all permissions have been granted.
- Click **Accept** to grant the permissions.

22.3.4.1 Azure Application Registration Permissions for Collect

The Collect application in Relativity aiR is a tool designed to streamline the data collection process for eDiscovery. Its primary purpose is to gather data from various sources, such as cloud-based applications and other data repositories, in a manner that is secure, defensible, and efficient. Collect aims to reduce the time and effort involved in data collection, ensuring that the data is accurate and complete, while maintaining chain of custody and compliance with legal and regulatory requirements.

Due to the architecture of the Collect application, Delegated permission can't be used and are not supported. The Collect application requires the use of Microsoft Graph API Azure Application permissions to facilitate the collection of data that occurs in processes running in the background.

The Collect application requires specific Graph API Application permissions be granted to an Azure Application Registration to facilitate efficient and comprehensive data collection for e-discovery and compliance purposes.

Following is an explanation of each Azure application Graph API permission required and why it is needed to support collections of M365 data. For a PDF of this information, see Azure Application Registration Permissions for Collect.

Required Azure Application Graph API Permissions:

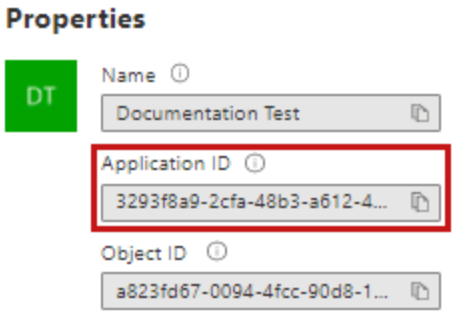
1. **Calendars.Read**—this permission allows Relativity to access calendar events. For e-discovery, it's important to capture calendar data as it can provide crucial context, timelines, and evidence related to the case or investigation.
2. **ChannelMember.Read.All**—this permission provides access to the membership information of all Teams channels. It allows Relativity to see who is part of each channel, which can be important for understanding who had access to certain communications and information during an investigation.
3. **ChannelMessage.Read.All**—this permission provides access to all messages in Microsoft Teams channels. It allows Relativity to capture and review conversations and discussions that take place in Teams channels, which may contain pertinent information for legal or compliance purposes.
4. **Chat.Read.All**—this permission enables Relativity to read all chat messages in Microsoft Teams. This includes private chats between users. Access to these messages is essential for gathering complete communication records and ensuring that no relevant information is overlooked in an investigation.
5. **Contacts.Read**—this permission allows access to contacts and is necessary to gather information about communications and relationships between individuals, which can be critical in understanding the full scope of interactions and connections in an investigation.
6. **eDiscovery.Download.Read**—this permission allows Relativity to download export packages and item reports from Microsoft Purview eDiscovery. These exports can contain documents, emails, Teams messages, and other collected data that are relevant to a legal matter or compliance review. This permission is required to retrieve exported data from Microsoft Purview for processing and review.
7. **eDiscovery.ReadWrite.All**—this permission allows Relativity to read and manage Microsoft Purview eDiscovery objects, including cases, custodians, holds, searches, review sets, and exports. It enables Relativity to create and manage e-discovery workflows programmatically, helping organizations automate the identification, preservation, collection, and review of potentially relevant information for legal and compliance matters.
8. **Files.Read.All**—this permission enables Relativity to access all files in OneDrive and SharePoint. It is essential for collecting documents, spreadsheets, presentations, and other files that might contain relevant information for a legal matter or compliance review. This permission is also required to support collection of linked OneDrive and SharePoint files in Outlook emails and Teams chats.

9. **Full_access_as_app Permission**—the Microsoft Graph API does not support accessing Outlook Online Archives (Archived Mailboxes). We utilize Microsoft's Exchange Web Services (EWS) API to collect Archived Mailboxes.
10. **Group.Read.All**—this permission allows Relativity to read all groups in the directory, including their properties and memberships. It helps in understanding the structure and membership of various groups within the organization, which can be important for context in e-discovery and compliance scenarios.
11. **Mail.Read**—this permission allows access to emails, which is one of the core components of e-discovery. This permission allows Relativity to read email messages in users' mailboxes to identify, preserve, and analyze communications that are pertinent to the case.
12. **Sites.Read.All**—this permission allows Relativity to access all SharePoint sites, including content and metadata. It ensures that any relevant information stored in SharePoint sites can be collected and reviewed.
13. **Team.ReadBasic.All**—this permission allows Relativity to read basic properties of all Teams. It helps in identifying and understanding the different Teams within the organization, their purposes, and their memberships, which can be relevant for investigations and compliance checks.
14. **TeamsTab.Read.All**—this permission allows Relativity to read the properties of all tabs in Microsoft Teams. Tabs can contain important resources, documents, and tools that users interact with. Access to this information can provide additional context and insights into the work and communications of users.
15. **User.Read.All**—this permission provides access to read the properties and membership of users. It is useful for identifying and understanding the roles, permissions, and activities of different users within the organization, which can be relevant for investigations and compliance checks.

22.4 Finding Azure credentials

If an application is already created and you need to find the application information to complete the Source Connection step, follow the steps below in the Azure Portal. For more information, see relevant Microsoft documentation on the Microsoft site.

1. Open your Azure Portal.
2. Click **Microsoft Entra ID** (formerly known as Azure Active Directory).
3. Navigate to **Enterprise applications**.
4. In the list of applications, locate and click on your application.The application page displays.
5. Navigate to **Properties**.
6. Click the **copy icon** next to the **Application ID**. The ID is copied to your clipboard to use as needed.



22.5 Revoking application access

Revoke the application from the Azure portal or by using a PowerShell script. For more information, see Microsoft's documentation.

22.5.1 Revoking access via Azure Portal

To revoke access from the Azure portal:

1. Open your Azure Portal.
2. Navigate to **Enterprise Application**.
3. Under **All applications**, search for your application and click its link.
4. Under **Manage > Properties**, click **Delete**.

Collect no longer has access.

22.5.2 Revoking access via Powershell

Revoke access in Powershell using the Remove-MsolServicePrincipal script. See the Powershell example below of retrieving and deleting an application registration.

```
Get-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602

ExtensionData : System.Runtime.Serialization.ExtensionDataObject
AccountEnabled : True
Addresses : {}
AppPrincipalId : 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
DisplayName : Relativity-Development-Application
ObjectId : 51798fb3-e72c-4373-8c63-6e7d0dd63ad7
ServicePrincipalNames : {19ab8a2e-ccce-4fa8-a9ee-eb16e220d602}
TrustedForDelegation : False

Remove-MsolServicePrincipal -AppPrincipalId 19ab8a2e-ccce-4fa8-a9ee-eb16e220d602
```

22.6 Creating the data source in Collect

The Collection Admin tab is where you create, edit, and remove data sources from your workspace. You only need to setup each data source once. You must create your data sources prior to setting up your custodian targets.

1. In Relativity aiR, navigate to **Collect**.
2. Click the **New Collection Source Instance** button.
3. Enter in a unique name for the data source.
4. Select **M365 - Teams** or **G365 - Teams**.

   Note: Collect automatically collects any preserved data in an in-place hold or litigation hold. Microsoft stored data on a hold in a preservation library and separate folders. For more information, see Microsoft Retention Policies.
5. Enter the required information in Settings. For more information, see Settings fields on the next page.
6. Click **Save**.

After clicking Save, Relativity verifies the parameters and connectivity to the Microsoft 365 data source. If successful, Collect saves the data source. If the connection fails, a message appears indicating the connection failed. If verification fails, verify that the values are correct. Collect will save the data source when it's corrected and verified.

Once the set up is complete, the data source information on the Collect Admin page.

22.7 Settings fields

To connect Relativity to a Microsoft Teams data source, you need to gather and enter the information for the following fields:

- **Domain**—enter the Tenant ID or Primary domain (domain name usually ends with .onmicrosoft.com) of the Microsoft 365 tenant the collection is intended for. To locate the tenant ID or primary domain name, see Microsoft documentation.
- **Application Id**—enter the application ID created during registering the Collect application in Microsoft 365.
- **Application secret**—enter the application secret created during registering the Collect application in Microsoft 365. For more information, see Accessing Microsoft 365 tenants on page 136.

Depending on your Relativity aiR license, commercial or government, and your Microsoft tenant, Microsoft 365 or Microsoft 365 Government, you will be able to collect from either Microsoft 365 or both Microsoft 365 and Microsoft 365 Government data sources. Commercial users can only collect from Microsoft 365 tenants. Government users can collect from Microsoft 365 and Government 365 tenants. These data sources act the same, but have different icons within Collect.

22.7.1 Data source details

Each data source details page includes an Action console. Each data source has different actions.

On the Microsoft Teams data source page, click **Validate Connection** in the Actions console to validate the client ID, certificate, and other credentials with Microsoft 365.

22.8 Configuring the data source in Collect

In Relativity aiR, configure the data sources chosen in the Collection Details step.

Notes:

- The Microsoft 365 Teams data source collects the most recent version of each message.
- Deleted messages are available to collect for 21 days from the time of deletion.
- Task module content is not currently supported for collection.

22.8.1 Data source criteria

Add criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.

  Note: You must add start and end dates to complete the Data Sources step.

- **Operator**—choose an operator such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

After selecting field options, you must click **Add Criteria**.

Details to know about criteria:

- Each criteria is then separated by an AND operator.
- Leave the data source criteria empty to collect all data from the sources.

The following table lists the filter criteria supported for Microsoft Teams collections.

Relativity collects Microsoft Teams data in RSMF.

Note: You must register Relativity in Microsoft 365 before using this data source. For information on registering Relativity in Microsoft 365, see Accessing Microsoft 365 tenants on page 136.

When using search criteria to filter for Teams, you must select start dates and end dates. All dates are in Coordinated Universal Time (UTC).

The maximum date range supported is five years. For example, you can select Start Date 1/1/2016 and End Date 1/1/2021, but no further.

Criteria	Operators	Description	Example
Chat Type	Equals	When you use the Chat Type property in a query, the search returns all messages in either Private Channels, Private Chats, or Public Channels.	If you search a Chat Type with the Public Channels operator selected, Relativity collects only messages in public channels that the custodians are in.
End Date	Less Than or Equals	When you use the End Date property in a query, the search returns all messages the day of and before the entered date.	If you search a Start Date of 1/1/2001 and an End Date of 1/1/2020, Collect returns all messages on and between the two dates.
Slice in Interval in Hours	Equals	When you use The Slice Interval in Hours property, the search returns all messages in a specific time range or defaults the slice interval to 24 hours.	If you search with a slice interval set to one hour and a conversation spans five hours, you will end up with five RSMFs after processing.
Start Date	Greater Than or Equals	When you use the Start Date property in a query, the search returns messages that exist the day of and after the entered date.	If you search a Start Date of 1/1/2001 and an End Date of 1/1/2020, Collect returns all messages on and between the two dates.

Included in the Microsoft 365 Teams criteria are two toggles:

- **Collect linked files external to M365**—enable the toggle to collect modern attachments, or files linked in Teams that are external to the Microsoft 365 tenant.
  - You must opt in to confirm that you want to collect files outside of Microsoft 365.
  - For more information, see Modern attachments below.

  Note: This option is only available for Relativity aiR production environments. Relativity aiR Government environments cannot collect external files.
- **Enable Dedupe**—enable the toggle to exclude cards contained in Teams chat messages. Due to the nature of how Microsoft provides card information, inclusion of cards prevents deduplication of RSMFs during processing. For more information, see Microsoft's documentation.

For more information, see Microsoft Security and Compliance Center documentation.

22.8.2 Modern attachments

When collecting Microsoft Teams data, files shared as modern attachments are collected as separate documents.

The Teams message contains a link to the file, while the file itself appears as a standalone record in Relativity aiR. This is expected behavior.

22.8.2.1 Validate modern attachments

Use the steps below to confirm that a modern attachment referenced in a Teams message was collected successfully.

1. Navigate to **Documents**.
2. Filter the *Record Type* by **File**.
3. Open a file and confirm Source Path shows a SharePoint or OneDrive location.
4. Copy part of the file name.
5. Search Documents for that file name.
6. Open the related Teams message.
   Record Type = Short Message, if available.
7. Confirm the message contains a cloud link to the file.

The file and message are linked as designed.

23 Refinitiv Eikon data source

This topic provides details on how to capture Refinitiv Eikon with Collect.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

23.1 Consideration

Note the following consideration about this data source:

- Refinitiv Eikon data is collected into grouped collections, resulting in a different data count compared to standard collections.
  - These grouped collections comprise a set of RSMFs (Relativity Short Message Format) containing all the chats for the assigned custodians. Due to this grouping, it is expected that custodian targets will have identical counts.
  - Essentially, when collecting data from multiple custodian targets, the item counts and sizes for each will match. This uniformity arises because the item count reflects the number of RSMF files generated for the job, while the size reflects the total size of the created RSMF file set.

23.2 Collection size

Eikon collections rely on SFTP-based export workflows, which introduces constraints on large exports.

Category	Details
Hard limits (enforced)	No global hard cap
Planning thresholds (guidance)	Long chat exports
When to split	Long date ranges

Category	Details
Notes	SFTP-based retrieval

Plan for segmentation when exporting long histories with SFTP.

23.3 Creating the data source

In Relativity aiR, use the following procedure to connect the Refinitiv Eikon data source to Collect.

1. Navigate to **Collection Admin** within Collect Admin of Set Up.
2. Click the **New Collection Source Instance** button.
3. Do the following:
    - Enter in a unique name for the data source.
    - Select the **Refinitiv Eikon** data source.
    - Enter the required information in the Settings fields. For more information, see Settings fields below.
4. Click **Save**. The data source displays on the Collection Admin page.

23.4 Settings fields

Find the information for these fields in the .json file:

- **Host**—enter the address of the Refinitiv Eikon host. For example, sftp.refinitiveikon.com.
- **Port**—enter the SFTP port.
- **Path**—enter the folder address of the stored files.
- **Username**—enter the username to your organization's Refinitiv Eikon site.
- **Password**—enter the password to your organization's Refinitiv Eikon site.

23.5 Configuring the data source

Each data source used in Collect has different search criteria on the Collection Details step when creating a collection job. The criteria needs to be configured next.

1. Configure search criteria to collect specific data.
    - **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
    - **Field**—choose the field to filter on within the data source.

      Note: You must add start and end dates to complete the Data Sources step.

    - **Operator**—choose an operator such as equals, contains, greater than, or less than.
    - **Value**—enter a value to find in the selected field.
2. Click **Add Criteria**. Each criteria is separated by an AND operator.

The following table lists the filter criteria supported for Refinitiv Eikon collections. Setting criteria for Refinitiv Eikon is not required.

Relativity collects Refinitiv Eikon chat data Relativity's short message format (RSMF).

All dates are in Coordinated Universal Time (UTC).

Criteria	Operators	Description	Example
Start Date	Greater Than or Equals	When you use the Start Date property in a query, the search returns chats that exist the day of and after the entered date.	When you search a Start Date of 1/1/2001 and an End Date of 1/1/2020, Relativity collects all calendar items on and between the two dates.
End Date	Less Than or Equals	When you use the End Date property in a query, the search returns all chats the day of and before the entered date.	When you search a Start Date of 1/1/2001 and an End Date of 1/1/2020, Relativity collects all calendar items on and between the two dates.

24 Slack data source

This topic provides details on how to capture Slack data with Collect.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

24.1 Considerations

Review the list of considerations before starting your collection:

- We recommend limiting the volume and number of custodians per job. Limiting both will reduce the collection time and reduce the chance of errors.
- We recommend limiting the date range of the collection. Extended date ranges can increase collection time and potentially create issues.
- We do not recommend collecting each custodian separately, with one collection collecting one custodian target.
  - This creates duplicate chats in cases where the custodians have been chatting with each other.
  - As a result, the collection can be more difficult to manage and review, and it may take longer to complete.
- Collect can retrieve messages from deactivated Slack users if the data still exists. This relies on the include_historical parameter.
  - Deactivation and channel membership does not block results. User accounts and message data remain tied to the user ID.
  - Retention is the key limiter. Deleted messages cannot be recovered; gaps require Slack Support review.
- Slack's discovery and compliance API does not support keyword searching.
  - This means Slack collections cannot include keyword-based searches.
  - Cannot use keyword search across direct or group messages.
  - For more information on Slack collection criteria, see Criteria on page 150.

24.1.1 Grouped collection

Slack data is collected into grouped collections. Chat conversations often include multiple custodians in the same message threads or channels. Relativity collects this data as a single grouped data set rather than splitting messages by individual custodian.

For more information on grouped collections, see Grouped collections on page 167.

24.1.2 Attachments and linked cloud files

Relativity includes files directly attached to conversations as children to the parent RSMF file that is generated during collection.

Retrieval of linked cloud files is not supported by Slack's Discovery API. Currently, the Collect application does not support ancillary collections during Slack collections to retrieve linked cloud files. Cloud file links are still present in the conversations contained in the generated RSMF files.

24.1.3 Collection size

Slack collections group shared messages, which improves efficiency, but activity level strongly impacts job size.

Government Slack follows the same general scaling patterns as commercial Slack but may introduce additional latency.

Category	Details
Hard limits (enforced)	30 custodians per job
Planning thresholds (guidance)	Greater than 20 custodians and 6 months or more, an active organization, is often too large
When to split	Greater than 6 months with high activity Greater than 12 months with low activity
Notes	Grouped collection shared messages collected once Gov environment may add latency

24.2 Task checklist

The table lists the order to perform the necessary tasks for setting up the data source for Collect.

Order	Application	Task
1	Slack	Slack application setup below
2	Collect	Creating the data source in Collect on the next page
3	Collect	Configuring the data source in Collect on page 150

24.3 Slack application setup

Before using the Slack data source in Collect, you must create and authorize Collect as an application within Slack.

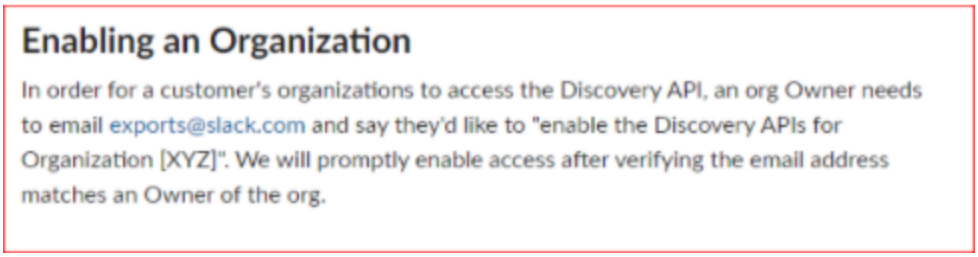
There are specific steps to connect Slack to Relativity when creating the data source. To set up the Slack data source, you need to enable API access with Slack and then complete the data source settings in Relativity.

For more information, see Relativity Collect: Collecting from a Slack Enterprise Data Source training video.

Your Slack organization must be on:

- **Enterprise Grid plan**—the Collect application requires the Enterprise Grid plan that provides access to the Discovery API.
- **GovSlack**—you will need a Slack FedRamp account. For more information, see Slack's documentation.

Before Slack can be set up as a Collect data source, the Slack organization owner needs to email exports@slack.com to gain Discovery API access. Follow the instructions on the Enabling an Organization window.



Once Slack confirms your Discovery APIs are enabled for your organization, proceed to set up your Slack data source in Relativity.

24.4 Creating the data source in Collect

After confirming that your Discover APIs are enabled, complete the set up process in Relativity aiR to connect the Slack data source to Collect

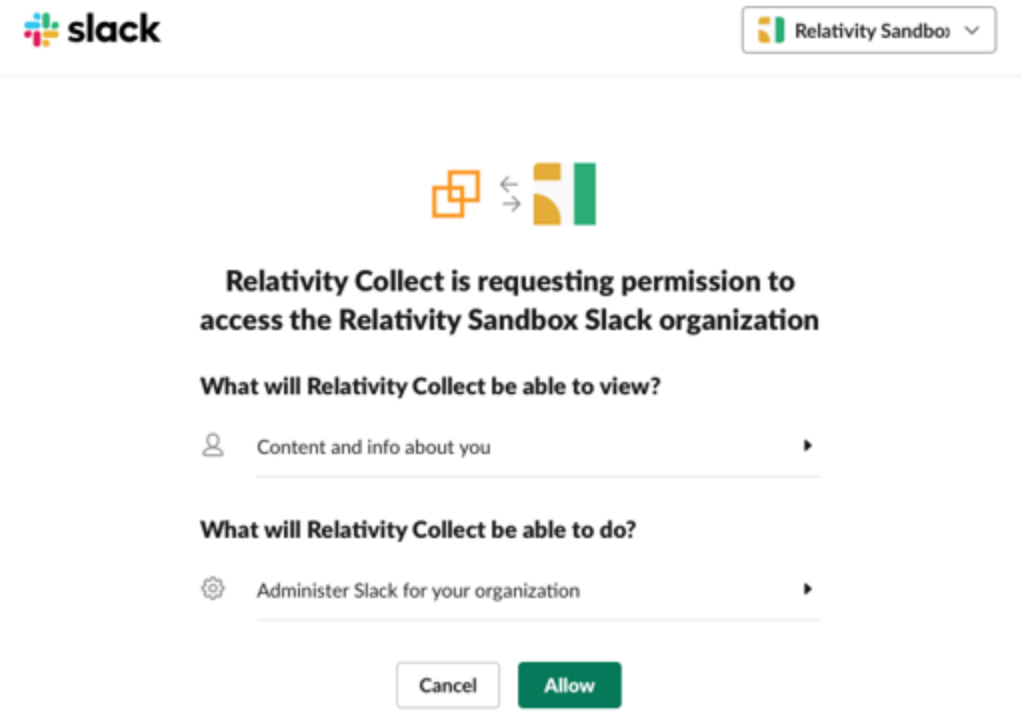
Note: You set up data source connections at a workspace level. You only need to set up a given data source connection once in a given workspace. For example, if you have three different workspaces to run collections in, you would need to set up the Slack data source connection three times, once for each workspace. If all collections are from just one workspace, then you only need to set up the data source once.

In Relativity aiR:

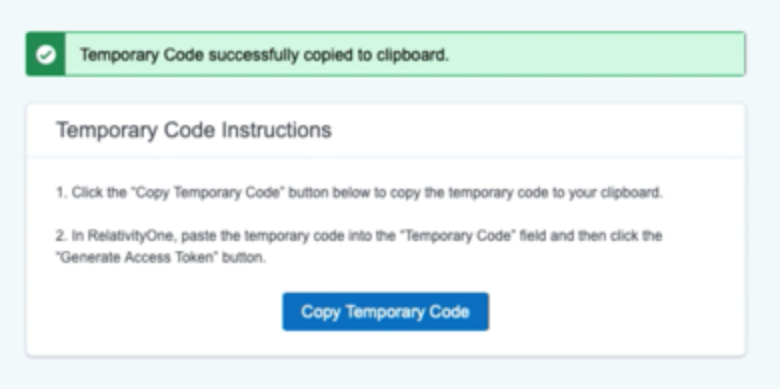
1. Navigate to **Collection Admin** within Collect Admin.
2. Click the **New Collection Source Instance** button.
    - **Name**—enter in a unique name for the data source.
    - **Type**—select the **Slack** data source.
3. Click **Install Application**. After clicking the **Install Application**, a window from Slack appears. You must disable pop-ups in your browser to see the window.

    Notes:
    - If you already logged in, you will see a window with an Allow button to authorize the Collect application. If you did not log in, you must log in as the organization owner. Make sure you enter the organization URL when signing in.
      If you logged into multiple organizations, make sure to select the correct one in the drop-down menu in the top-right corner. If you do not know your organization URL, you can find it in the Overview section of **About This Workspace** in Slack.
    - Add an organization to the drop-down menu by opening a new window outside of this workflow and sign into another organization. Another option is to log out of the current organization before clicking Install Application and logging in when requested.

4. Click the **Allow** button.



5. After clicking **Allow**, navigate in the same window to a page where you will copy a temporary token.
6. Click **Copy Temporary Code** to copy to your clipboard.



7. Once copied, you can close that window and return to Relativity aiR.
8. In Collect, paste the code in the **Temporary Code** field.
9. Click **Generate Access Token**.The access token will be generated and populated in the Access Token field below.

   Notes: Paste this token in the Access Token field in any other additional workspaces you want to setup.

10. Click **Save**.

24.5 Settings fields

To connect Relativity to the Slack data source, you need to gather and enter the information for the following fields. Setting up Slack includes steps outside of Collect. To get the steps to gather the temporary code and access token, see Slack application setup on page 147.

- **Temporary Code**—enter the code provided by Slack after installing application. The Generate Slack Access token section provides steps to retrieve the Temporary Code and Access Token.
- **Access Token**—enter the application token retrieved after authorizing Relativity as an application in Slack. For more information, see Slack documentation.

24.6 Configuring the data source in Collect

Each data source used in Collect has different search criteria on the Collection Details step when creating a collection job. The criteria needs to be configured next.

1. Configure search criteria to collect specific data.
    - **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
    - **Field**—choose the field to filter on within the data source.

      Note: You must add start and end dates to complete the Data Sources step.

    - **Operator**—choose an operator such as equals, contains, greater than, or less than.
    - **Value**—enter a value to find in the selected field.
2. Click **Add Criteria**. Each criteria is separated by an AND operator.

24.6.1 Criteria

The following table lists the filter criteria supported for Slack collections. Slack collections require you to enter the start date and end data criteria. Slack puts a limit on how far back you can run a collection. Your organization's Slack enterprise retention policy sets this time period. For more information, see Slack documentation.

Note: You need to register Relativity in Slack before using this data source. For information on registering Relativity in Slack, see Slack documentation.

When using the Slack data source:

- You can collect Archived Slack channels.
- You cannot collect deleted Slack channels.
- Relativity collects Slack data in Relativity Short Message Format (RSMF).
- RSMF has a 2 GB processing limit. For more information, see the RSMF guide.

All dates are in Coordinated Universal Time (UTC).

Criteria Field	Operators	Description	Example
Channel Name	Equals	When you use the Channel Name property, the search returns all message within the channels that equals the search word or phrase	If you use the Channel Name property in a query, the search returns all messages that the channel name equals the text you're searching for. In other words, the query does not return only those messages from channels that have an exact match. For example, if you

Criteria Field	Operators	Description	Example
		in the channel's name.	search for subject “finance_team,” your results include messages from channels like "finance_team_project.”
Conversation Type	Equals	When you use the Conversation Type property in a query, the search returns all messages that were either in a direct message or group message.	If you use the Group Message conversation type in a query, the search results returns messages that exist in group messages. Direct, one-on-one messages will not be included in the collection.
End Date	Less Than Or Equals	When you use the End Date property in a query, the search returns all messages the day of and before the entered date.	If you search a Start Date of 1/1/2001 and an End Date of 1/1/2020, the search returns all messages on and between the two dates. We recommend limiting the date range to maintain a high performance level and a lower collection time.
Inclusive Channels	Equals	When you use the inclusive option, only the specified channels will be collected. You can enter channel names and/or channel IDs; use commas to separate multiple entries.	If you want to include the General and Contracts channels, enter: general, contracts. **Note:** Channel names and IDs are not case sensitive.
Exclusive Channels	Equals	When you use the exclusive option, all channels except the excluded channels will be collected. You can enter channel names and/or channel IDs; use commas to separate multiple entries.	If you want to exclude the General and Contracts channels, enter: general, contracts. **Note:** Channel names and IDs are not case sensitive.
Slice Interval in Hours	Equals	When you use The Slice Interval in Hours property, the search returns all messages in a specific time range or defaults the slice interval to 24 hours.	If you search with a slice interval set to one hour and a conversation spans five hours, you will end up with five RSMFs after processing.
Start Date	Greater Than Or Equals	When you use the Start Date property in a query, the search returns messages that exist the day of and after the entered date.	If you search a Start Date of 1/1/2001 and an End Date of 1/1/2020, the search returns all messages on and between the two dates. We recommend limiting the date range to maintain a high performance level and a lower collection time.
Workspace Name	Equals	When you use the Workspace Name property, the search returns all messages in all channels within the workspace that equals the search word or phrase in the workspace's name	If you use the Workspace Name property in a query, the search returns all messages that the instance name equals the text you’re searching for. For example, if you search for subject “Company A,” your results include messages from that instance.

Included in the Slack Criteria are two toggles:

- **Disable RSMF conversion**—enable this toggle to keep data in its original format by preventing Relativity from converting the files into Relativity's short message format (RSMF) files.

  Note: Relativity provides you win .json files when running collections with this toggle enabled.

- **Deleted Messages Only**—enable this toggle to collect only deleted message that fit within the selected criteria.

24.6.2 Configuration considerations

Consider the following when configuring the Slack data source:

- If a Slack channel with same name exists across multiple Slack workspaces within a collection, Collect will collect all content in both channels in both workspaces.
- You can collect Direct Messages, Group Messages, or both Direct and Group messages. Do not select a conversation type if you want to collect all messages.
- The *Slice Interval in Hours* criteria defaults the slice interval to 24 hours. This means Collect will create one file for the conversations within that 24-hour interval. If the conversation goes beyond 24 hours, a second Relativity Short Message File (RSMF) will be created. Another example is if you have a slice interval set to one hour and a conversation spans five hours, you will end up with five RSMFs after processing.
- Collections include deleted messages. Relativity displays deleted messages on the day the user deleted the message, not the day the user sent the message.
  - Also, Relativity collects only the message when a deleted message includes an attachment. Files sent as attachments without a message and then deleted, the metadata is available for 24 hours, but the file is not collected.
  - When Relativity collects deleted messages in threads, Relativity displays the messages outside of the thread in the RSMF.
- Relativity collects conversations in public or private channels for each day in the date range regardless if the custodian participated in that channel on a given day.
- When collecting multiple custodians' data, and each custodian is in the same channel, Relativity collects the channel once.

25 Slack best practices

Collection time depends on collection scope, not data size.

25.1 Date range

Date range is one of the biggest factors. Collect reviews every day in every channel across your full date range. Each extra day increases collection time.

Multi-year date ranges are very large.

25.2 Channel scope

Channel scope is the other major driver. Slack content falls into four categories:

- **Direct messages (1:1s)**—private conversations between two users.
- **Multi-person direct messages (MPDMs)**—private group conversations outside channels.

- **Private channels**—invite-only channels.
- **Public channels**—channels open to all workspace members.

Collections with only direct messages and MPDMs are usually the fastest and most manageable. These collections typically do not need to be split by date range.

Adding channels increases scope:

- Private channels increase scope.
- Public channels, especially those with high message volume and many members, can greatly increase collection time.

For large date ranges with thousands or tens of thousands of channels, a single collection job across the full period is likely to fail.

25.3 Recommended approach for large collections

Run separate collection jobs by content type in this order:

1. Direct messages and MPDMs
2. Private channels
3. Public channels

This approach keeps jobs manageable and aligns with typical attorney priorities: direct messages first, private channel activity second, and public channel activity last.

For collections that include private or public channels:

- Start with a 3-month date range.
- If the job completes successfully, expand the range in later collections.
- If the job becomes slow or fails, reduce the date range and continue in smaller increments.

25.4 Intended use

The Slack connector is designed for targeted eDiscovery collections, not bulk data export. Slack's Discovery API supports precise, targeted data collection and is not built for bulk export use cases.

If you need to export large volumes of Slack data:

1. Export the data directly from Slack.
2. Use the Relativity aiR processing engine to convert the export to Relativity Short Message Format (RSMF).

Before you begin, review the Relativity aiR Processing supported file types for Slack to confirm your export will convert successfully.

26 X1 data source

This topic provides details on how to capture X1 data sources with Collect.

Note: This documentation contains references to third-party software, or technologies. While efforts are made to keep third-party references updated, the images, documentation, or guidance in this topic may not accurately represent the current behavior or user interfaces of the third-party software. For more considerations regarding third-party software, such as copyright and ownership, see Terms of Use.

26.1 Considerations

X1 data sources require separate licensing, configuration, and training through a third party. For example, X1. For more information, see X1's licensing documentation.

26.2 Collection size

X1 collections depend on upstream exports and behave similarly to email or file shares.

Category	Details
Hard limits (enforced)	Export-defined
Planning thresholds (guidance)	Large historical exports (Email) Large repositories (Files)
When to split	Long date ranges Large directory trees
Notes	Depends on upstream export

Split based on export size and structure, not just time or custodians.

26.3 Creating the data source

Use the following procedure to create a new Collect source instance.

1. Navigate to **Collection Admin** within Collect Admin of Set Up.
2. Click the **New Collection Source Instance** button.
3. Do the following:
   - **Name**—enter in a unique name for the data source.
   - **Type**—select **X1 Emails** or **X1 Files** the type of data source.
   - **Settings**—enter the required information in the Settings fields. For more information, see Settings fields below.
4. Click **Save**. The data source displays on the Collection Admin page.

26.4 Settings fields

To connect Relativity to an X1 data source, you need to gather and enter the information for the following fields. For more information on X1 fields, see X1's user documentation:

- **X1 Enterprise Manager Endpoint URL**—enter the endpoint URL of the X1 Manager Service. An example of a URL is https://mapleproject.x1dev.com:8443/. For more information, see X1's user documentation.
- **X1 Enterprise Manager Endpoint Port**—enter the port number used for Manager Service traffic.
- **X1 Downloader API Endpoint URL**—enter the endpoint URL of the X1 Downloader Service. An example of a URL is https://mapleproject.x1dev.com:8443/.
- **X1 Download API Endpoint Port**—enter the port number used for Downloader Service traffic.
- **Client ID**—enter the X1 Client ID found on the API Clients page in X1. For more information, see X1's user documentation.

- **Client Secret**—enter the X1 secret OAuth token copied from the X1 user interface. For more information, see X1's user documentation.
- **Project ID**—enter the Project ID found in the X1 user interface to automate X1 with a third party client via the API. For more information, see X1's user documentation.
- **Project Path**—enter the Global Project Collection path found in the X1 user interface. For more information, see X1's user documentation.
- **Target External ID**—enter the specific identifier of the email locations. Collect only searches the specified location.
- **Certificate Thumbprint**—enter the secured thumbprint that validates a self-signed SSL certificate. Locate the thumbprint in X1. For more information on locating the Certificate Thumbprint, see X1's user documentation.

26.5 Configuring the data source

Configure the data sources chosen in the Collection Details step. If you select multiple data sources in the first step, you'll configure all sources in the step. Switch between each source by clicking the name of the data source in the left navigation menu. Clicking **Next** and **Previous** also moves you through the data sources. Select individual data sources by clicking on the checkbox and then using the right arrows to select them. After selecting the data sources to configure, fill out the criteria. Each data source has different criteria to enter.

26.5.1 Data source criteria

Add criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.
- **Operator**—choose an operator such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

After selecting field options, you must click **Add Criteria**. Things to know about criteria:

- Each criteria is then separated by an AND operator.
- Leave the data source criteria empty to collect all data from the sources.

Filter a data source's data that you want to collect by adding criteria. This section covers the different criteria for each data source. This section also includes what you can search within each data source. The criteria options change based on the selected data source.

26.5.1.1 X1 emails

The following table lists the filter criteria supported for X1 Emails collections. Setting criteria for X1 emails is not required.

Note: You must register Relativity in X1 before using this data source. For information on registering Relativity in X1, see X1's user documentation.

All dates are in Coordinated Universal Time (UTC).

Criteria Field	Operators	Description	Example
Attachment	Contains,	When you use the Attachment Name,	If you search for "quarterly financial records,"

Criteria Field	Operators	Description	Example
Name	Does Not Equal, Equals	the search returns all attachments that contain the text in the name of the attachment file.	your search results will include the searched phrase from all attachment names in X1 email data sources.
BCC	Contains, Does Not Equal, Equals	When you use the Email From property in a query, the search returns all messages that contain the text in the Email BCC field.	If you search “@example.com,” your results include all blind carbon copied messages received by people with the @example.com in their email address.
CC	Contains, Does Not Equal, Equals	When you use the Email From property in a query, the search returns all messages that contain the text in the Email CC field.	If you search “@example.com,” your results include all carbon copied messages received by people with the @example.com in their email address.
Email Body	Contains	When you use the Email Body property in a query, the search returns all messages email message contains the text you’re searching for.	If you search “Dear John,” your results include all messages that contain the text in email body. Note that this is not the same as searching for “Dear” OR “John”. In order to do that, you need to separate keyword by OR
Folder Path	Contains, Does Not Equal, Equals	When you use the File Path property in a query, the search returns all messages equals/does not equal or contain the folder path entered.	If you search “Contains C:/-documents/Relativity,” your results include all files within the listed folder and any folder beyond the file path entered.
Free Form Search	Equals	Searches across all data sources simultaneously with general searching options. For more information on X1 searching, see Basic Search Commands and Advanced Search Command.	If you search for "quarterly financial records," your search results will include the searched phrase from all X1 email data sources.
From	Contains, Does Not Equal, Equals	When you use the Email From property in a query, the search returns all messages that contain the text in the Email From field.	If you search “@example.com,” your results include all messages sent by people with the @example.com in their email address.
Has Attachments	Equals	When you use the Has Attachments property, the search returns emails with or without attachments based on the Value setting.	If you mark toggle the Value setting On, your results include all messages that include an attachment.
Indexing Status	Contains, Does Not Equal, Equals	When you use the Indexing Status property in the query, the search returns all files that contains, equals, or does not equal one of the listed indexing statuses. The list of statuses are Starting, Indexing, Finished, Paused, Queued, Error, Cancelled. For more information on Indexing Statuses, see X1 documentation	If you search Does Not Equal "Error," your search results will include all files without the Error index status.
Received	Equals,	When you use the Email Received	If you search “Less Than 1/1/2020,” your res-

Criteria Field	Operators	Description	Example
Date	Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	Date property in a query, the search returns all messages that equal/-doesn't equal, greater/less than the date entered.	ults include all emails received before January 1, 2020.
Sent Date	Equals, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the email Sent Date property in a query, the search returns all messages that equal/doesn't equal, greater/less than the date entered.	If you search "Greater Than 1/1/2001," your results include all emails sent after January 1, 2001.
Subject	Contains, Does Not Equal, Equals	.When you use the Subject property, the search returns all messages that contains the search word or phrase in the email's title.	If you use the Subject property in a query, the search returns all messages which the subject line contains the text you're searching for. In other words, the query doesn't return only those messages that have an exact match. For example, if you search for subject "Quarterly Financials," your results include messages with the subject "Quarterly Financials 2018"
To	Contains, Does Not Equal, Equals	When you use the email To property in a query, the search returns all messages that contain the text in the Email To field.	If you search "@example.com," your results include all messages sent to people with the @example.com in their email address.

26.5.1.2 X1 files

The following table lists the filter criteria supported for X1 Files collections. Setting criteria for X1 files is not required.

Note: You must register Relativity in X1 before using this data source. For information on registering Relativity in X1, see X1's user documentation.

Criteria Field	Operators	Description	Example
Date Created	Equals, Greater Than, Greater Than or Equals, Less Than, Less Than or Equals	When you use the Creation Date property in a query, the search returns all messages that equal/doesn't equal, greater/less than the date entered.	If you search "Greater Than 1/1/2001," your results include all messages created after January 1, 2001.
Date Modified	Equals, Greater Than,	When you use the Modification Date property in a query, the search returns all updated files that equal/doesn't	If you search "Less Than 1/1/2020," your results

Criteria Field	Operators	Description	Example
	Greater Than or Equals, Less Than, Less Than or Equals	equal, greater/less than the date entered.	include all files modified before January 1, 2020.
Document Type	Contains, Does Not Equal, Equals	When you use the Document Type property in a query, the search returns all documents that contain, equal, or does not equal what you entered.	If you search "spread-sheet, your results include Excel files.
Extension	Contains, Does Not Equal, Equals	When you use the File Extension property in a query, the search returns all files that contain the entered file exten-sion.	If you search “Contains docx,” your results include all Microsoft Word files saved with that extension.
Free Form Search	Equals	Searches across all data sources simultaneously with general searching options. For more information on X1 searching, see Basic Search Commands and Advanced Search Command.	If you search for "quarterly financial records," your search results will include the searched phrase from all X1 file data sources.
Indexing Status	Contains, Does Not Equal, Equals	When you use the Indexing Status property in the query, the search returns all files that contains, equals, or does not equal one of the listed indexing statuses. The list of statuses are Starting, Indexing, Finished, Paused, Queued, Error, Cancelled. For more information on Index-ing Statuses, see X1 documentation.	If you search Does Not Equal "Error," your search results will include all files without the Error index status.
Name	Contains, Does Not Equal, Equals	When you use the File Name property in a query, the search returns all files that equals/does not equal or con-tain the value entered.	If you search “Equals Important_Document,” your results include all files with that text in the file-name.
Path	Contains, Does Not Equal, Equals	When you use the File Path property in a query, the search returns all messages equals/does not equal or contain the folder path entered.	If you search “Contains C:/-documents/Relativity,” your results include all files within the listed folder and any folder beyond the file path entered.

27 Collection

Before you begin collecting, you must create a collection job and associate it with a specific matter, custodians, and one or more data sources. Add the custodians, data sources, and other information using the Collect wizard. Once completed, start the collection using the Collect console. Finally, download a results report that details the items collected and a summary report of the entire collection job. For more information, see Reports on page 172.

27.1 Considerations

Before creating a collection for any data source, consider the factors that can affect collection performance.

- Collection time can increase when you use:
  - Large date ranges.
  - A high number of custodians.
  - Multiple collections running at the same time.
- Combining large scopes with high concurrency can slow down collections. This behavior is expected across all data sources.
- When you migrate a Collect workspace, data source credentials do not move with the workspace. You must re-enter credentials before running new Collect jobs. For more information, see Migrate.

27.2 Best practices for time-sensitive collections

To improve performance and reduce collection time:

- Use smaller date ranges whenever possible.
- Limit the number of custodians included in each collection.
- Reduce concurrency, or run collections sequentially when appropriate.
- Create multiple collection jobs when necessary.

Following these practices can help collections complete more quickly and predictably.

27.3 Creating a collection

Before you begin creating a collection, make sure to create a matter. For more information, see Matters on page 17.

Use the following procedure to create a collection:

1. On the Collect tab, click the **Collections** sub-tab. Collect displays a list of the collections currently added to this application.
2. Click **New Collection**.
3. Complete the steps in the Collect wizard. See Using the Collect wizard below
4. On the Collection Details page, click **Run Collection** in the console. See Collect console on page 165.

For information on running concurrent Microsoft 365 collection jobs, see Accessing Microsoft 365 tenants on page 98.

27.4 Using the Collect wizard

The Collect wizard takes you through each step to create a collection. After completing the collection setup, run a collection from the Collection console.

Collection wizard security permissions

- **Custodian**—View

When a step is complete, click **Next** or the hyperlink under the next step shown. Click the **Previous** button to move to the previous step. Relativity auto-saves your information when moving between steps. If any required information is wrong or missing, an error message displays and you cannot move to the next step.

27.4.1 Collection Details

Complete the Collection Details step by entering information in the following fields:

- **Name**—the name of the collection. Enter a name using alphanumeric characters only. You cannot use special characters, such as periods, commas, and em dashes. Special characters will cause an error.
- **Collection Matter**—the name of the matter associated with this collection. Click **Edit** to select an existing matter or click **Add** to define a new one. See Creating a matter on page 18.
- **Job Number**—lists a number assigned to the job for reporting purposes.
- **Processing Source Location**—the file repository for collected data to be stored for future processing of documents or for storing collected data. All data sources that produce RSMF have a limit of 2 GB. For more information, see Processing documentation.
- **ZIP Collected Files**—toggle on to compress all collected data into ZIP64 formatted containers. Relativity can compress Microsoft 365, Slack, and X1 data into zip folders.
    - Selecting *Yes* on the Collect Files in ZIP field adds your collected data into containers and puts it into a password protected compressed folder. The compressed folders separated by the custodian target collected. Each custodian target collect has its own folder. These folders will split when reaching a set size. The compressed folders are then stored in the processing staging area by default.
    - You can secure these compressed folders with a password. You can enter a password that you, or another user, needs to enter to open the compressed folder. Relativity stores these passwords in the password bank. You can retrieve them there at a later time.
    - To export your collected data, use the Staging Explorer.
    - Google compresses the data on their end and they exclude Google data from the ZIP64 formatted containers.
    - iManage does not support adding data to ZIP64 formatted containers.
- **Zip Password**—enter a password that is required by anyone attempting to decompress the ZIP64 container files.
    - If you have Processing installed in the workspace, Collect automatically populates the Processing Password Bank with the password so it is available at the time the collection is processed.
    - Click the Show Password box to display the actual password in the field to ensure the characters are correct.
    - Zip is supported by Microsoft 365, Slack, and X1. Google is exported as pre-zipped.
- **Enable Auto-Processing**—toggle on to enable auto-processing. If enabled, select the workspace, profile, and document prefix. Relativity processes all data in a completed collection, or completed with errors collection, after a collection finishes.
    - **Workspace**—select a workspace within your instance to use when creating a processing job.
    - **Processing Profile**—select a processing profile available in the drop-down menu. The available profiles are from the selected workspace.
    - **Document prefix** —select the document prefix option of *Use Entity Document Number Prefix* or *Use Processing Profile Document Number Prefix* to apply to each file in the processing set once it's published to a workspace.
- **Description**—enter a description of the collection used for reporting purposes.
- **Receive Progress Notifications**—toggle on to send or receive collection job status emails. The statuses include:
    - **Completed**—includes completed or completed with errors job status.
    - **Failed**—includes job status and reason for failure.

- **Notification Address**—enter the email address of person that wants to receive collection job statuses.
- **Data Source Type**—select one or more data sources to use in the collection. For more information, see Data source types on page 22.

27.4.2 Data source

Configure the data sources chosen in the Collection Details step. Each data source has different criteria to enter. See the list of data source types under Data sources on page 21 for information on each one.

You can select multiple data sources in the first step if you want to configure all or multiple sources in the step. Switch between each source to configure its criteria by using any of these methods:

- Click the name of the data source in the navigation menu.
- Click **Next** and **Previous** to move you through the data sources.
- Select individual data sources by clicking on the checkbox and then using the right arrows to select them.

27.4.2.1 Data source criteria

Add criteria to collect specific data. To configure the data sources, complete the following fields:

- **Select and unselected tabs**—choose the data sources to collect from by moving unselected data sources to the selected list.
- **Field**—choose the field to filter on within the data source.
- **Operator**—choose an operator such as equals, contains, greater than, or less than.
- **Value**—enter a value to find in the selected field.

After selecting field options, you must click **Add Criteria**. You can add multiple criteria to search data sources.

Note the following about criteria:

- Each criteria is then separated by an AND operator.
- Leave the data source criteria empty to collect all data from the sources.

27.4.3 Custodians

Complete the Custodians step by assigning custodians to the project. Follow the steps below to assign a custodian.

1. From the Unselected custodians table, use the column filters to locate custodians.
2. Select a checkbox next to a custodian.

Notes: If you select multiple Slack custodians in the same collection, the channels they share will only collect once.

- Collect supports up to 30 custodians, or entities, assigned in a collection job.
- If you need more than 30 custodians, you need to create another collection job.
- This limit only applies to the number of custodians.
- There is no limit to the number of targets to be collected.
- For example, you can select 30 custodians and three data sources for a total of 90 targets for the collection job.

3. Click the right arrow icon to add select custodians. Click double right arrow icon to add all custodians.
4. Click **Next**.

Note: There is a limit of 10,000 listed custodians with targets in the custodian picker.

27.4.4 Non-custodial

Note: This section only applies when SharePoint or Smarsh (Advanced Access) is selected as the data source.

Select non-custodial data sources to complete this step. Non-custodial data means you select the specific locations or archives you want to collect from. Selecting custodians is not required.

To select non-custodial data:

1. Click one or more data sources in the **Select Sources** column.
2. With one of the data sources highlighted, select the check boxes next to the sites you want to collect.
    1. **SharePoint**—you can collect from parent-level sites only. All sub-sites under a parent site are automatically collected.
    2. **Smarsh**—Smarsh organizes data into cases. Select the cases you want to collect from. Collect only supports collection jobs of one case for Smarsh.
3. (Optional) Toggle on the **Show selected only** option to display only the locations selected for collection. The selected locations display in a concise list for review before you proceed to the Summary step.
4. Click **Next**.

27.4.5 Collection Summary

Complete the creation of the collection by reviewing all steps, custodians, data sources, and targets, before finalizing.

If Google Workspace Microsoft 365 Slack X1 custodian targets were not created before you started the project, click **Generate Targets**.

Click **Generate Targets** to check if targets exist for the custodians you have selected for collection. If the targets do not exist, Collect automatically creates them based on the email address contained in the Entity record for each custodian.

27.4.5.1 Targets

In the Targets section, a number appears next to each custodian's name. The number listed is the number of custodian targets found in the associated data source.

Number	Meaning
0	Collect did not find any custodian targets with that email address in that data source.
1	Collect found a single custodian target associated with the email address within the data source.
2+	Collect found multiple custodian targets with that email address within the data source.

The number is also color-coded to indicate how the target was generated:

- **No highlight**—Collect already found and generated the custodian target.
- **Green**—Collect autogenerated the custodian target.

- **Red**—Collect could not autogenerate the custodian target.
  - You can still manually generate it.
  - For more information, see Creating a custodian target on page 20.

Click **View Collection Details** to finish setup. The Collection Details page appears. From the Collection Details page, you can preview and run the collection from the Collection Summary on the previous page.

27.4.5.2 Non-custodian targets

Note: This section only applies when SharePoint is selected as the data source.

The *Non-Custodian Targets* section displays the target, target identifier, and the status.

- **Target**—the name you gave when creating the data source.
- **Target Identifier**—the URL of the SharePoint site.
- **Status**—a message telling you if the target is valid or invalid. If invalid, navigate to the data source details page and click the **Refresh Sites** button.

28 Viewing or editing Collection data

You can view and edit collection details. You can also use the Collect console to start and stop collections and view reports.

28.1 Collection details

You can display the collection details by clicking the name of a collection on the Collections tab. Collection also displays these details immediately after you add a new collection.

On the Collection Details page, use the buttons at the top of the page to edit, delete, go back, edit permissions, or perform other collection tasks. Editing a collection takes you to the first step in the wizard. For more information, see Using the Collect wizard on page 159.

Note: Once a collection has started, the collection details are read-only and cannot be changed.

- **Collection Details**—displays the information that you entered or selected when you created the collection:
  - **Name**—lists the name given to the collection.
  - **Collection Matter**—the matter used in the collection.
  - **Job Number**—the number assigned to the job for reporting purposes.
  - **Description**—the description of the collection used for reporting purposes.
  - **Processing Source Location**—the file repository that collected data is stored for future processing of documents or for storing collected data.
  - **Auto Processing Workspace**—the processing workspace if you toggled the field on.
  - **Auto Processing Profile**—the processing profile if you toggled the field on.
  - **Auto Processing Document Numbering Prefix Option**—the prefix option if you selected one.
  - **Job Status**—status of the collection. Statuses are New, Not Started, Started, Completed, Error, and Completed with Errors.
  - **Error Message**—the message if collection job did not complete due to errors.

- **Zip Collected Files**—if you selected to zip collected files this box is checked.
- **Zip Password**—the password that everyone needs to use to decompress the ZIP64 container files.
- **Receive Email Notifications**—if you toggled on to send or receive collection job status emails this checkbox is checked.
- **Notification Address**—the email address of the person that will receive collection job statuses.

- **Collection Console**—displays buttons that you can use to perform the tasks listed. See Collect console on the next page.
- **Data Sources**—lists all the collection activities associated with this collection.
  - **Custodian**—the custodian associated with the collection.
  - **Source Instance**—the name of the data source associated with the collection.
  - **Data Type Name**—the name of the target associated with the collection.
  - **Status**—displays one of the following statuses:
    - **Not Started**—the collection has not been started.
    - **Started**—the collection is in progress.
    - **Completed**—the collection is done.
    - **Completed with Errors**—the collection of the target completed and one or more targets had errors. For more information, see the Errors report on page 173.
    - **Failed**—the collection failed. For more information, see Graph Error Codes on page 173.
  - **Error**—lists the error message if the status is Failed.
  - **Collected Items**—the number of files collected from the target without error. If nothing is collected, a 0 is listed.
  - **Collected Item Total**—the number of files that there are to collect without errors. If nothing is collected, a 0 is listed.
  - **Target**—the custodian target associated with the data source.
  - **Result Link**—a Comma Separated Values file download listing all individual items collected from the target. It contains all the associated metadata for each collected item as well. If no results, the file is empty. For more information, see Viewing or editing Collection data on the previous page.

    Note: Google Workspace results download as a .xml file that you can convert into a .csv file using a third-party tool.

  - **Error Link**—a Comma Separated Values file download listing any individual items that couldn't be collected because of errors during the collection. The report provides as much metadata as it can along with as much error information as we can get from the source to help identify what caused the error. If no errors, the file is empty. For more information on errors, see the Errors report on page 173.

    Note: Google Workspace results download as a .xml file that you can convert into a .csv file using a third-party tool.

- **Previews**—the status and estimated number of items and size of collection. This is available after starting a preview. For more information, see Preview on the next page.

- **Custodian Details**—the status of the custodian and the source instance. This card also includes the filter criteria, items, size, and errors.

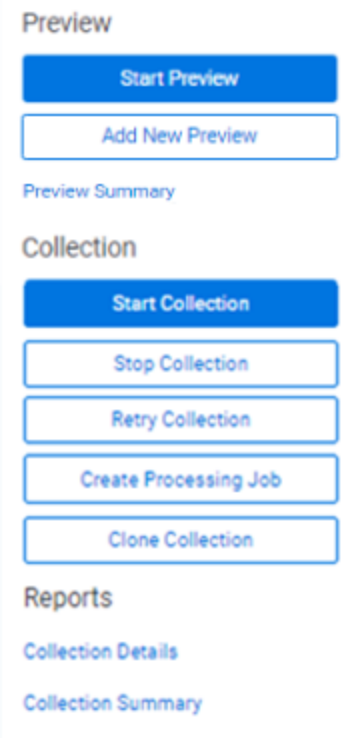
28.2 Viewing collected data

When Relativity collects the data, Relativity accepts the path names and file names that the source provides. On occasion, the collection source modifies the path name or file name.

There is a difference between viewing grouped and individual collections data. To view grouped collections data, for sources like Bloomberg Chat, Google Chat, Slack, and Teams, click the **Get Results** link to view your collection data. Although the Data Sources table will show N/A in the Collected Items and Collected Item Total columns, the collected data is still available in the download. These columns show N/A because more than one set of custodian data is included in the collection.

28.3 Collect console

After completing a setup, run the collection with the collection console. Verify connection, start or stop a collection, and view a collection report from the Collection console on the Collection Details page.



28.3.1 Preview

After setting up your collection job, you can preview the job. This is an inventory phase without running a full collection. You can see the estimated number of discovered items and collection size for each custodian target. These preview options help you decide to move forward or adjust your collection job.

Notes: Only available for Microsoft 365 Outlook mailboxes, calendars, contacts, and OneDrive. For more information, see Microsoft 365 - Outlook data source on page 105 and Microsoft 365 - OneDrive data source on page 97. Inactive mailboxes are not included in preview.

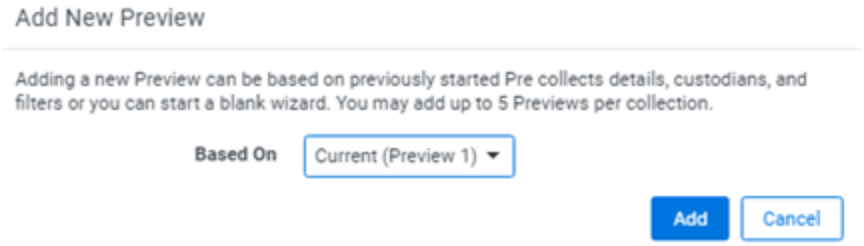
28.3.1.1 Start Preview

Click the **Start Preview** button to gain insight into the number of items and size of the collection as the collection is currently set up.

From here, you can start your collection or add a new preview.

28.3.1.2 Add New Preview

Click the **Add New Preview** button to adjust your collection job setup. In the Add New Preview modal, you can add a new preview based on previously started collect details or a blank wizard. You can add up to five previews.



Selecting the **Blank Wizard** option takes you back to the Collection Details step. You then need to complete the collection wizard with a new setup.

From here, you can start your collection.

28.3.2 Collection

Once you decide to move forward with your collection, you will use this section of the console to start, stop, and adjust your collection job.

28.3.2.1 Start Collection

Click the **Start Collection** button the begin the collect project.

28.3.2.2 Stop Collection

Click **Stop Collection** to end the collection project that is currently running. Once you click this button, a warning pop-up message appears to confirm that you want to stop. Once you stop a collection, the collection cannot be restarted.

28.3.2.3 Retry Collection

The Retry Collection button is only available when a collect job does not complete because of errors. Click **Retry Collection** to start another collect job that only retries the targets that have failed. You cannot retry targets that completed successfully.

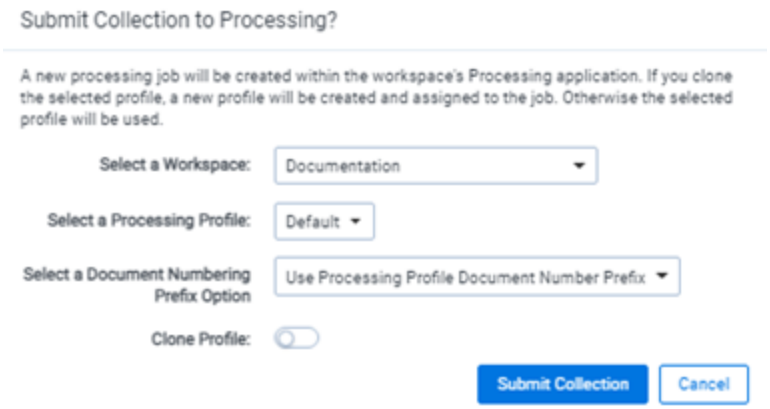
28.3.2.4 Create Processing Job

Click **Create Processing Job** to create a processing set from the collected documents from the data sources. Locate these documents in the Processing Source Location set in Collection Details.

When you click the Create Processing Job button, a pop-up window displays with two fields:

- **Select a workspace**—select a workspace within your instance to select a Processing profile to use when creating a processing job.
- **Select a Processing Profile**—select a processing profile available in the drop-down menu. The available profiles are from the selected workspace.
- **Select a Document Numbering Prefix Option**—select *Use Processing Profile Document Number Prefix* or *Use Processing Profile Document Number Prefix* to apply to each file in the processing set once it is published to a workspace.

- **Clone Profile**—toggle off to use the selected processing profile. Toggle on to clone the selected processing profile and use the clone profile in conjunction with the created processing set.



After selecting a processing profile and deciding on cloning the profile, click the **Submit Collection** button. Once you submit the collection, Relativity creates a processing set with the same name as the collection job. The processing set includes all data that was collected in the collection job.

28.3.2.5 Clone Collection

Click **Clone Collection** to duplicate the open collect job. You can clone any collect job that has a status other than New.

After clicking the Clone Collection button, a pop-up modal displays the progress and completion of the clone.

Once the job is cloned, it is placed in the Not Started status and you can find it in the Collections list under the same name with "Cloned - YYYY-MM-DD HH.MM.SS" amended to the end. All collection totals for the cloned job associated targets are reset to zero. The Collection Detail Custodian Target fields are reset to zero. The cloned collect job also generates the new targets.

28.3.2.6 Reports

Collect includes comprehensive reporting capabilities that you can use to view information about your collections. You can generate these reports in the collection console within a collection project. Click on the name of a report to download. When generating a report, Relativity downloads different files through your browser. For more information on specific reports, see Reports on page 172.

28.4 Delete collections

A collection will not delete if they have an existing custodian tied to it.

When you delete a collect job, Relativity deletes all of the related custodian targets for the job. The custodian targets table remain the same. The targets within Custodian Targets are not related to any specific collect jobs. Relativity creates job-specific copies of the custodian targets for the job when it's created.

29 Grouped collections

A grouped collection means that all conversations for the selected custodians are combined into a single set of RSMF output files.

This approach is used to:

- Minimize collection size
- Prevent duplicate conversations

If each custodian were collected separately, any shared conversations, such as direct messages, group chats, or shared channel content, would be collected multiple times. This would:

- Increase the overall data volume
- Expand storage requirements
- Require additional downstream deduplication effort during processing and review

29.1 Grouped data sources

Within Collect, there are short message data sources that Relativity collects in a grouped format when more than one custodian is selected.

Grouped collection data sources:

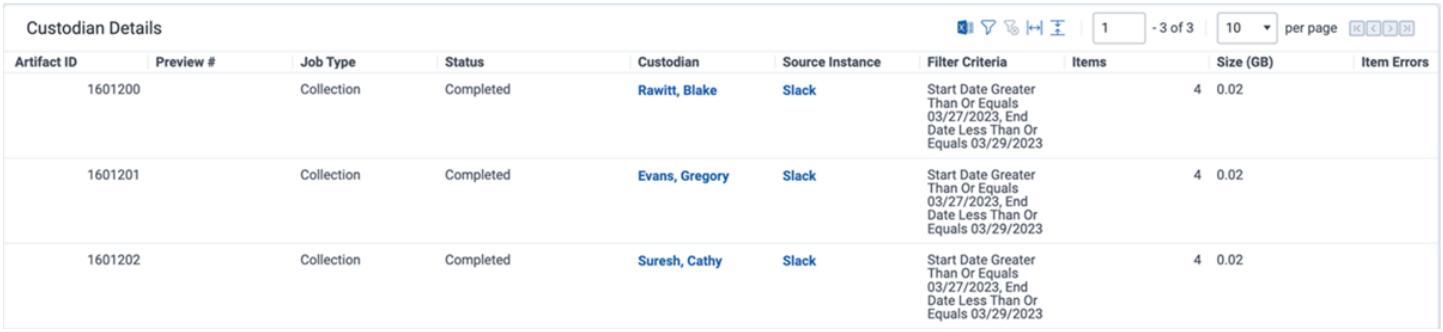
- Microsoft 365 Teams
- Slack
- Google Chat

29.2 Grouping messages

Grouping ensures that shared content is collected once. This helps reduce duplicates and keeps the dataset consistent.

When viewing grouped collection results on the Collect job details page, the reported artifacts collected and collection size show the same value for all involved custodians. This reflects that there is one collection of RSMFs containing all chats for the collected custodians.

The reported *Items* collected is the number of RSMF files that were generated during the collection. We currently do not support reporting the number of individual messages attributable to each custodian independently. The reported *Size (GB)* represents the aggregate size of all generated RSMF files.



Custodian Details

1 - 3 of 3 | 10 per page

Artifact ID	Preview #	Job Type	Status	Custodian	Source Instance	Filter Criteria	Items	Size (GB)	Item Errors
1601200		Collection	Completed	Rawitt, Blake	Slack	Start Date Greater Than Or Equals 03/27/2023, End Date Less Than Or Equals 03/29/2023	4	0.02	
1601201		Collection	Completed	Evans, Gregory	Slack	Start Date Greater Than Or Equals 03/27/2023, End Date Less Than Or Equals 03/29/2023	4	0.02	
1601202		Collection	Completed	Suresh, Cathy	Slack	Start Date Greater Than Or Equals 03/27/2023, End Date Less Than Or Equals 03/29/2023	4	0.02	

29.3 Custodian assignment considerations

Grouped collections create a limitation during processing because the Processing capability supports only one custodian per processing set data source.

Relativity assigns an Entity representing the data source as the custodian for the processing set when using *auto-processing* or the *Create Processing Job (on-demand)* feature in Collect.

This prevents the system from applying a single custodian to the entire RSMF dataset, which would incorrectly suggest all messages belong to one person.

29.4 Manual processing guidance

When manually creating a processing set, you encounter the same limitation of needing to assign a single custodian to the grouped RSMF data.

Recommended approach:

- Create or use an Entity of type *Other*
- Name the Entity to clearly represent the data set

Example: *Slack – Acme Matter – 2026-02-10*

This approach accurately reflects that the data set represents multiple custodians and maintains consistency with Collect's automated processing behavior.

30 Migrate Collect workspaces

When you migrate a Collect workspace, using *Archive, Restore, and Migrate (ARM)* or *Integration Points*, Relativity moves workspace data but does not move data source credentials.

After the migration, you must re-enter credentials before you can run Collect jobs.

Note: This behavior applies to all Collect data sources.

30.1 Migrate Collect workspaces

You can migrate Collect workspaces using ARM or Integration Points.

During a migration:

- Relativity restores the Collect workspace and its objects.
- Relativity does not restore data source credentials.
- Data sources appear in the restored workspace but are not connected.

Relativity does not provide a supported way to move or copy Collect credentials. This protects sensitive authentication information.

30.2 Credentials do not migrate

To protect from compromising sensitive authentication information, Relativity does not support moving or copying Collect credentials from migration.

30.3 After migration

Until you re-enter credentials, Collect cannot access the data sources.

After a migration:

- Data sources appear in the restored workspace.
  - The credentials will not work.
  - The connections are invalidated.
- You must re-enter the credentials for each data source and revalidate each data source.
- New collection jobs cannot be run until the data sources are connected again.

Note: You do not need to remake the credentials for the data sources. If the existing credentials are still valid you need to re-input.

30.3.1 Considerations

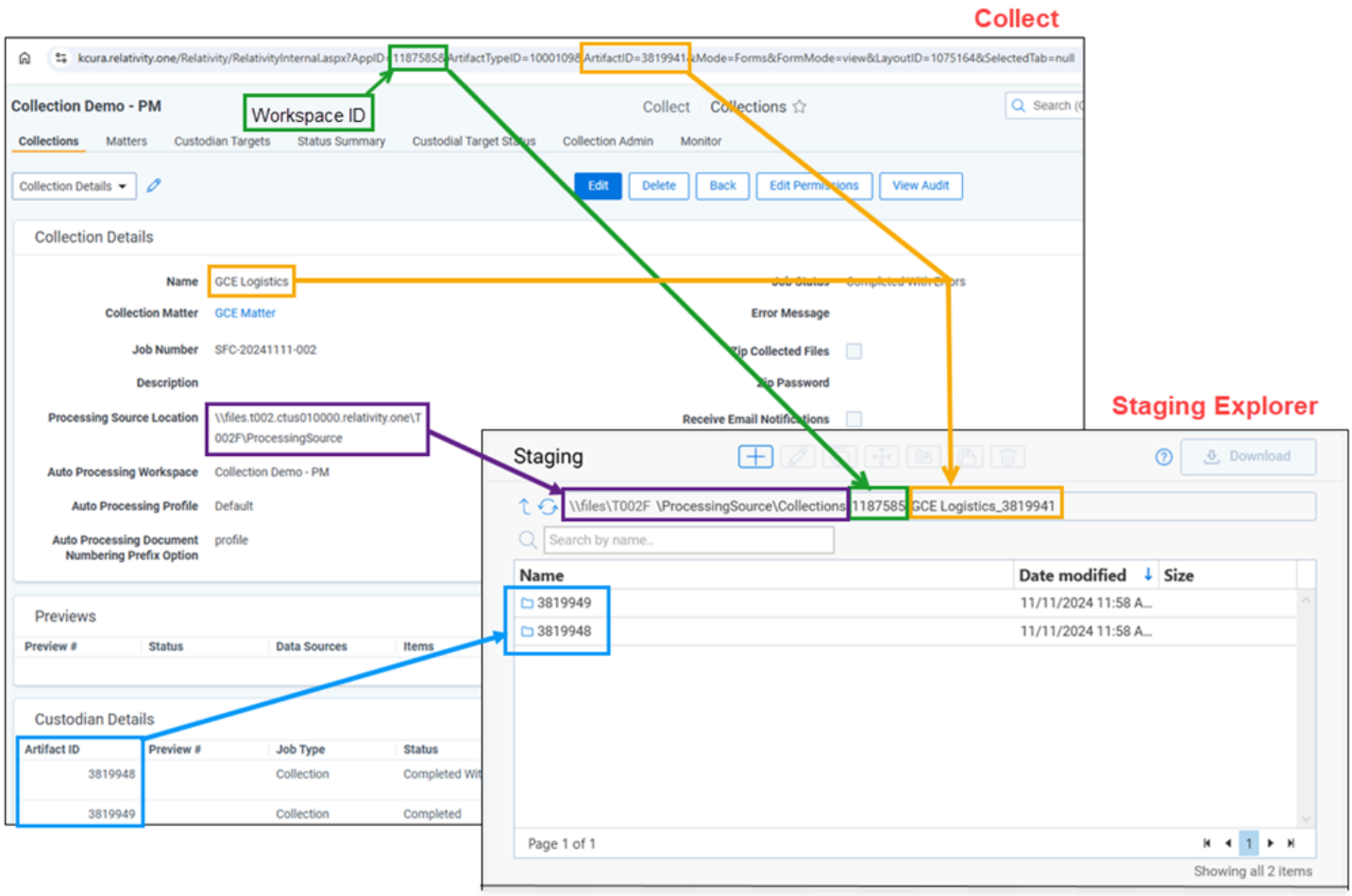
Consider the following when using Microsoft or Google:

- **Microsoft 365**—the app created for Microsoft 365 data sources has a secret value which is only exposed on initial creation.
    - This secret value must be stored and re-entered correctly for the data source to work.
    - If the Secret Value is forgotten, please generate a new secret value.
- **Google**—for Google data sources, a refresh token is generated on the first Google data source that was set-up and used for subsequent Google data sources.
    - This refresh token value must be stored and re-entered in the data sources in order for the data sources to work.
    - If the token is invalidated or forgotten, please see Troubleshooting for instruction on generating a new refresh token.

31 Identifying Collection data in Staging Explorer

This section helps to identify the components of the folder information within the Staging pane of the Staging Explorer as it relates to the Collections setup fields.

Use the sample screen below as a general guide for each data source type.



Here is a breakdown of the folder components within the Staging pane of the Staging Explorer:

\\files\<T####>\ProcessingSource\Collections\<WorkspaceID>\<CollectionName>_<CollectionArtifactID>\<DataSourceArtifactID>

- The Processing Source Location from the Collections page becomes the file location for the data in Staging Explorer. It contains a sub-folder for Collections to house the Collection data. Using the above example, it would be:

  \\files\T002F\ProcessingSource\Collections

- The Workspace ID folder in the Staging pane corresponds to the Workspace ID number listed after the "AppID=" in the URL. For example, 1187585 would be the Workspace ID from this URL: kcur-a.relativity.one/Relativity/RelativityInternal.aspx?AppID=**1187585**...

  \\files\T002F\ProcessingSource\Collections\1187585

- The Name of the Collection from the Collections page and the Collection Artifact ID become the folder name within the Workspace ID folder. Using the above example, it would be:

  \\files\T002F\ProcessingSource\Collections\1187585\GCE Logistics_3819941

- The Artifact ID of the data source used becomes the sub-folder. Using the above example, they would be:

\\files\T002F\ProcessingSource\Collections\1187585\GCE Logistics_3819941\3819948
\\files\T002F\ProcessingSource\Collections\1187585\GCE Logistics_3819941\3819949

In the case of grouped collections, such as Teams and Slack, there will be a folder within the collection folder corresponding to the data source type. Using Teams as an example, the file structure would be:

\\files\T002F\ProcessingSource\Collections\1187585\GCE Logistics_3819941\Teams

32 Reports

Collect offers comprehensive reporting capabilities that you can use to view information about collections. You can set options to generate these reports based on matter and collection as well as other combinations.

32.1 Running reports

You can generate these reports in the collection console within a collection project. Click on the name of a report to download. Locate the Collection Summary and Collection Details report in the collection console. Locate the Results and Error report in the Data Sources table on the Collection Details page.

When generating a report, Relativity downloads different files through your browser.

Note: All report timestamps are in UTC.

32.1.1 Collection Summary report

The Collection Summary report includes the target, target status, number of items collected, and the collection size. The report is grouped by custodians. Grouping by custodians makes it easy to sort the targets for each custodian with subtotals for each custodian. Grand totals are at the end of the report. The report downloads as a PDF file.

This report also includes filters that were used at any point in the collection. For example, if a modification date that is greater than or equal to 1/1/2010 is added at the criteria level, then that filter is listed in the summary report table. If no filter criteria was specified for the job, the report lists a "No Filter Criteria Applied" message.

Group-type data sources are also included in the list of data sources. This section is at the beginning of the report. For example, if you collect from Outlook calendars, Outlook mailboxes, and Slack, all collection summaries are included in the report.

The short message grouped collections lists the custodians involved in the collect, along with the data sources. The top of the report includes the custodian list. This section's title is "Short Message Grouped Collections." The report table includes the data source, target status, the number of items collected, and the collection size in gigabytes.

32.1.2 Collection Details report

The Collection Details report includes two files: the first file includes the successfully collected results of all items and their metadata. The second file includes the errored collection data. The error file includes as many of the items and as much of the items' metadata as it can. The report downloads as a CSV file.

This report, both files, is also stored in the assigned Entra ID file share. It is included in the collection output.

32.1.3 Results report

The Results report link for each target downloads as a CSV or XML file that contains a list of all individual items collected. These items include emails, files, or other data. It contains all of the associated metadata for each item. If no items were collected the file is empty.

The Results report is a CSV file download of the results collected from Bloomberg, Box, iManage, Microsoft, Refinitiv Ikon, Slack, or X1 targets.

The Results report is an XML file download of the results collected from a Google target.

32.1.3.1 Hash identifier - SHA-256

Inside the spreadsheet there is an electronic fingerprint named SHA-256. When collecting documents, Microsoft adds the SHA-256 hash identifiers and then stores the hashes. A user can verify the original file by matching the SHA-256 identifiers. For more information, see Microsoft's Retention Policies.

The SHA-256 is included in the Results report file and the Collection details report files.

32.1.4 Errors report

A Comma Separated Values file download of the errors that occurred during the collection from the target. If no errors occurred, the file is empty.

If the application is reporting errors with requests, creating objects, or parsing, check for correct permissions, check for healthy connections, and check if the fileshare is working. If the setup is correct, start diagnosing errors.

32.1.4.1 Errors.csv

The report file lists one error per line. Each item is listed with an error ID alongside the message of the error that caused the item failure. Per-item errors only occur in the download phase of the collection; if an error occurs before (for example, if data is unavailable during our check) or after (for example, the worker cannot write the results.csv file to the fileshare) then there will be no record in the errors.csv report.

32.1.4.2 Graph Error Codes

The Graph Error Codes category of error codes will occur if there is an issue with Graph when downloading an item. For more information, see Microsoft's Graph Errors documentation. There are different error categories. Handle each category error following instructions below. If the suggested resolutions don't fix the issue or if the code is not listed, contact Relativity Support.

Transient

Transient errors appear in the report if the Microsoft Graph API has received too many requests in too short a time. If these errors appear, then the collection is putting too much pressure on external services. Retry the collection later.

- activityLimitReached
- quotaLimitReached
- serviceNotAvailable

Authentication

These errors deal with authentication of the Collect application. Check the Microsoft Azure application associated with the collection source instance and ensure it has the proper permissions.

- accessDenied
- notAllowed
- unauthenticated

For more information, see Accessing Microsoft 365 tenants on page 98.

Modification

Modification errors appear when data changes between discovery and download. For example, moving data would cause a modification error. Restart the collection to resolve the error.

- itemNotFound
- resourceModified

File

The Microsoft Graph API prevents Relativity from collecting items marked as malware. Items marked as malware will always error. Relativity doesn't collect these files. To download these items, you must download them manually.

- malwareDetected

The other error codes shouldn't appear in Errors file, as they either deal with the uploading of data (which Collect doesn't do) or they deal with a malformed request, which indicates a bug. If they appear, contact Relativity Support.

HTTP Errors

This error category occurs alongside Graph errors, as well as in a few other cases. For example, an HTTP error occurs when a file stream doesn't download. If the suggested resolution does not fix the issue or if the code is not listed, contact Relativity Support.

Of the HTTP error codes, here are examples of some that may appear:

- **400: Bad Request**—the application requested a resource improperly. If this occurs, contact Relativity Support.
- **401: Unauthorized**—the application doesn't have the proper permissions and the app key is correct.
- **403: Forbidden**—the application doesn't have the permissions and the app key is correct. These may also be associated with attempting to download a file with malware (see malwareDetected).
- **404: Not Found**—an item was moved between discovery and downloading. Restart the collection.
- **429: Too Many Requests**— the application has received more requests than it can handle. Retry the collection later.
- **504: Gateway Timeout**—this is related to the stability of the tenant being collected from. Retry the collection again later.
- **509: Bandwidth Limit Exceeded**—the application cannot support the amount of bandwidth needed. Retry the collection again later.

Other Errors

InvalidOperationException ("The item's downloaded hash does not match Microsoft's reported hash value.") – this occurs if the downloaded item's hash identifier and Microsoft's hash identifier differs. This error usually indicates something happened with the download that caused the data to become corrupted and can represent a transient error. Retry running the collection.

ArgumentExceptions ("Non-file attached to...") - these exceptions occur when something other than a file is attached to an event or message. Relativity does not collect these items.

There are messages indicating that there was an issue creating a VCard, MIME, or iCal object. These indicate that there was an error translating Microsoft's response on these items into files, and are usually bugs in the Collection application. contact Relativity Support.

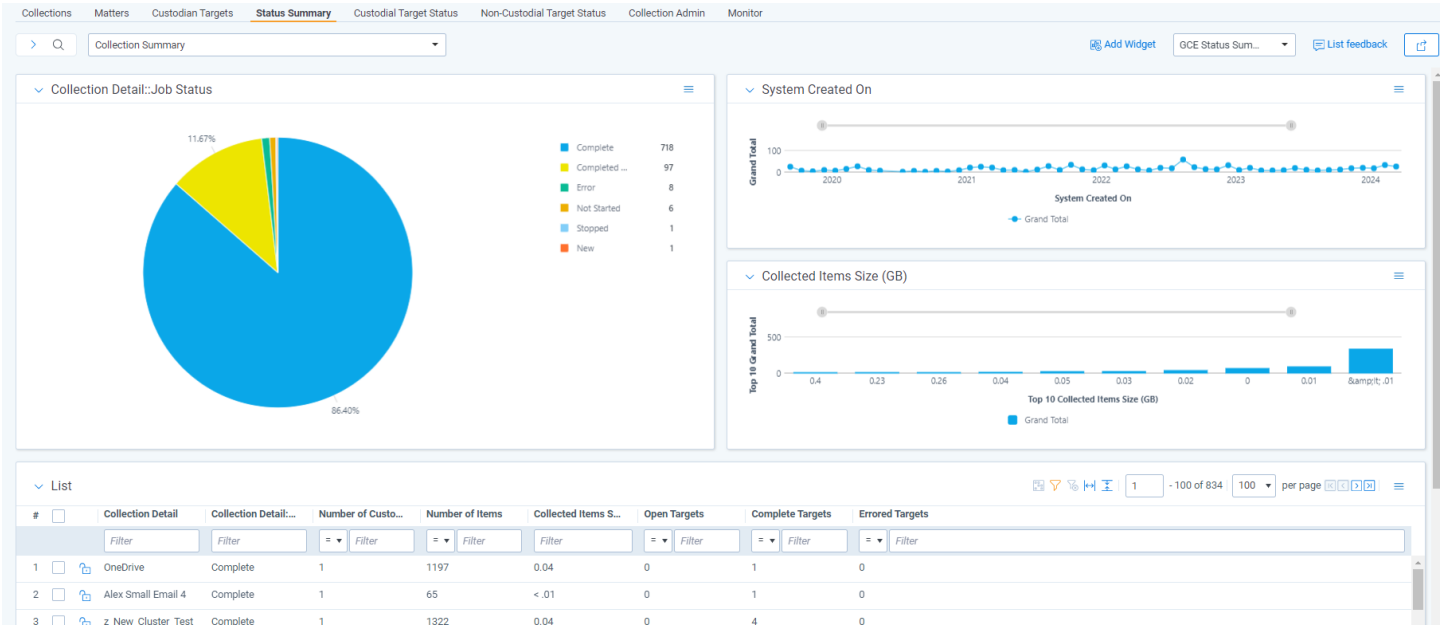
There are messages indicating problems writing files to the file share. In this case, download went correctly, but there is an issue with the Relativity File Share preventing the write. contact Relativity Support.

33 Status Summary

In Collect, you manage multiple collect jobs and you need to track all of them.

33.1 Job status

The job status dashboard to see the statuses of collection jobs. You can drill into each job from this dashboard. Able to look into the targets by custodian, data sources, or status to find out more about your collections. Focus on the collected components with this dashboard.



33.2 Reviewing job statuses

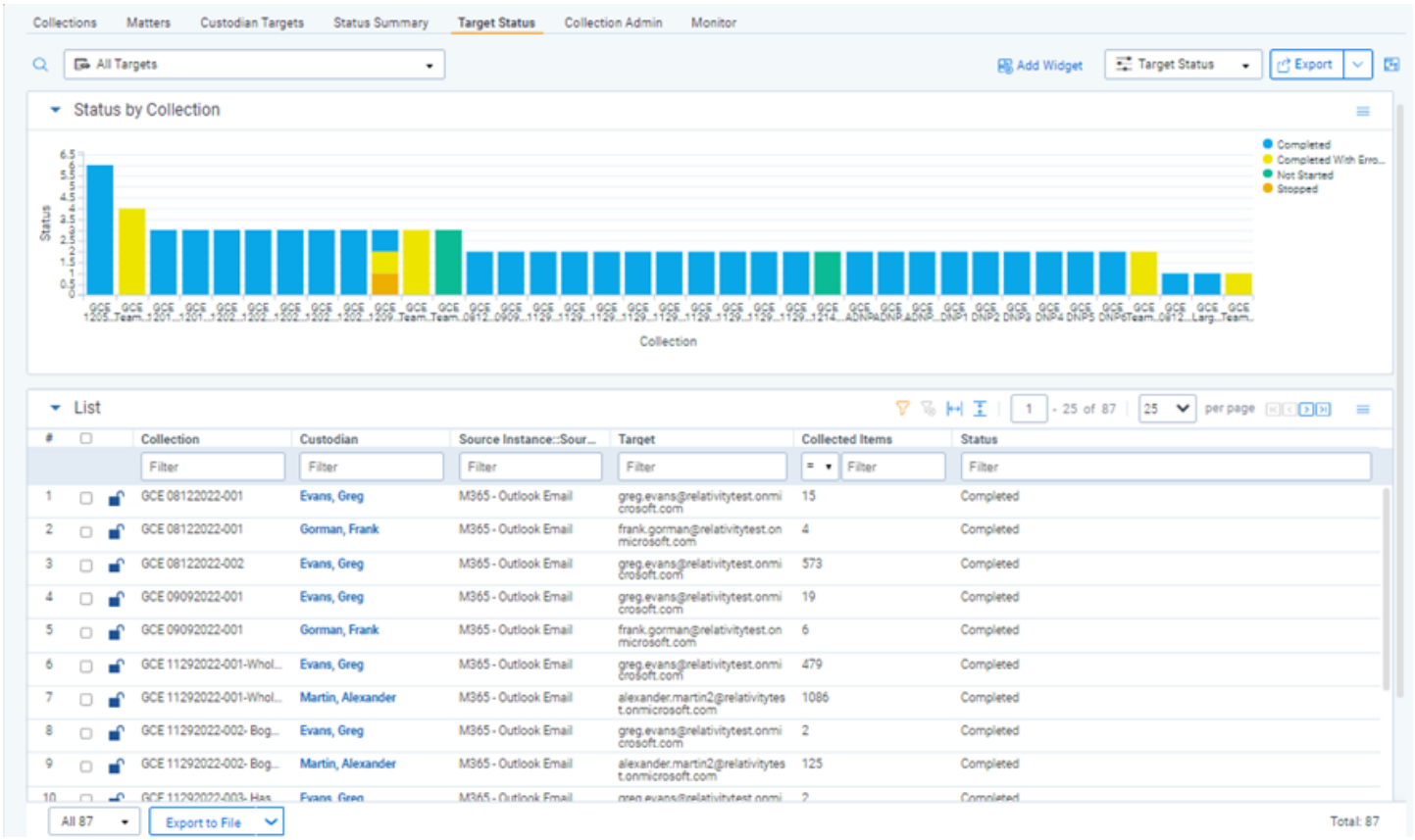
The job status dashboard is available after generating targets. To learn how to generate targets for a collection, see Collection Summary on page 162. Once you generate targets, the dashboard organizes by collection jobs.

Status:

- **Not started**—the collection is set up, but hasn't been started.
- **Started**—the collection started and has not completed.
- **Completed**—the collection of the target completed without any errors.
- **Completed with Errors**—the collection of the target completed and had individual items that couldn't be collected. For more information, see the Errors report on page 173.
- **Error**—the collection did not run successfully and couldn't collect from the target.

34 Target Status

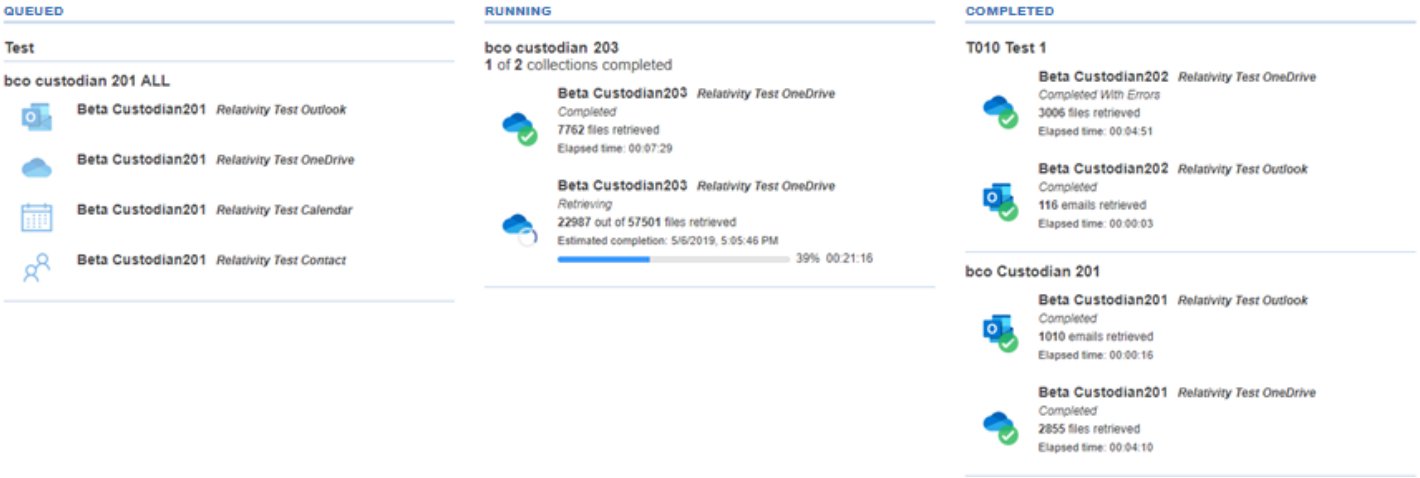
The Target Status tab is a dashboard to see the statuses of collections. You can drill into each target from this dashboard. Able to look into the targets by custodian, data sources, or status to find out more about your collections. Focus on the collected components with this dashboard.

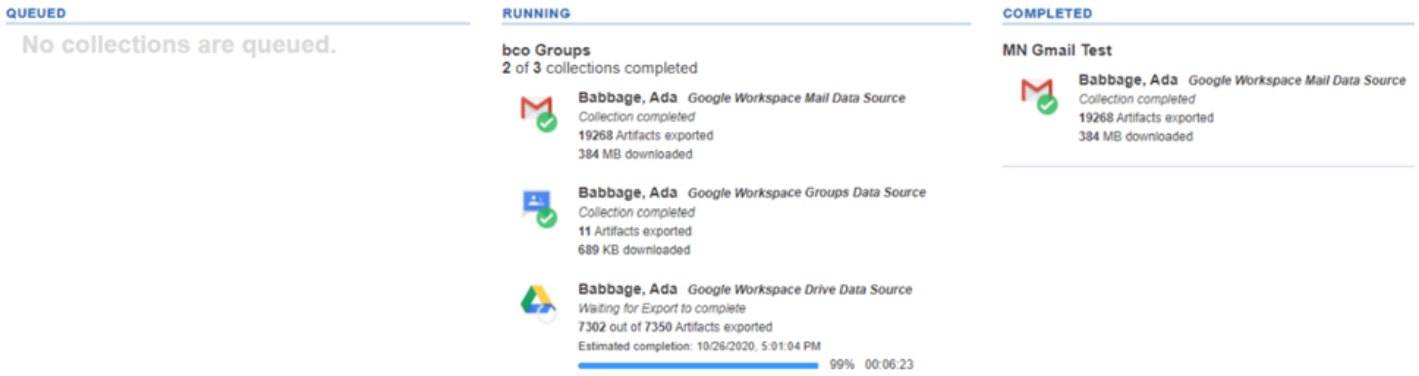


35 Monitor

Monitor pending, running, and completed collect jobs in the Monitor tab. The Monitor page only tracks collect jobs from the last 24-hour time range.

- **Queued**—this column lists the created collect jobs that have not started.
- **Running**—this column lists collect jobs in progress and with their current progress displayed in a status bar.
- **Completed**—this column lists collect jobs completed successfully, completed with errors, the amount of data collected, and the elapsed time.




QUEUED
No collections are queued.
RUNNING
bco Groups
2 of 3 collections completed
Babbage, Ada Google Workspace Mail Data Source
Collection completed
19268 Artifacts exported
384 MB downloaded
Babbage, Ada Google Workspace Groups Data Source
Collection completed
11 Artifacts exported
689 KB downloaded
Babbage, Ada Google Workspace Drive Data Source
Waiting for Export to complete
7302 out of 7350 Artifacts exported
Estimated completion: 10/26/2020, 5:01:04 PM
99% 00:06:23
COMPLETED
MN Gmail Test
Babbage, Ada Google Workspace Mail Data Source
Collection completed
19268 Artifacts exported
384 MB downloaded

Proprietary Rights

This documentation ("**Documentation**") and the software to which it relates ("**Software**") belongs to Relativity ODA LLC and/or Relativity's third party software vendors. Relativity grants written license agreements which contain restrictions. All parties accessing the Documentation or Software must: respect proprietary rights of Relativity and third parties; comply with your organization's license agreement, including but not limited to license restrictions on use, copying, modifications, reverse engineering, and derivative products; and refrain from any misuse or misappropriation of this Documentation or Software in whole or in part. The Software and Documentation is protected by the **Copyright Act of 1976**, as amended, and the Software code is protected by the **Illinois Trade Secrets Act**. Violations can involve substantial civil liabilities, exemplary damages, and criminal penalties, including fines and possible imprisonment.

©2026. Relativity ODA LLC. All rights reserved. Relativity® is a registered trademark of Relativity ODA LLC.

36 Index

A

Azure Application Registration Secret Expires 74, 82, 91, 99, 109, 128, 137

Azure Client secret expired 74, 82, 91, 99, 109, 128, 137

C

Collect 158, 172

Collect wizard 159