Connect Code42 to OneDrive

Updated 5 months ago

Overview

To help protect you from data loss, you can use Code42 to monitor files moving to and from users' Microsoft OneDrive for Business.

When you add Microsoft OneDrive for Business as a data connection, you must authorize Code42 using your global administrator account in OneDrive for Business. Once connected, we monitor your organization's OneDrive environment to capture when a user:

- Creates or uploads a file
- Shares a link to a file
- Shares a file directly with users inside or outside your organization
- Deletes a file
- Modifies a file's contents, name, or location

This article explains how to add OneDrive as a data connection.

Considerations

The following considerations apply to OneDrive. See also the considerations applicable to all cloud storage environments.

- Code42 requires a Microsoft license or subscription that includes Audit (Standard) in order to monitor file activity in your OneDrive environment.
- Audit must be turned on in your OneDrive environment.
- Code42 attempts to use the **UserPrincipalName** in OneDrive when displaying user information in Forensic Search. If this attribute in Azure is not an email address, trusted domains do not work as expected.
- Microsoft OneDrive limits API requests made by third-party integrations such as Code42. Throttling these API requests allows Microsoft to better control their resources, but may slow down Code42 file metadata collection, especially after first configuring access to OneDrive. Consider allowing access to OneDrive when you have decreased activity in your environment.
- Because Code42 prioritizes file-based monitoring, detection of sharing permissions changes to folders in OneDrive may be delayed.

> **Monitoring and alerting tools may report download activity**
> When ongoing file activity is detected, Code42 temporarily streams files from your cloud storage or email service to the Code42 cloud to calculate the file hash. (Code42 does not calculate hash value during the initial inventory process.)
>
> This appears in your vendor logs as users downloading files. The requesting service's IP address may point to Microsoft Azure hosts. Consider adding these IP addresses to your allowlist to reduce false alerts in your vendor logs, keeping in mind that these addresses can change.
>
> Code42 never stores file contents or writes them to disk during this process.

> **A single file event in Forensic Search may represent more than one action in cloud storage**
> There's not always a strict one-to-one relationship between the actions a user takes on a file in your corporate cloud storage environment and the file event representing those actions in Code42. After detecting activity, Code42 makes a best effort to interpret the user's actions on a file in cloud storage. Code42 may combine several of those actions into one file event to more efficiently and effectively display those details. For example, a user modifying a file repeatedly a few seconds apart in the cloud storage environment may appear as one "file modified" event in Forensic Search.
> Throttling of API requests by the cloud storage vendor can also slow Code42's metadata collection and affect how file events are displayed in Forensic Search. Both this throttling and Code42's interpretation of actions can cause multiple actions in cloud storage to be displayed in fewer events in Forensic Search.

Before you begin

Before you authorize the Code42 connection to your OneDrive environment, follow the directions in Configure Microsoft for the Code42 OneDrive data connection to properly set up your OneDrive environment to allow Code42 to collect data.

Authorize Code42's connection to OneDrive

1. Sign in to the Code42 console.
2. Select **Administration > Integrations > Data Connections**.

Support

3. Click **Add data connection**.
   *The **Add data connection** panel opens.*
4. From **Data connection**, select **Microsoft OneDrive for Business** under **Cloud storage**.
5. Enter a **Display name**. This name must be unique.
6. Code42 prompts you to verify that auditing is turned on in your Microsoft environment. You completed this verification when you configured your Microsoft environment in preparation for the connection, so select the **I've completed these steps** check box and then click **Continue**.
7. Select the scope of users in your OneDrive environment to monitor:
   - **All**: Monitors all OneDrive users in your environment.
   - **Specific users**: Monitors only the OneDrive users you designate.
     1. Click **Upload .CSV file**.
     2. Select the scoping CSV file that contains a list of only those users you want to monitor.
   - **Specific groups**: Monitors only the users in the OneDrive groups you designate.
     1. Click **Upload .CSV file**.
     2. Select the scoping CSV file that contains a list of only those groups in OneDrive whose users you want to monitor.
8. Click **Authorize**.
   The Microsoft OneDrive for Business sign in screen appears.
9. Enter your OneDrive administrator credentials.
10. Review the terms and agreements, including the permissions that the Code42 connection requires, and click **Accept**.
    Microsoft OneDrive is added as a data connection and Code42 begins the initial inventory process.

> **Permissions can be delayed in Microsoft Azure**
> The permissions you accept during the authorization process can take up to 1 hour to flow through your Microsoft Azure environment. During this time, Code42 may report an error with the new connection in the Data Connections list. This error clears automatically as soon as Code42 is able to access the Microsoft audit log.

Next steps

Now that you have added OneDrive as a data connection, learn more about:

- Common use cases for investigating security incidents with Forensic Search
- How to use Forensic Search
- Adding trusted domains to easily identify when files are shared with users not on your list of approved domains
- Viewing and managing a cloud storage file's sharing permissions

Troubleshooting

Issues in your OneDrive environment can cause errors with the Code42 connection. When such issues occur, the connection in the **Data Connections** table is highlighted in red and an error message is displayed at the top of the screen. When this occurs, click the connection in the **Data Connections** table. The detail panel opens and lists the specific error so that you can resolve it.

Refer to these articles to troubleshoot specific errors that can appear for the OneDrive connection in the **Data Connections** list:

- Resolve "There is an issue with the connection" error
- Resolve maximum user drives exceeded errors
- Troubleshoot app permission errors for Microsoft OneDrive and Office 365 email
- Resolve "Microsoft Audit Log is inaccessible" errors for OneDrive
- Reconfigure scoping for user and group monitoring

External resources

Microsoft:

- Manage sharing in OneDrive and SharePoint
- Microsoft Graph permissions reference
- Turn auditing on or off

Related topics

- Introduction to adding data connections
- Data Connections reference
- Permissions required for the Microsoft OneDrive connector

- Vendor license requirements for Code42 data connections