Connect Code42 to Microsoft Office 365 email

Updated 5 months ago

Overview

To help protect you from data loss, you can use Code42 to investigate attachments sent through users' Microsoft Office 365 Outlook email accounts or mailboxes.

When you add Microsoft Office 365 as a data connection, you must authorize Code42 as a registered client API using your administrator account. Once connected, Code42 monitors your organization's email environment from that point forward to collect information about all attachments emailed by monitored users. That attachment file information then becomes available in Forensic Search for investigation.

This article explains how to add Microsoft Office 365 email as a data connection.

Considerations

> **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.

See also the considerations applicable to all email services.

Before you begin

Before you connect Code42 to Microsoft Office 365 email, complete these steps:

1. Verify that the users you want to monitor are active users that have an Exchange email account or mailbox in your Microsoft environment.
2. Plan user or group scoping to identify the users you want the Code42 connection to monitor.

Connect Code42 to Microsoft Office 365 email

Support

1. Sign in to the Code42 console.

2. Select **Administration > Integrations > Data Connections**.
3. Click **Add data connection**.
   *The **Add data connection** panel opens.*
4. From **Data connection**, select **Microsoft Office 365** under **Email services**.
5. Enter a display name. This name must be unique.
6. Select the scope of email users in your Microsoft Office 365 environment to monitor:
   - **All**: Monitors all email users with Office 365 mailboxes in your environment.
   - **Specific users**: Monitors only the Office 365 mailboxes for the email users you designate.
     1. Click **Upload .CSV file**.
     2. Select the scoping CSV file that contains a list of only those Office 365 email user accounts that you want to monitor.
   - **Specific groups**: Monitors only the mailboxes of the email users in the Office 365 groups you designate.
     1. Click **Upload .CSV file**.
     2. Select the scoping CSV file that contains a list of Office 365 groups whose user mailboxes you want to monitor.
7. Click **Authorize**.
   The Microsoft Office 365 sign in screen appears.
8. Enter your Microsoft Office 365 administrator credentials.
9. Review the terms and agreements, including the requested Office 365 email permissions, and click **Accept.**
   Microsoft Office 365 is added to the Data Connections list as an email data connection.

> **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.

The next time that an attachment is emailed by a monitored user, information about that file is recorded as an event by Code42. For details, see Attachment metadata below.

Next Steps

Now that you have added Microsoft Office 365 as a data connection, learn more about:

- Common use cases for investigating security incidents with Forensic Search
- How to use Forensic Search

Attachment metadata

Once you complete authorization, information about email attachments becomes available in Code42 Forensic Search. When an attachment is emailed by a monitored user, information about that attachment is sent to Code42. This attachment information includes the following:

- Filename
- Hash, when available
- Email address of the sender and recipients

> **Forensic Search timing**
> Email attachment information typically becomes available in Forensic Search results within 30 minutes, but may take longer in some cases.
>
> The **Date Observed** for the event indicates the date and time the attachment was emailed through Microsoft Office 365, not when the file event appeared in Code42.

> **More information on file activity**
> For more information on the specific metadata and file events visible in Forensic Search, see the File event metadata reference.

Troubleshooting

Issues in your Microsoft Office 365 email 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 email connection in the **Data Connections** list:

- Resolve "There is an issue with the connection" error
- Troubleshoot app permission errors for Microsoft OneDrive and Office 365 email
- Troubleshoot missing file events for Microsoft Office 365 email
- Reconfigure scoping for user and group monitoring

External resources

Microsoft documentation: Compare Exchange Online plans

Related topics

- Data Connections reference
- Introduction to adding data connections

- File event metadata reference
- Forensic Search use cases