# Use sharing auditing in the audit log

By robmazz

Archived: 2026-04-02 11:52:16 UTC

Sharing is a key activity in SharePoint Online and OneDrive for Business, and organizations widely use it. Administrators can use sharing auditing in the audit log to determine how sharing is used in their organization.

Sharing events (not including events related to sharing policy and sharing links) differ from file- and folder-related events in one primary way: one user performs an action that affects another user. For example, when a resource User A gives User B access to a file. In this example, User A is the *acting user* and User B is the *target user*. In the SharePoint File schema, the acting user's action only affects the file itself. When User A opens a file, the only information needed in the **FileAccessed** event is the acting user. To address this difference, there's a separate schema, called the *SharePoint Sharing schema* that captures more information about sharing events. This schema ensures that administrators have visibility into who shared a resource and the user the resource was shared with.

The Sharing schema provides two additional fields in an audit record related to sharing events:

- **TargetUserOrGroupType:** Identifies whether the target user or group is a Member, Guest, SharePointGroup, SecurityGroup, or Partner.
- **TargetUserOrGroupName:** Stores the UPN or name of the target user or group that a resource was shared with (User B in the previous example).

These two fields, in addition to other properties from the audit log schema such as User, Operation, and Date tell the full story about *which* user shared *what* resource with *whom* and *when*.

Another schema property is important to the sharing story. When you export audit log search results, the **AuditData** column in the exported CSV file stores information about sharing events. For example, when a user shares a site with another user, this action adds the target user to a SharePoint group. The **AuditData** column captures this information to provide context for administrators. See Step 2 for instructions on how to parse the information in the **AuditData** column.

Sharing occurs when a user (the *acting* user) shares a resource with another user (the *target* user). Audit records related to sharing a resource with an external user (a user who is outside of your organization and doesn't have a guest account in your organization's Microsoft Entra ID) are identified by the following events, which the audit log records:

- **SharingInvitationCreated:** A user in your organization tries to share a resource (likely a site) with an external user. This event results in an external sharing invitation sent to the target user. The invitation grants no access to the resource at this point.

- **SharingInvitationAccepted:** The external user accepts the sharing invitation sent by the acting user and now has access to the resource.
- **AnonymousLinkCreated:** An anonymous link (also called an "Anyone" link) is created for a resource. Because an anonymous link can be created and then copied, it's reasonable to assume that any document that has an anonymous link is shared with a target user.
- **AnonymousLinkUsed:** This event is logged when an anonymous link is used to access a resource.
- **SecureLinkCreated:** A user creates a "specific people link" to share a resource with a specific person. This target user might be someone who is external to your organization. The person that the resource is shared with is identified in the audit record for the **AddedToSecureLink** event. The time stamps for these two events are nearly identical.
- **AddedToSecureLink:** A user is added to a specific people link. Use the **TargetUserOrGroupName** field in this event to identify the user added to the corresponding specific people link. This target user might be someone who is external to your organization.

## Sharing auditing work flow

When a user (the acting user) wants to share a resource with another user (the target user), SharePoint (or OneDrive for Business) first checks if the email address of the target user is already associated with a user account in the organization's directory. If the target user is in the directory (and has a corresponding guest user account), SharePoint takes the following actions:

- Immediately assigns the target user permissions to access the resource by adding the target user to the appropriate SharePoint group, and logs an **AddedToGroup** event.
- Sends a sharing notification to the email address of the target user.
- Logs a **SharingSet** event. This event has a friendly name of "Shared file, folder, or site" under **Sharing and access request activities** in the activities picker of the audit log search tool. See the screenshot in Step 1.

If a user account for the target user isn't in the directory, SharePoint takes the following actions:

- Logs one of the following events, based on how the resource is shared:
    - **AnonymousLinkCreated**
    - **SecureLinkCreated**
    - **AddedToSecureLink**
    - **SharingInvitationCreated** (this event is logged only when the shared resource is a site)
- When the target user accepts the sharing invitation (by clicking the link in the invitation), SharePoint logs a **SharingInvitationAccepted** event and assigns the target user permissions to access the resource. If the target user is sent an anonymous link, the **AnonymousLinkUsed** event is logged after the target user uses the link to access the resource. For secure links, a **FileAccessed** event is logged when an external user uses the link to access the resource.

Additional information about the target user is also logged, such as the identity of the user the invitation is to and the user who accepts the invitation. In some cases, these users (or email addresses) can be different.

A common requirement for administrators is creating a list of all resources that administrators shared with users outside of the organization. By using sharing auditing in Office 365, administrators can generate this list. Here's how.

### Step 1: Search for sharing events and export the results to a CSV file

Search the audit log for sharing events. For more information (including the required permissions) about searching the audit log, see Search the audit log.

Complete the following steps to search for sharing events:

1. Sign in to the Microsoft Purview portal.
2. Select the **Audit** solution card. If the **Audit** solution card isn't displayed, select **View all solutions** and then select **Audit** from the **Core** section.
3. On the **Search** page and under **Activities - friendly names**, select **Sharing and access request activities** to search for sharing-related events.
4. Select a date and time range to find the sharing events that occurred within that period.
5. Select **Search** to run the search.
6. When the search finishes and displays the results, select **Export results** > **Download all results**.

   After you select the export option, a message at the bottom of the window prompts you to open or save the CSV file.
7. Select **Save** > **Save as** and save the CSV file to a folder on your local computer.

### Step 2: Use the PowerQuery Editor to format the exported audit log

Use the JSON transform feature in the Power Query Editor in Excel to split each property in the **AuditData** column (which consists of a multi-property JSON object) into its own column. This feature lets you filter columns to view records related to sharing.

For step-by-step instructions, see "Step 2: Format the exported audit log using the Power Query Editor" in Export, configure, and view audit log records.

### Step 3: Filter the CSV file for resources shared with external users

In this step, you filter the CSV file for the different sharing-related events that the SharePoint sharing events section describes. Alternatively, you can filter the **TargetUserOrGroupType** column to display all records where the value of this property is **Guest**.

After you follow the instructions in the previous step to prepare the CSV file by using the PowerQuery editor, complete the following steps:

1. Open the Excel file that you created in Step 2.
2. On the **Home** tab, select **Sort & Filter**, then select **Filter**.
3. In the **Sort & Filter** dropdown list on the **Operations** column, clear all selections, then select one or more of the following sharing-related events and select **Ok**.
    - **SharingInvitationCreated**
    - **AnonymousLinkCreated**
    - **SecureLinkCreated**
    - **AddedToSecureLink**

    Excel displays the rows for the events you selected.
4. Go to the column named **TargetUserOrGroupType** and select it.
5. In the **Sort & Filter** dropdown list, clear all selections, then select **TargetUserOrGroupType:Guest**, and select **Ok**.

    Now Excel displays the rows for sharing events **and** where the target user is outside of your organization, because external users are identified by the value **TargetUserOrGroupType:Guest**.

Tip

For the audit records that are displayed, the **ObjectId** column identifies the resource that you shared with the target user. For example, `ObjectId:https:\/\/contoso-my.sharepoint.com\/personal\/sarad_contoso_com\/Documents\/Southwater Proposal.docx`.

---