

NetWitness® Platform XDR

Dropbox Event Source Log Configuration Guide

Dropbox

Event Source Product Information:

Vendor: [Dropbox](#)

Event Source: Dropbox

Versions: API v2.0

NetWitness Product Information:

Supported On: NetWitness Platform XDR 11.7 or later

Note: Dropbox is supported from NetWitness Platform XDR 11.5 or later. However, NetWitness recommends you to update NetWitness Platform XDR to the latest version.

Event Source Log Parser: cef

Note: The CEF parser parses this event source as `device.type=dropbox`.

Collection Method: Plugin Framework

Event Source Class.Subclass: Host.Cloud

Contact Information

NetWitness Community at <https://community.netwitness.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates and are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

November, 2022

Contents

- Collect Dropbox Events in NetWitness Platform XDR 5**
- Configure the Dropbox Event Source 6**
- Set Up the Dropbox Event Source in NetWitness Platform XDR 10**
 - Deploy the Dropbox Files from NetWitness Live 10
 - Configure the Event Source 10
- Dropbox Collection Configuration Parameters 12**
- Getting Help with NetWitness Platform XDR 13**
 - Self-Help Resources 13
 - Contact NetWitness Support 13
 - Feedback on Product Documentation 14

Collect Dropbox Events in NetWitness Platform XDR

The Dropbox event monitoring product gathers information about your organization's Dropbox operational events. You can use these events to analyze usage trends and user behavior. The [Dropbox Business API](#) allows apps to manage the user lifecycle for a Dropbox Business account and perform [API actions](#) on all members of a team.

The Dropbox integration consumes team information and the team's detailed activity log using Dropbox V2 API. The Dropbox V2 API aggregates team member actions which are organized by the event category and event type.

To configure Dropbox , you must follow the steps below:

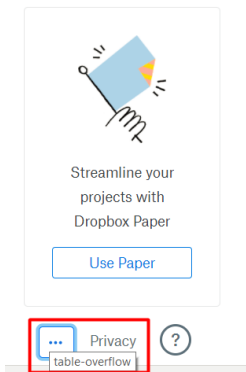
- I. [Configure the Dropbox Event Source](#)
- II. [Set Up the Dropbox Event Source in NetWitness Platform XDR.](#)

Configure the Dropbox Event Source

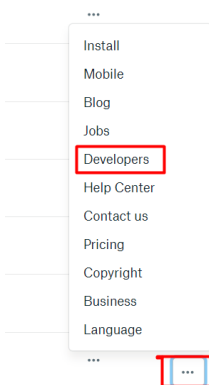
To configure the Dropbox, you must create a Dropbox connected app.

To create a Dropbox connected app

1. Log-in to your Dropbox account using the Dropbox URL:
<https://www.dropbox.com/login>.
2. Once you have logged in, click on the table over-flow button.



3. Select **Developers** from the drop-down menu.



4. Click **My apps** and then click **Create app** to create a connected app.



My apps

Create app



API v2

My apps

API Explorer

Documentation



HTTP

.NET

5. Choose the **Dropbox Business API** button and then select the **Team Auditing** for type of access.

Create a new app on the DBX Platform

1. Choose an API

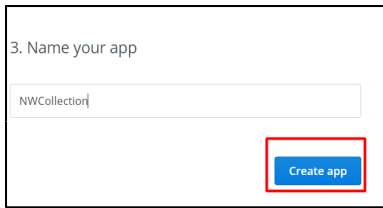
| | | | |
|--|---|--|---|
| <input type="radio"/> Dropbox API For apps that need to access files in Dropbox. Learn more |  | <input checked="" type="radio"/> Dropbox Business API For apps that need access to Dropbox Business team info. Learn more |  |
|--|---|--|---|

2. Choose the type of access you need

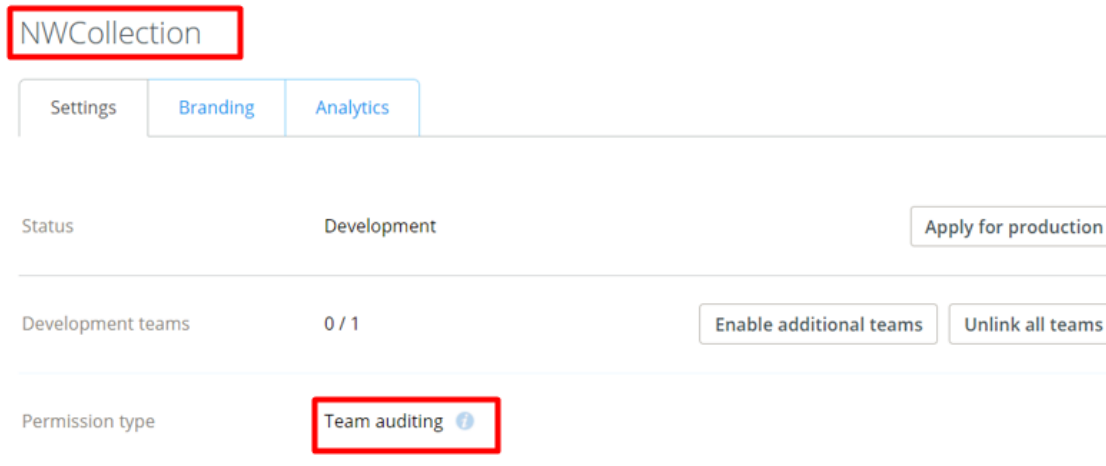
[Learn more about access types](#)

| |
|---|
| <input type="radio"/> Team information - Information about the team and aggregate usage data. |
| <input checked="" type="radio"/> Team auditing - Team information, plus the team's detailed activity log. |
| <input type="radio"/> Team member file access - Team information and auditing, plus the ability to perform any action as any team member. |
| <input type="radio"/> Team member management - Team information, plus the ability to add, edit, and delete team members. |

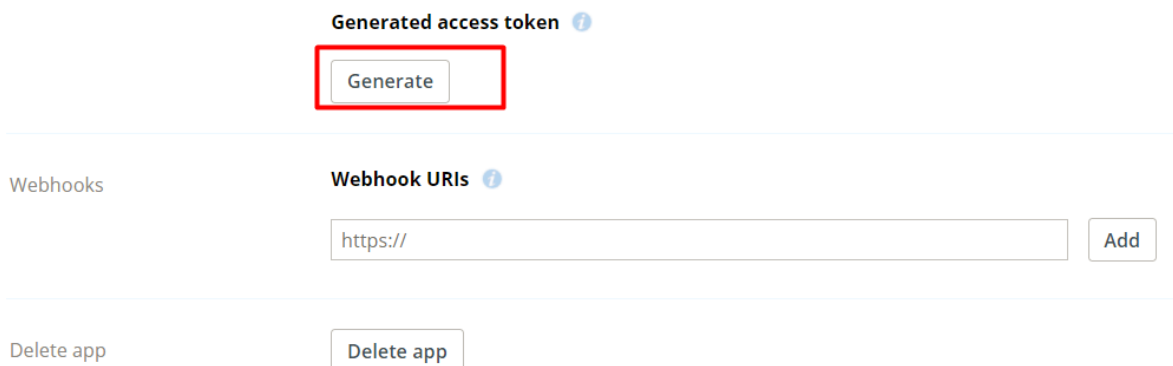
6. Enter a name for your connected app and click **Create app**.



The connected app is created as shown here:

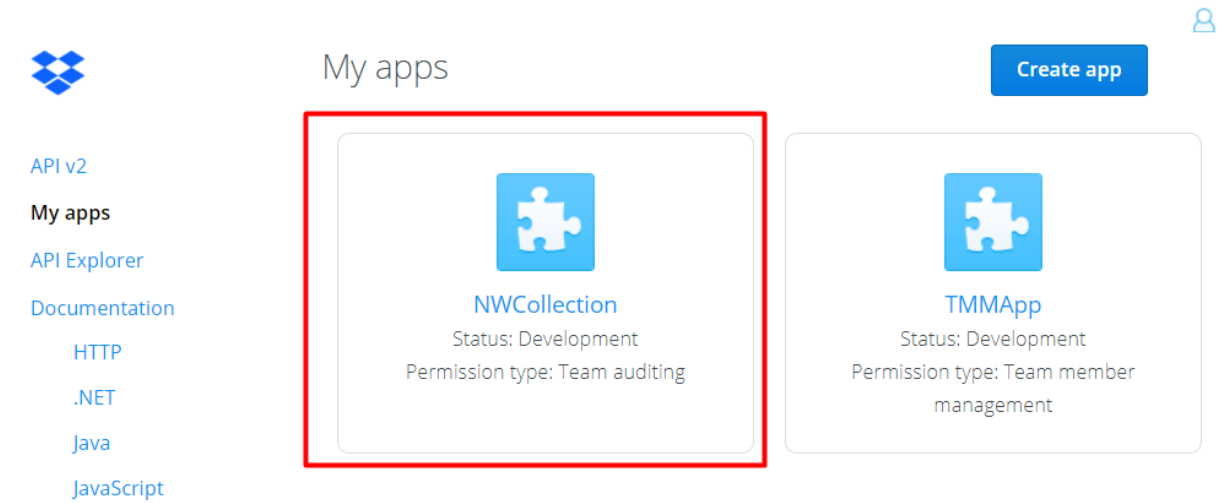


7. Click **Generate** to create the access token.



IMPORTANT: Make sure to save the access token, as you need access token when you configure Dropbox in NetWitness Platform XDR.

The connected app has been created as shown here:



Note: Please make sure that below URL is allowed to open in your network firewalls/proxies as we use them for event collection.
- https://api.dropboxapi.com/2/team_log/get_events.

Set Up the Dropbox Event Source in NetWitness Platform XDR


In NetWitness Platform XDR, perform the following tasks:

- I. [Deploy the Dropbox Files from NetWitness Live](#)
- II. [Configure the Event Source](#).

Deploy the Dropbox Files from NetWitness Live

Dropbox requires resources available in Live in order to collect logs.

To deploy the Dropbox files from Live:

1. In the NetWitness Platform XDR menu, select  **(Configure)** > **Live Content**.
2. Browse Live Content for the **cef** parser, using **NetWitness Log Device** as the **Resource Type**.
3. Select the **Dropbox** parser from the list and click **Deploy** to deploy it to the appropriate Log Decoders using the Deployment Wizard.
4. You should also deploy the Dropbox package. Browse Live for Dropbox content by typing "Dropbox" into the Keywords text box and click **Search**.
5. Select the package and click **Deploy** to deploy it to the appropriate Log Collectors.

Note: On a hybrid installation, you should deploy the package on both the Virtual Log Collector (VLC) and the Log Collector (LC). If you deploy the package on the LC, you should restart the log decoder and log collector services, otherwise logs will not be collected.



6. Restart the nwlogcollector service.

For more details, see the [Add or Update Supported Event Source Log Parsers](#) topic.

Configure the Event Source

This section contains details on setting up the Dropbox event source in NetWitness Platform XDR. In addition to the procedure, the [Dropbox Collection Configuration Parameters](#) are described.

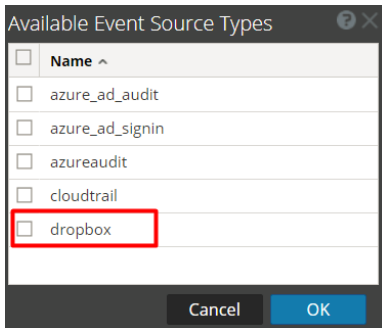
To configure the Dropbox Event Source:

1. In the NetWitness Platform XDR menu, select  **(Admin)** > **Services**.
2. In the Services grid, select a Log Collector service, and from the **Actions** () menu, choose **View** > **Config** > **Event Sources**.
3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

The Event Categories panel displays the File event sources that are configured, if any.

- In the Event Categories panel toolbar, click **+**.

The Available Event Source Types dialog is displayed.

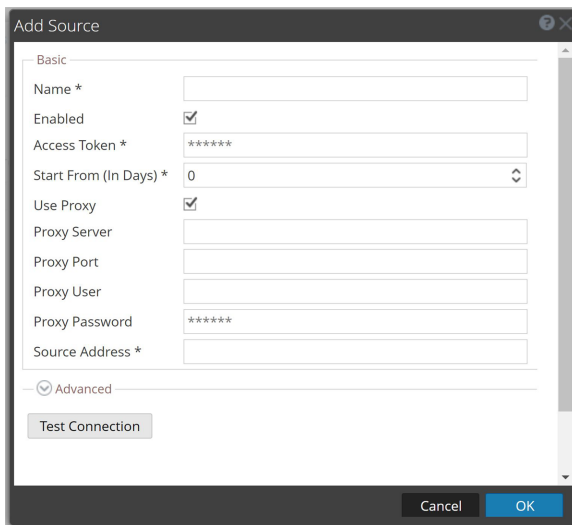


- Select **dropbox** from the list, and click **OK**.

The newly added event source type is displayed in the Event Categories panel.

- Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.



- Define parameter values, as described in [Dropbox Collection Configuration Parameters](#).
- Click **Test Connection**.

The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

Note: The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and NetWitness Platform XDR displays an error message.

- If the test is successful, click **OK**.

The new event source is displayed in the Sources panel.

Dropbox Collection Configuration Parameters

The following table describes the configuration parameters for the Dropbox integration with NetWitness Platform XDR. Fields marked with an asterisk (*) are required.

Note: When run from behind an SSL proxy, if certificate verification needs to be disabled, uncheck the SSL Enable checkbox in the Advanced section.

| Name | Description |
|-----------------|--|
| Name * | Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen. |
| Enabled | Select the box to enable the event source configuration to start collection. The box is selected by default. |
| Access Token * | The access token to retrieve the dropbox event logs. This is the same access token that you have generated and saved at step 7 during the Configure the Dropbox Event Source procedure. |
| Start From * | Choose the date from which to start collection. This parameter defaults to the current date, i.e, 0 and logs will be collected from last 60 mins. The Maximum value is 90 and logs will be collected from last 90 days in that case. IMPORTANT: Specify the number of days prior to the current date, from which log collection should start. Default value is 0 (current day), and the range is 0–90. For example, current date is 21 Apr 2023 and you want to collect logs from 19 Apr 2023, set the value to 2. |
| Test Connection | Checks the configuration parameters specified in this dialog to make sure they are correct. |

Getting Help with NetWitness Platform XDR

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: <https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation>.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: <https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions>.
- See the NetWitness Knowledge Base: <https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base>.
- See Troubleshooting section in the guides.
- See also [NetWitness® Platform Blog Posts](#).
- If you need further assistance, [Contact NetWitness Support](#).

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform XDR or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

| | |
|--|---|
| NetWitness Community Portal | https://community.netwitness.com In the main menu, click Support > Case Portal > View My Cases . |
| International Contacts (How to Contact NetWitness Support) | https://community.netwitness.com/t5/support/ct-p/support |
| Community | https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions |

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.