Your Mission: Use F-Response to collect OneDrive account data

Using F-Response to connect to OneDrive and collect its contents

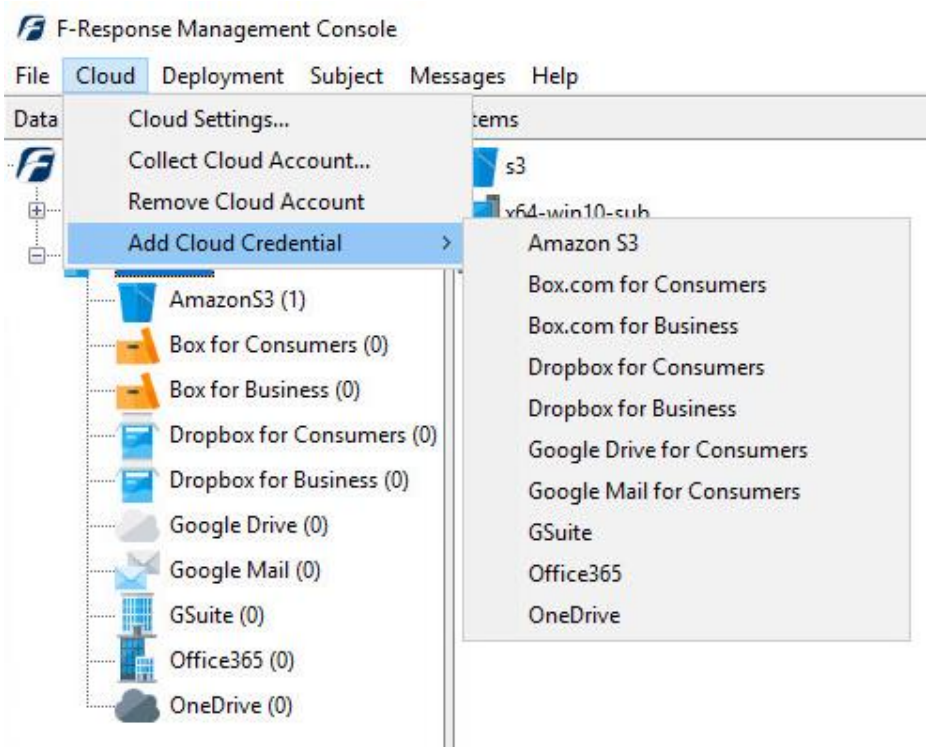
Important Note

Disclaimer: F-Response provides access to 3rd party data sources via Application Programming Interfaces (APIs) and internal structures presented by the provider. 3rd party provided data sources by their very nature are volatile. The afore mentioned F-Response products provide "best effort" for accessing and interacting with those 3rd party data sources however service disruptions, API changes, provider errors, network errors, as well as other communications issues may result in errors or incomplete data access. F-Response always recommends secondary validation of any 3rd party data collection.

F-Response Cloud Collector Options Supported		
Revision History	Not available.	Microsoft Onedrive does not support revision history. Enabling Revision History in F-Response will have no effect on the collection.
Hash Verification	Available and supported.	Microsoft Onedrive provides sha1 hashes of items which will be automatically checked in F-Response if Verify Hashes is enabled.
Rerun Collection	Available and supported.	F-Response can retry to collect specific items that have errored out. This option is only available when collecting to a local directory.

Step 1: Open the OneDrive Credential Configuration Window

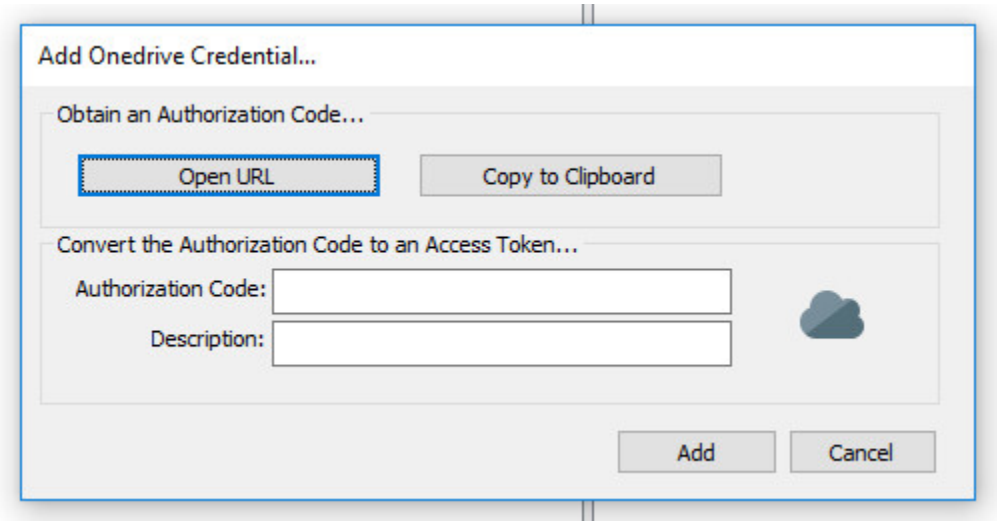
Open the F-Response Management Console and navigate to Cloud->Add Cloud Credential->OneDrive, or double click on the appropriate icon in the Data Sources pane.



F-Response Management Console

Step 2: Open URL or Copy to Clipboard

The first step in obtaining access to the OneDrive for Consumers account is to request access either via the browser directly, or if you do not have access to the account in question, copying the request URL to the clipboard to be shared with the account holder via email, IM, etc.

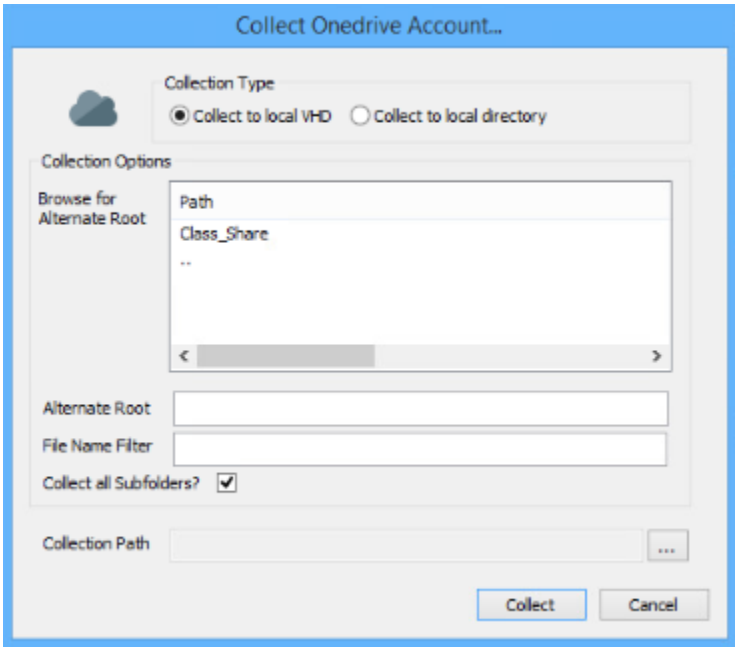


Credentials Dialog

Regardless of the method chosen, the web browser user will be asked to login to OneDrive and authorize the F-Response Connector, upon completion they will be redirected to the F-Response website where an Authorization code will be presented. This is the OneDrive Authorization Code. That code and a Description must be inputed into the dialog window. Press Add to verify and add this credential.

Step 3: Start a collection

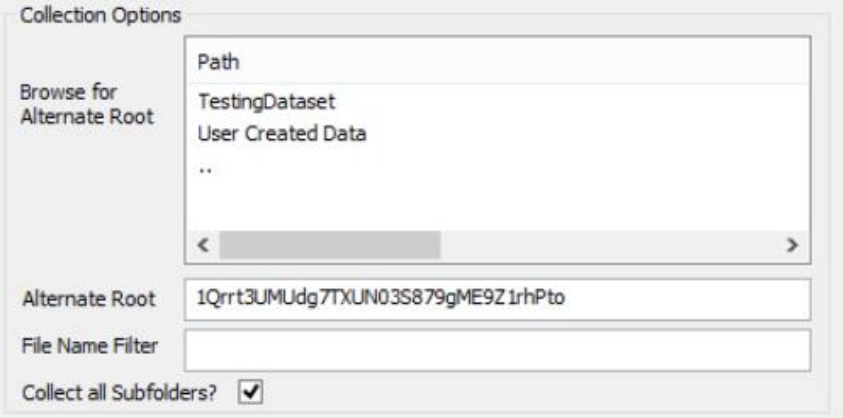
Select the OneDrive icon under Data Sources and then double click on the newly added OneDrive account under Items. This will prepare a new dialog for collecting the account's contents.



Starting a new collection

To collect the full account specify whether you would like to collect the contents to a virtual hard disk or a local directory under **Collection Type**, choose a location to place the data in the **Collection Path** field (Note: collection path must be local as you cannot collect to a network share) and click the **Collect** button.

To refine the scope of the collection some, or all, of the **Collection Options** can be invoked to reduce the size of the data set to be collected. The options are as follows:



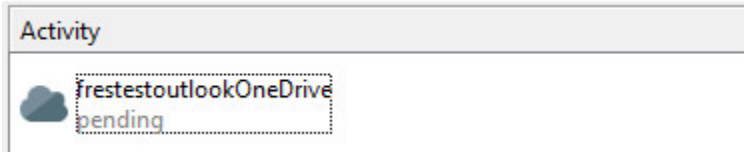
Browse for Alternate Root: This option will allow you to select a different starting location to pull data from. Click on an item and wait a moment for the subdirectories to parse. Continue to click and drill as far down the path as you need to narrow the scope of the collection accordingly (the 'double dot' option will take you back). The **Alternate Root** field below will populate with the correct information.

File Name Filter: Will check the string entered here against files as presented by the provider. There is no need to enter wildcards (*.*) and it does not use regular expressions. For example, to collect only Excel files in the account, just type **.xls** in the box.

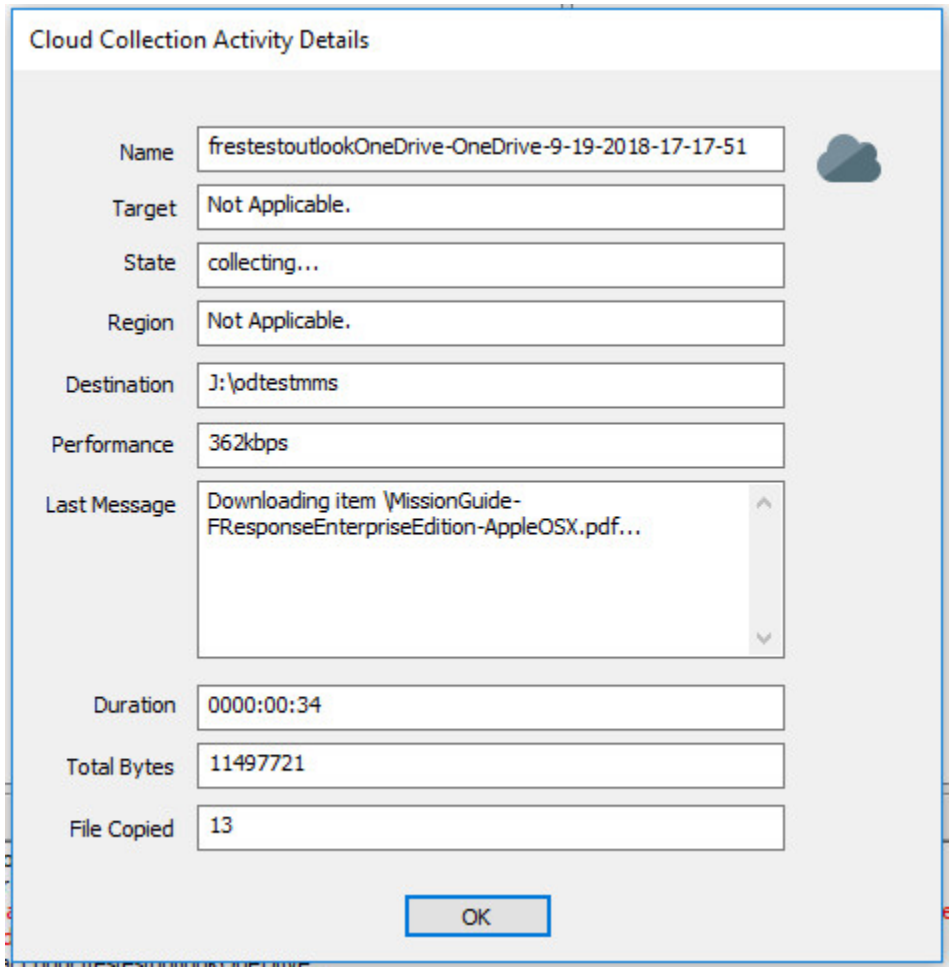
Collect all Subfolders? If checked, it will collect the content of all subfolders, if unchecked, it will only collect that folder's file contents.

Step 4: Check the Activity Pane

The Activity Pane shows the active collection. Double clicking on the collection will provide additional details.



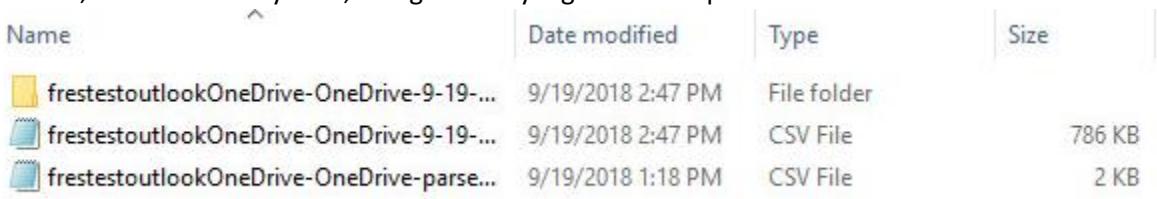
Activity



Collection Details…

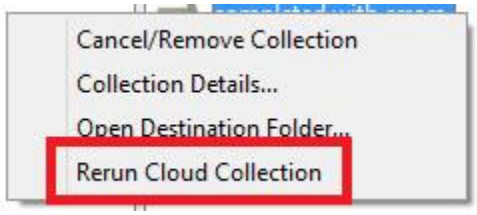
Step 5: Review the collection

Navigate to the destination folder at the completion of the collection to review the individual files collected, or the summary VHD, along with any log or error reports.



Collected items

Rerunning a collection



If your cloud collection completes with errors, F-Response can be used to rerun the collection and target only those files/folders it was unable to collect. This operation can be performed multiple times until a collection completes successfully. Not all providers offer rerunning options, and not all errors can be reattempted. To rerun a cloud collection, right click on the completed collection in the Activity column and choose **Rerun Cloud Collection**.

***Note**: Rerunning a collection is only available when collecting to a local directory, this not an option when collecting in VHD format.

Additional Details

The following file datetime values are used by F-Response during the collection *(Any missing dates are set to 1601-01-01T00:00:01Z)*:

WINDOWS TIME	PROVIDER VALUE
MODIFIED	lastModifiedDateTime
ACCESSED	
CREATED	createdDateTime

Troubleshooting

I receive error code 600 while parsing the Onedrive account, why is that?

All Onedrive accounts include one or more Onenote documents. Onenote files are not supported by the Onedrive API and return data we do not support at this time. Error code 600 indicates we have found the Onenote files, but cannot process them.