Your Mission: Use F-Response to collect Office365 OneDrive data

Using F-Response to connect to Office365 Onedrive and collect its contents

Important Note

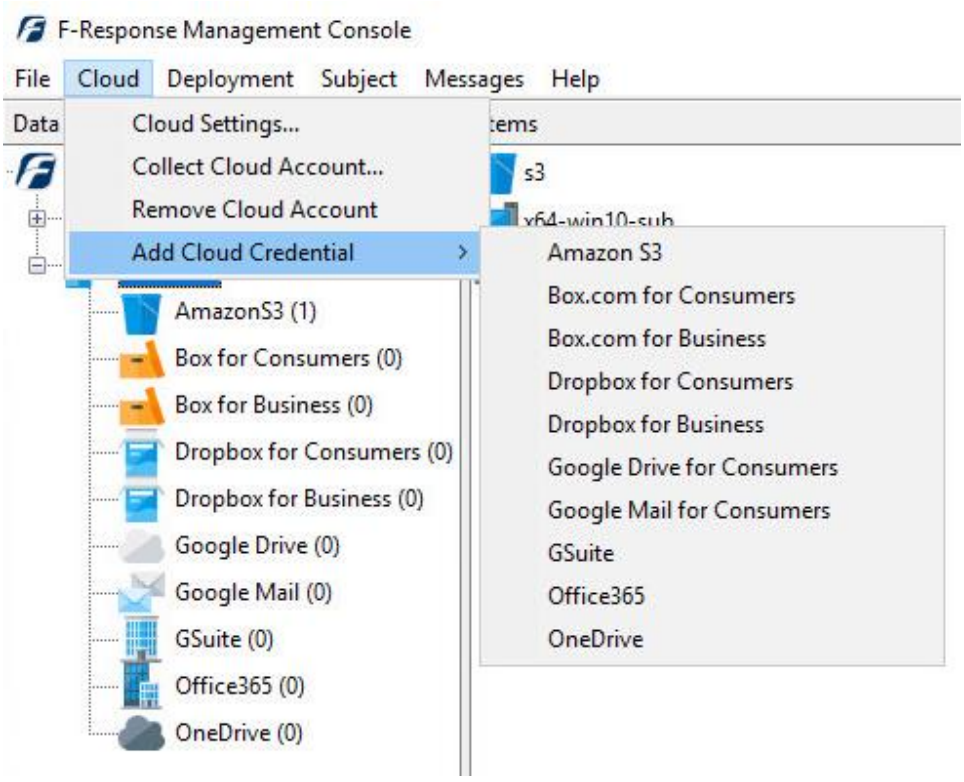
Disclaimer: F-Response provide access to 3rd party data sources via Application Programming Interfaces (APIs) and internal structures presented by the provider. 3rd party provided data sources by their very nature are volatile. The afore mentioned F-Response products provide "best effort" for accessing 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 Office365 does not support revision history. Enabling Revision History in F-Response will have no effect on the collection.
Hash Verification	Available and supported.	Microsoft Office365 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

*Note: Office365 collection should be run from a Windows 10 or newer OS.

Step 1: Open the Office365 Credential Configuration Window

Open the F-Response Management Console and navigate to Cloud->Add Cloud Credential->Office365, or double click on the appropriate icon in the Data Sources pane.

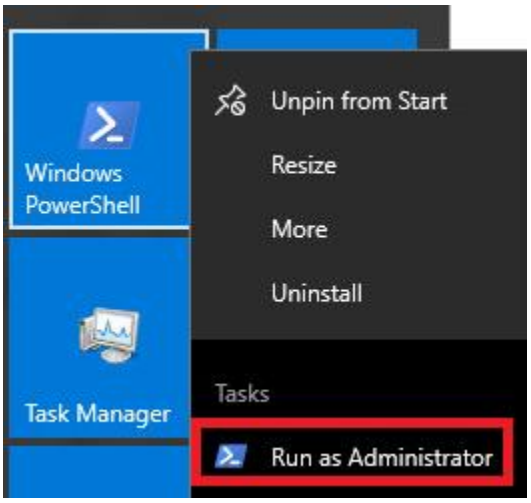


F-Response Management Console

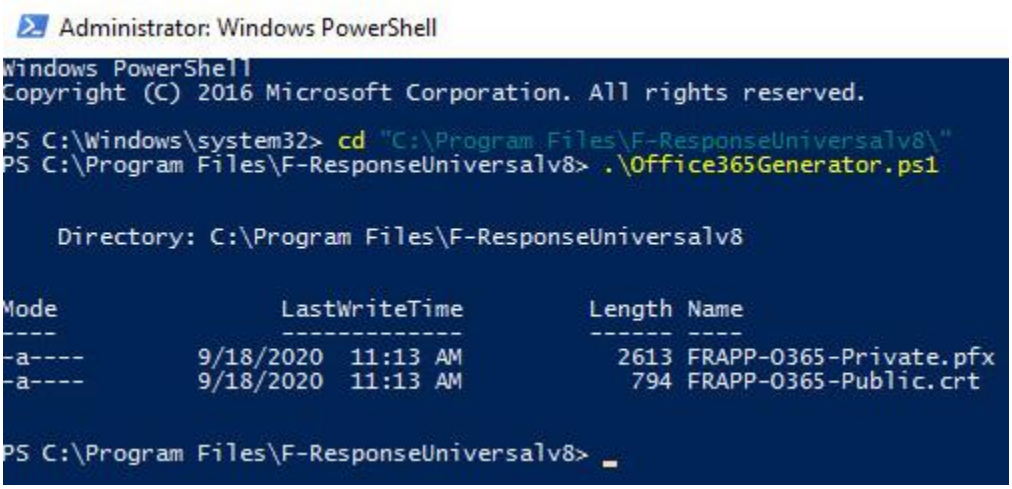
Step 2: Create a Client Credentials Flow Account on Azure AD for the Office365 Domain

Before you can access Office365 custodian Onedrive accounts you will need to create a "Client Credentials Flow" account on Azure AD for the Office365 Domain. This is a one time process and does not need to be done again for a year. The account we will create requires a custom certificate for authentication. Generating this certificate can be time consuming, so we have provided a Powershell script in the F-Response installation folder that does all the heavy lifting for you.

You will need to open an Administrator Powershell console:



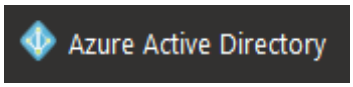
and execute the provided "Office365Generator.ps1."



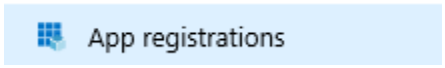
This script will create a both a "**FRAPP-O365-Public.pfx**" file and a "**FRAPP-O365-Private.crt**" file that contain all the details necessary for an Office365 Application Registration.

Once you have those files you may start by logging into https://portal.azure.com with an Office365 Administrator username and password.

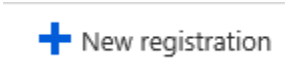
You'll then need to locate the Azure Active Directory on the left side menu.



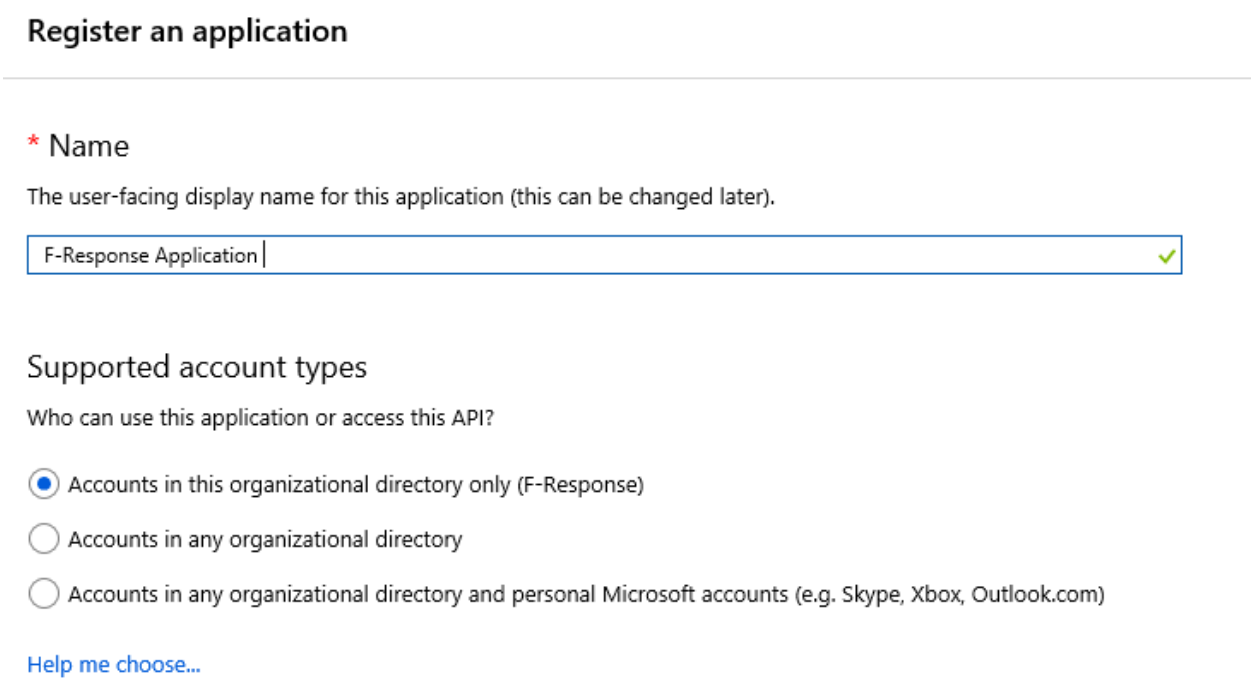
From there you will need to select App registrations.



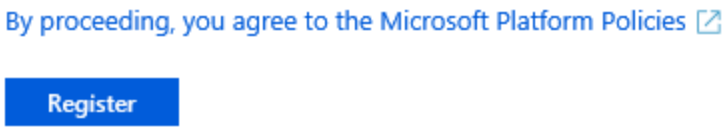
Then press New registration.



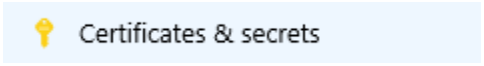
The details under new registration aren't important, however feel free to use the following:



Register the new application by pressing the Register.

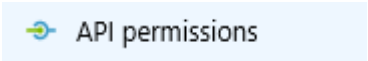


Now that your F-Response App has been created you'll need to click on Certificates & secrets to access the application's public key.

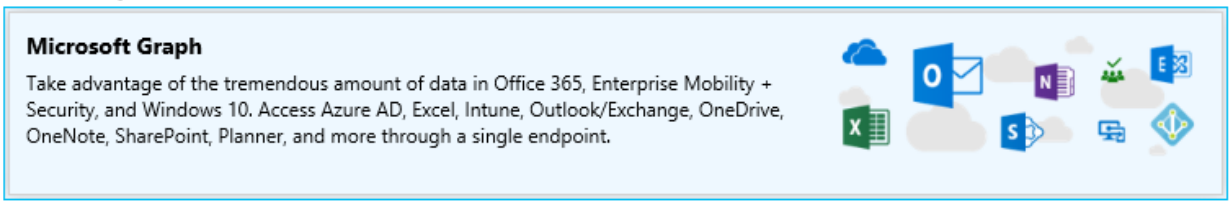


Use the Upload certificate button to upload the **FRAPP-O365-Public.crt** file generated by the Powershell script included with your installation.

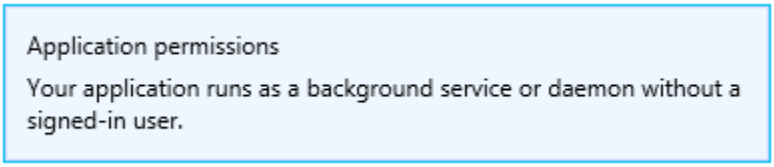
Once you have successfully uploaded the certificate, press on the API permissions button to set the necessary permissions for F-Response.



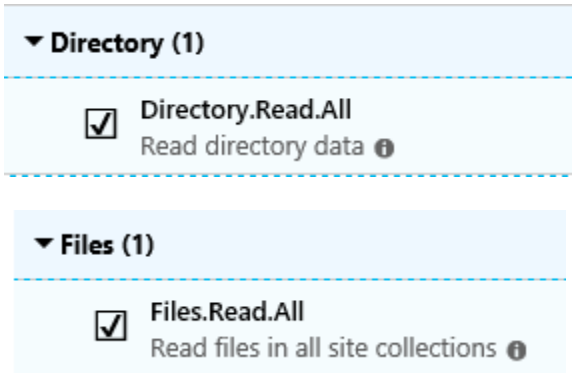
Use the Add a permission button, then select Microsoft Graph permissions.



You will want to select Application permissions

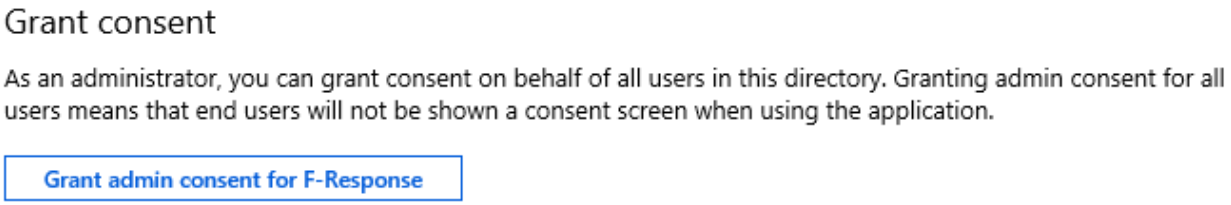


You will want to select Directory.Read.All and Files.Read.All. See below for more details.



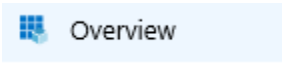
You may receive a warning about administrator grants, you may safely ignore that warning.

Once the Permissions have been added press Grant admin consent to assign the requested permissions to the application.

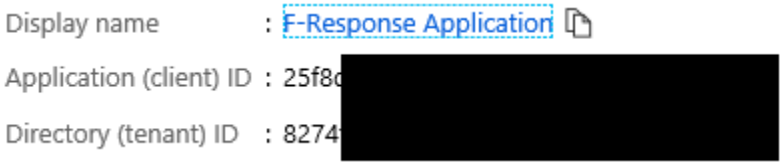


You will need two more pieces of information to complete the process and setup the F-Response account.

Press Overview to show the required details.



Locate the Directory Id and Application Id on the overview page and save these along with the FRAPP-O365-Private.pfx file to input into the F-Response Office365 Credential interface.

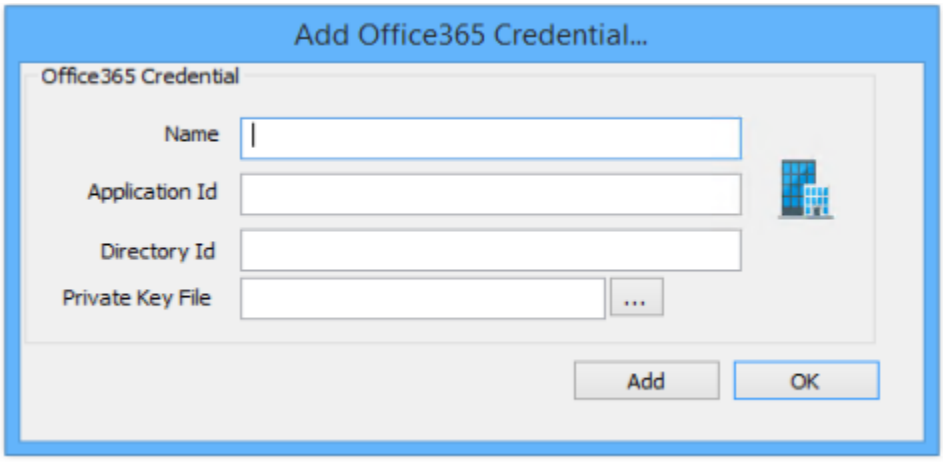


In summary you should have the following:

- Application ID
- Directory ID
- FRAPP-O365-Private.pfx

Step 3: Adding the Office 365 Credential

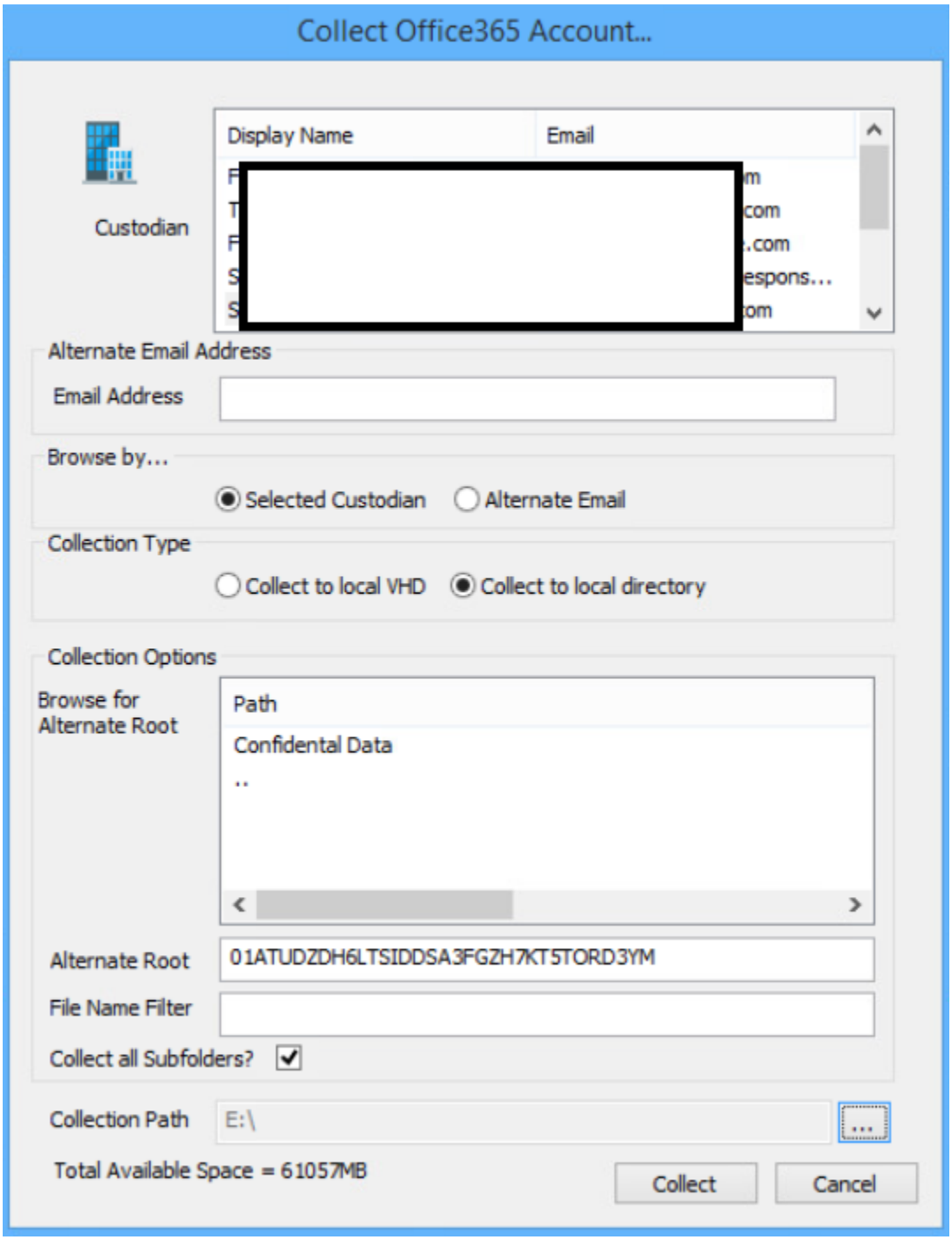
To configure Office365 access you will need to enter the Application Id, Directory Id, and the Private Key file generated earlier.



Add an Office 365 Credential

Step 4: Start a collection

Select the Office365 icon under Data Sources and then double click on the newly added Office365 account under Items. This will prepare a new dialog for collecting the account's contents.



Starting a new collection...

Highlight the specific user account you would like to collect from the **Custodian** list or enter the known email address in **Alternate Email Address** and select the appropriate **Browse by…** option according to your choice. Select whether you would like to collect the contents to a virtual hard disk or a local directory under **Collection Type**. Lastly, enter the location where the collected data is to be stored in the **Collection Path** and click the **Collect** button to begin the collection. (Note: collection path must be local as you cannot collect to a network share).

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:

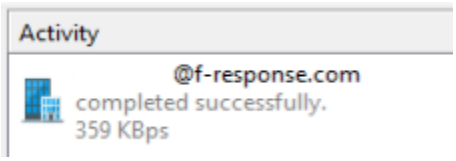
Browse for Alternate Root: This option will allow you to select a different starting location to pull data from. Click on an item and wait a moment for the subdirectories to parse. Continue to click and drill as far down the path as you need to narrow the scope of the collection accordingly (the 'double 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.

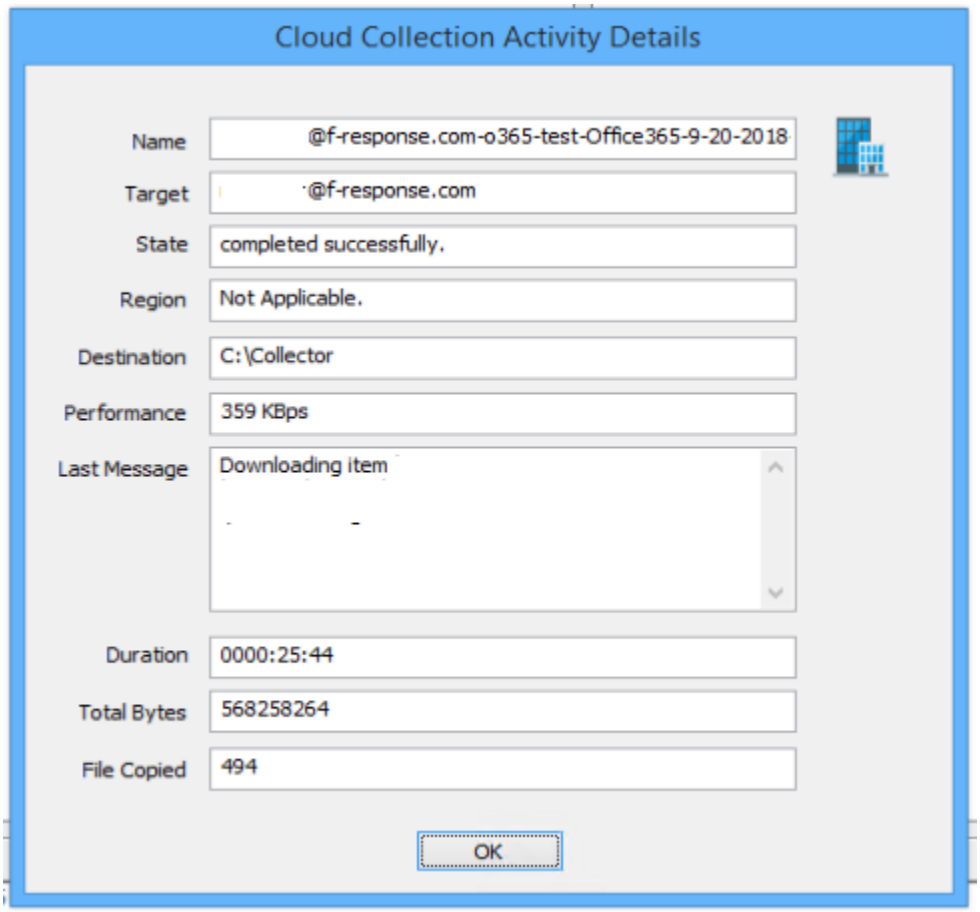
Collect all Subfolders? If checked, it will collect the content of all subfolders, if unchecked, it will only collect that folder's file contents.

Step 5: Check the Activity Pane

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



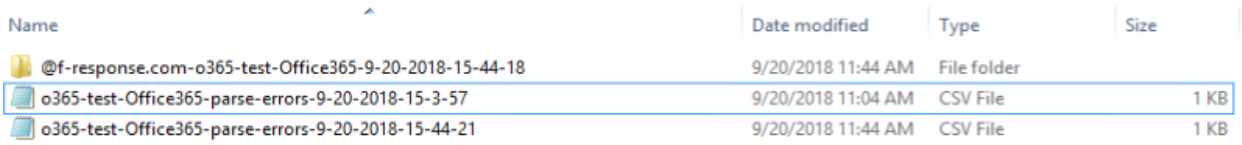
Activity



Collection Details…

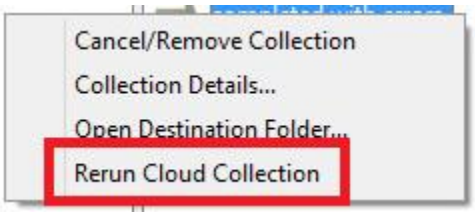
Step 6: Review the collection

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