Mission Guide: Office 365 OneDrive

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

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

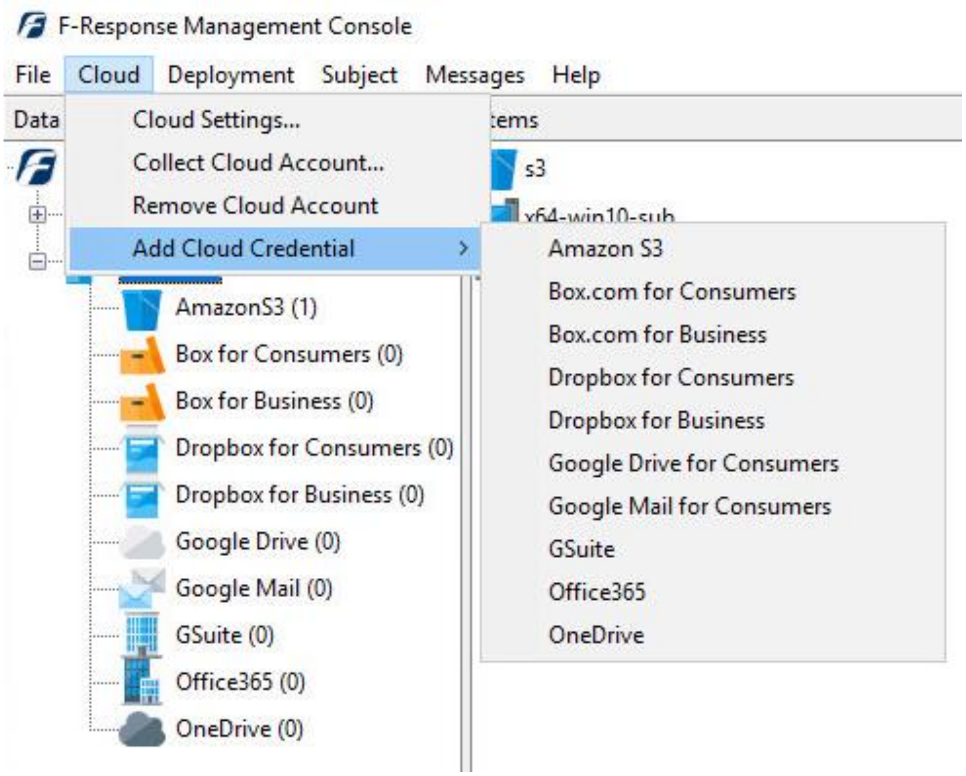
Important Note

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.

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

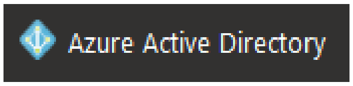
Before you can access Office365 custodian Onedrive accounts you will need to create a "Client Credentials Flow" account on Azure AD for the Office365 Domain. This is a one time process and does not need to be done again for a year. The account we will create requires a custom certificate for authentication. 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."

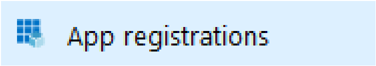
This script will create a both a "FRAPP-O365.pfx" file and a "keyCredentials.txt" file that contain all the details necessary for an Office365 Application Registration.

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

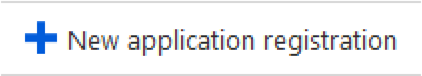
You'll then need to locate the Azure Active Directory on the left side menu.



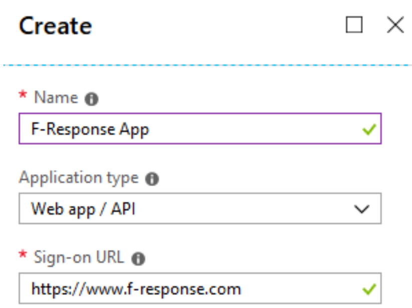
From there you will need to select App registrations.



Then press New application registration.



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



Create

* Name

F-Response App

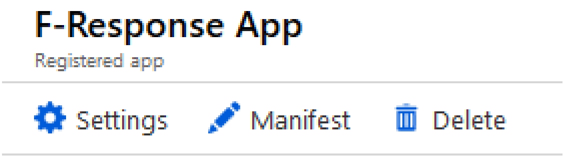
Application type

Web app / API

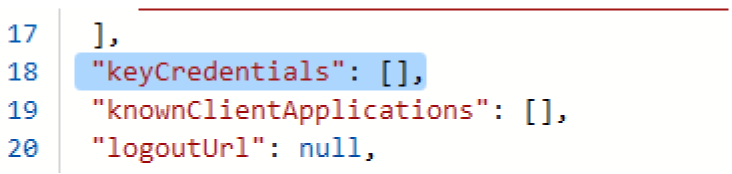
* Sign-on URL

https://www.f-response.com

Now that your F-Response App has been created you'll need to click on Manifest to access the application's text manifest details.

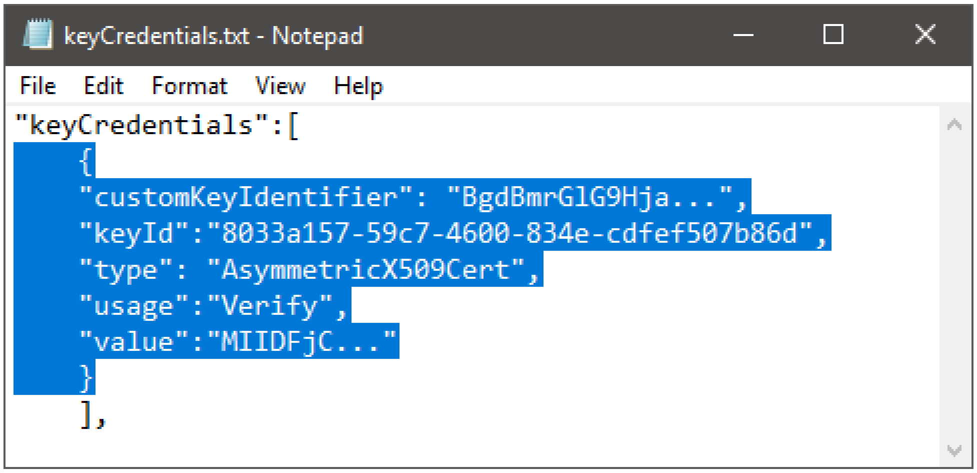


Look for the "keyCredentials" section, it should be empty, ie. "[]".



```
],
"keyCredentials": [],
"knownClientApplications": [],
"logoutUrl": null,
```

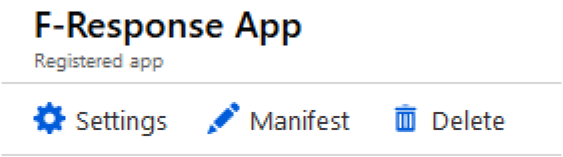
Now open the generated keyCredentials.txt file created by our provided Powershell script and copy the contents to the online manifest. You will want to only select the curly brackets and all values in between. See below for details *(Note: Your values will be different and may be longer.)*:



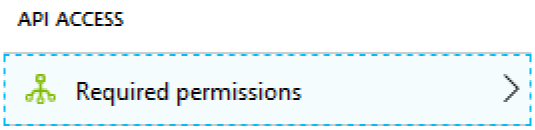
```
"keyCredentials":[
    {
    "customKeyIdentifier": "BgdBmrG1G9Hja...",
    "keyId":"8033a157-59c7-4600-834e-cdfef507b86d",
    "type": "AsymmetricX509Cert",
    "usage":"Verify",
    "value":"MIIDFjC..."
    }
    ],
```

Paste the new keyCredentials values in the online manifest editor and press Save.

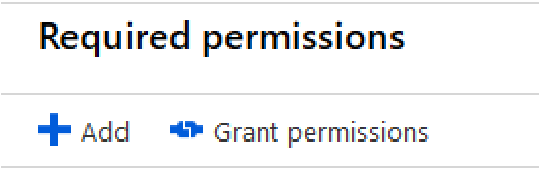
Now return to the F-Response App section and press Settings to assign permissions.



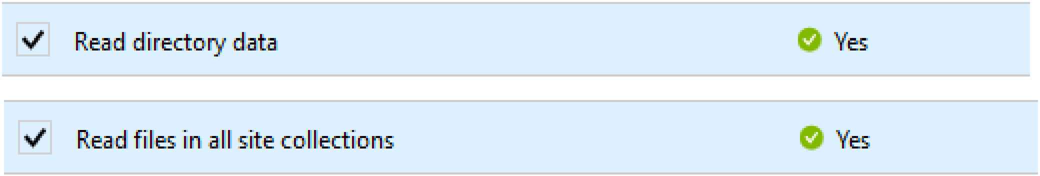
You will find the Required Permissions under API Access.



Under Required Permissions press Add and select Microsoft Graph.



Under Enable Access you will need to select two Application Permissions.

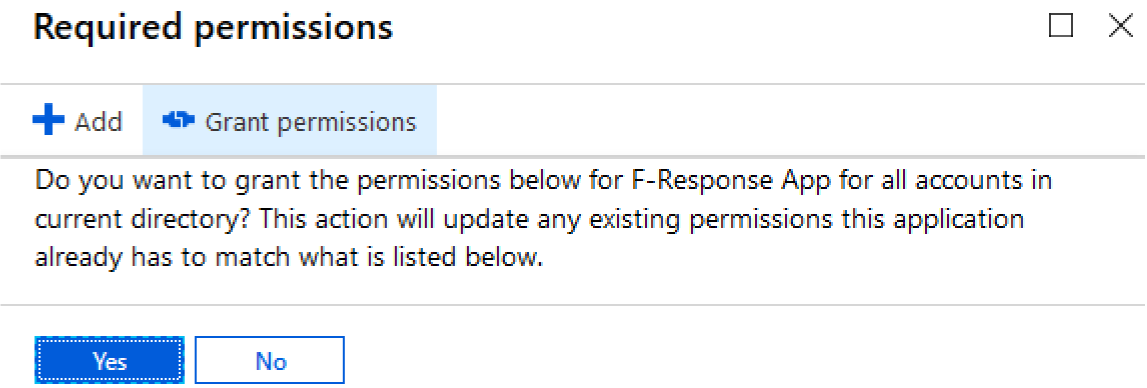


☑ Read directory data ✓ Yes

☑ Read files in all site collections ✓ Yes

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

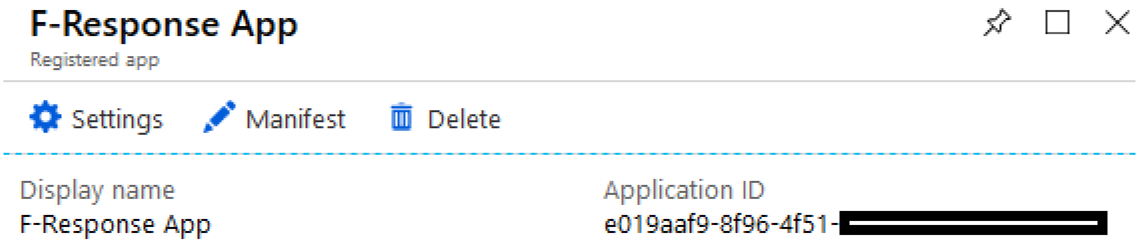
Once the Permissions have been added press Grant permissions to assign the requested permissions to the application.



Do you want to grant the permissions below for F-Response App for all accounts in current directory? This action will update any existing permissions this application already has to match what is listed below.

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

First you will need the Application ID, you will find that under the F-Response App section:



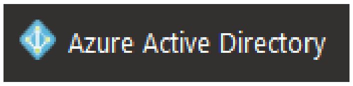
F-Response App

Registered app

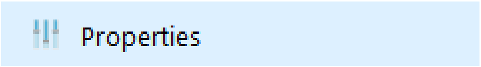
Display name: F-Response App

Application ID: e019aaf9-8f96-4f51-[redacted]

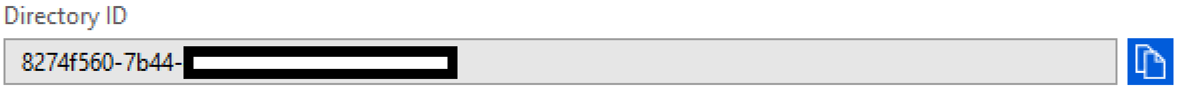
And you will need the Directory Id. For that you will need to click on Azure Active Directory



Then click on Properties.



And save a copy of the Directory ID.



Directory ID

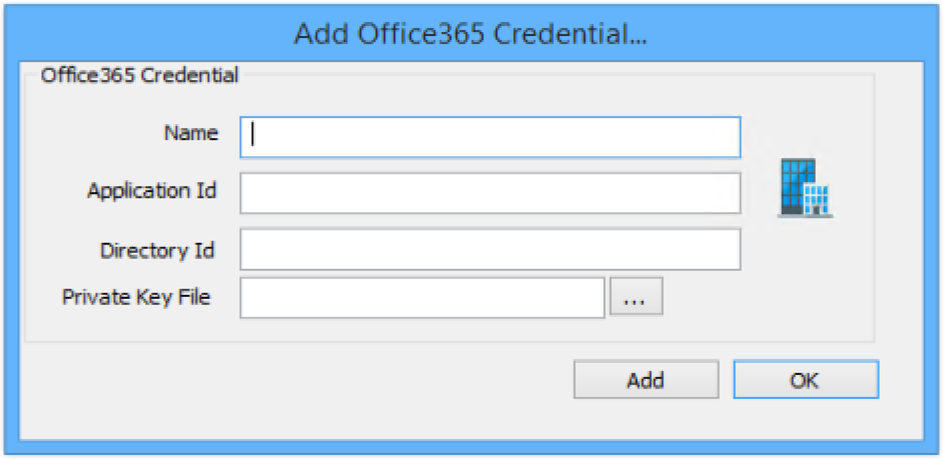
8274f560-7b44-[redacted]

In summary you should have the following:

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

Step 3: Adding the Office 365 Credential

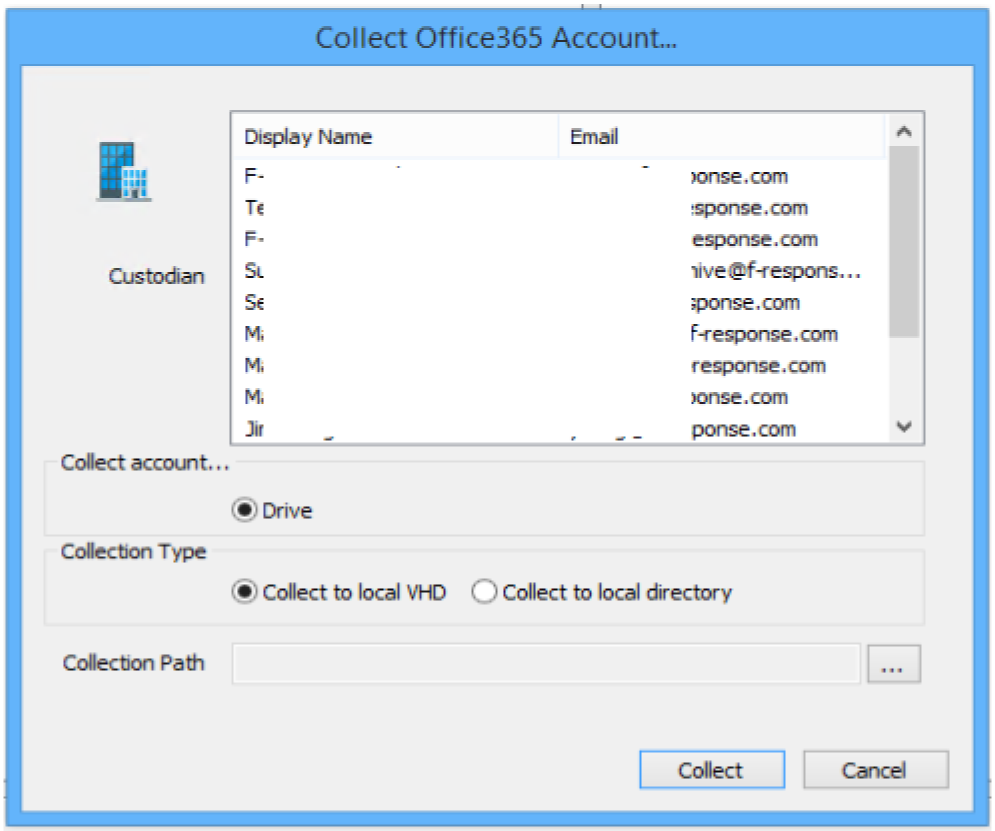
To configure Office365 access you will need to enter the Application Id, Directory Id, and the Private Key file generated earlier.



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.



Collect Office365 Account...

Custodian

Display Name	Email
F-	›onse.com
Te	:sponse.com
F-	esponse.com
Su	›ive@f-respons...
Se	sponse.com
Mi	f-response.com
Mi	response.com
Mi	›onse.com
Jir	ponse.com

Collect account...

● Drive

Collection Type

● Collect to local VHD ○ Collect to local directory

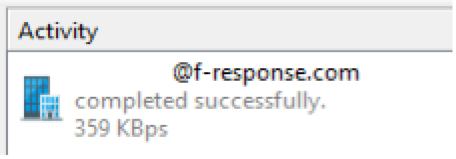
Collection Path

Starting a new collection...

Select the specific user account you would like to collect, and whether you would like to collect the contents to a virtual hard disk or a local directory.

Step 5: Check the Activity Pane

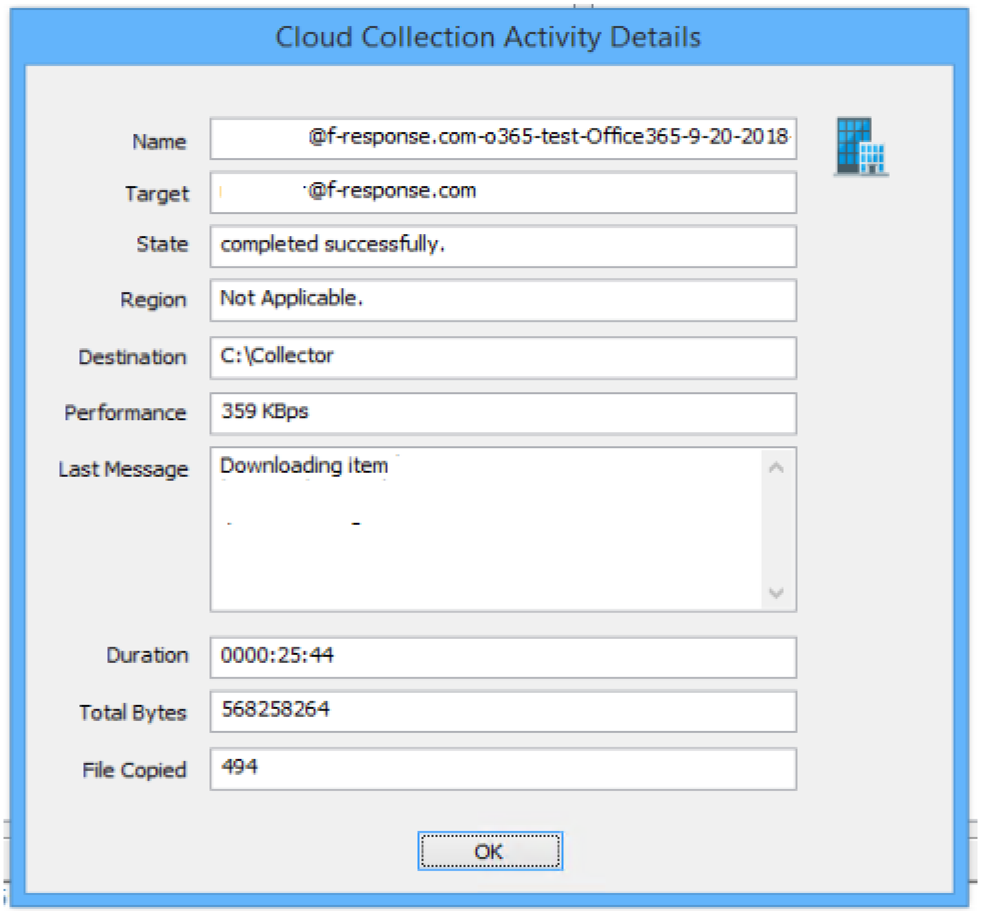
The Activity Pane shows the active collection. Double clicking on the collection will provide additional details.



Activity

@f-response.com
completed successfully.
359 KBps

Activity



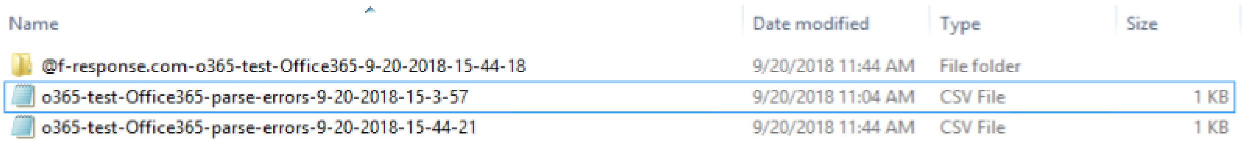
Cloud Collection Activity Details

Name	@f-response.com-o365-test-Office365-9-20-2018
Target	@f-response.com
State	completed successfully.
Region	Not Applicable.
Destination	C:\Collector
Performance	359 KBps
Last Message	Downloading item
Duration	0000:25:44
Total Bytes	568258264
File Copied	494

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.



Name	Date modified	Type	Size
@f-response.com-o365-test-Office365-9-20-2018-15-44-18	9/20/2018 11:44 AM	File folder	
o365-test-Office365-parse-errors-9-20-2018-15-3-57	9/20/2018 11:04 AM	CSV File	1 KB
o365-test-Office365-parse-errors-9-20-2018-15-44-21	9/20/2018 11:44 AM	CSV File	1 KB

Collected items

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