Your Mission: Use F-Response to access Amazon S3 Cloud Storage Buckets

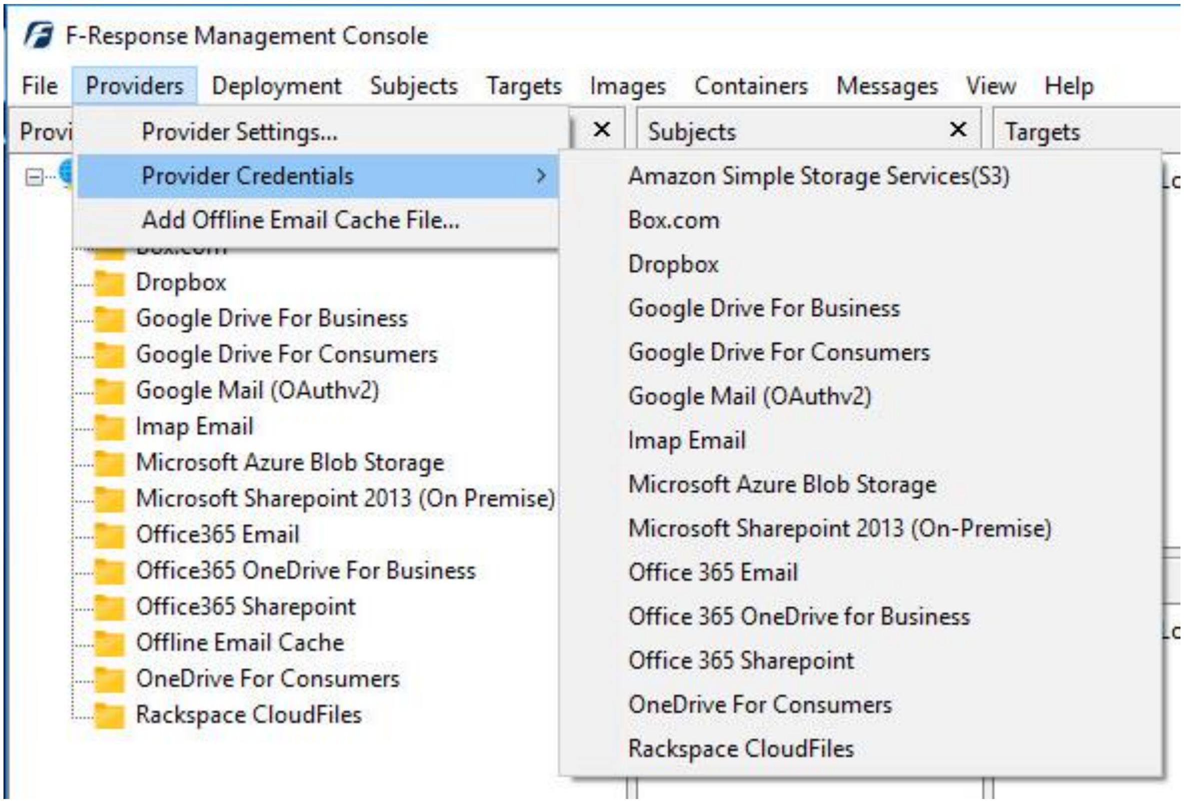
Using F-Response to connect to Amazon S3 Storage Bucket and collect their contents

Important Note

Disclaimer: The F-Response Connector and legacy Connector products (F-Response Email Connector, Cloud Connector, and Database Object Connector) 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.

Step 1: Open Amazon S3 Credential Configuration Window

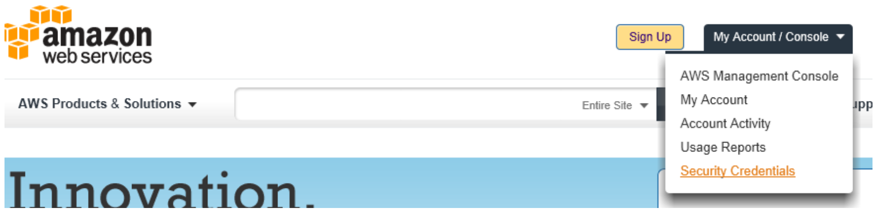
Open the F-Response Management Console and navigate to the Providers->Provider Credentials->Amazon Simple Storage Services (S3) menu item.



F-Response Management Console

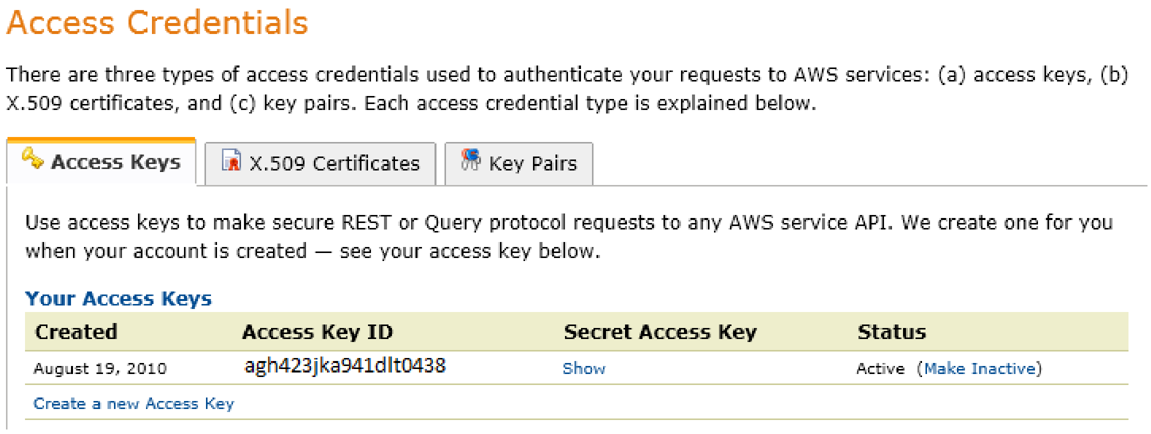
Step 2: Obtain Amazon S3 Credentials

Amazon S3 Storage Credentials are found on the Amazon AWS Console (see **aws.amazon.com**). The specific credentials required are available under the "**Security Credentials**" link under **My Account**, see below:



Amazon Web Services Main Page

Locate the **Access Credentials** section and record (copy/paste) **the Access Key ID**, then click "**Show**" to open a secondary window containing the **Secret Access Key**.



Access Credentials

There are three types of access credentials used to authenticate your requests to AWS services: (a) access keys, (b) X.509 certificates, and (c) key pairs. Each access credential type is explained below.

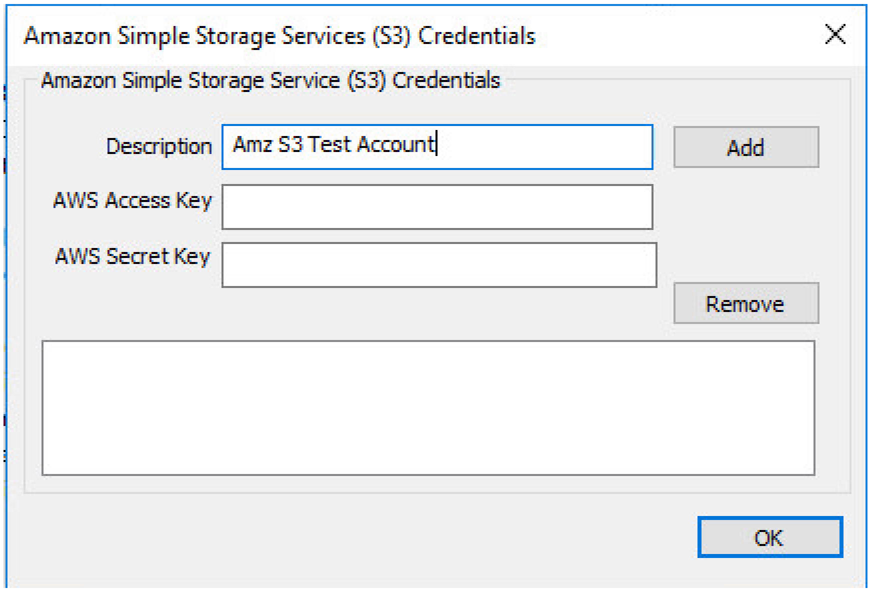
Use access keys to make secure REST or Query protocol requests to any AWS service API. We create one for you when your account is created — see your access key below.

Your Access Keys

Created	Access Key ID	Secret Access Key	Status
August 19, 2010	agh423jka941dlt0438	Show	Active (Make Inactive)
Create a new Access Key			

Amazon AWS Access Key and Secret Access Key

The preceding credentials (Access Key and Secret Key) must be entered in the corresponding fields in the **Configure Amazon S3 Credentials** dialog. The Description field is **not** optional and is used to provide a secondary human readable identifier for the credential set (Ex "Client X Account").


Amazon Simple Storage Services (S3) Credentials
Amazon Simple Storage Service (S3) Credentials
Add
Remove
OK

Description: Amz S3 Test Account

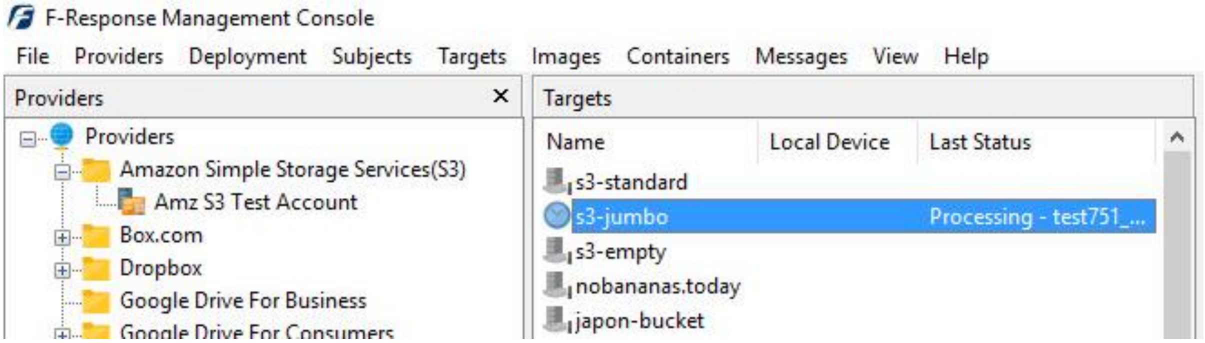
AWS Access Key:

AWS Secret Key:

Configure S3 Credentials

Step 3: Scan and Enumerate Amazon S3 Buckets

Double click on the newly added Amazon S3 account under the Providers tree. This will scan the provider and result in a listing of available targets in the Targets window.



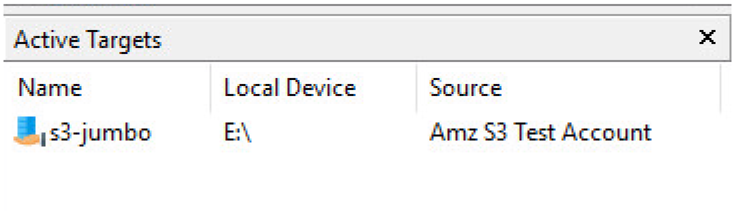
- Providers
  - Amazon Simple Storage Services(S3)
    - Amz S3 Test Account
  - Box.com
  - Dropbox
  - Google Drive For Business
  - Google Drive For Consumers

Name	Local Device	Last Status
s3-standard		
s3-jumbo		Processing - test751_...
s3-empty		
nobananas.today		
japon-bucket		

Listing Targets

Step 4: Login and Mount one or more Amazon S3 Buckets

Double click on an individual target in the Targets window to begin the mounting process. Once attached the share will present a drive letter.



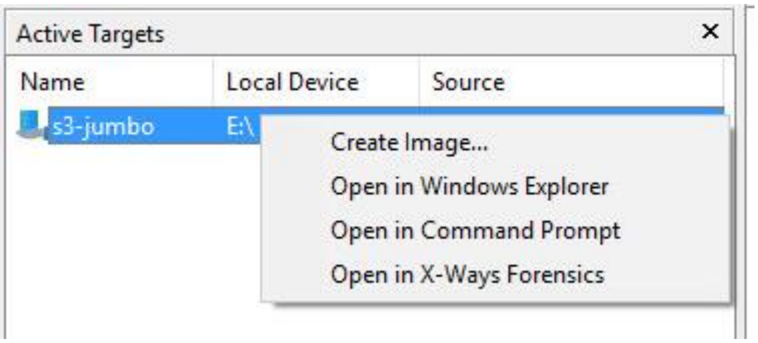
Active Targets

Name	Local Device	Source
s3-jumbo	E:\	Amz S3 Test Account

Attached Volume

Step 5: Create Image of attached volume

Select the newly attached target and right click on it in the Local Device column. Use the “Create Image…” option to open the “Image” dialog to begin imaging the device.

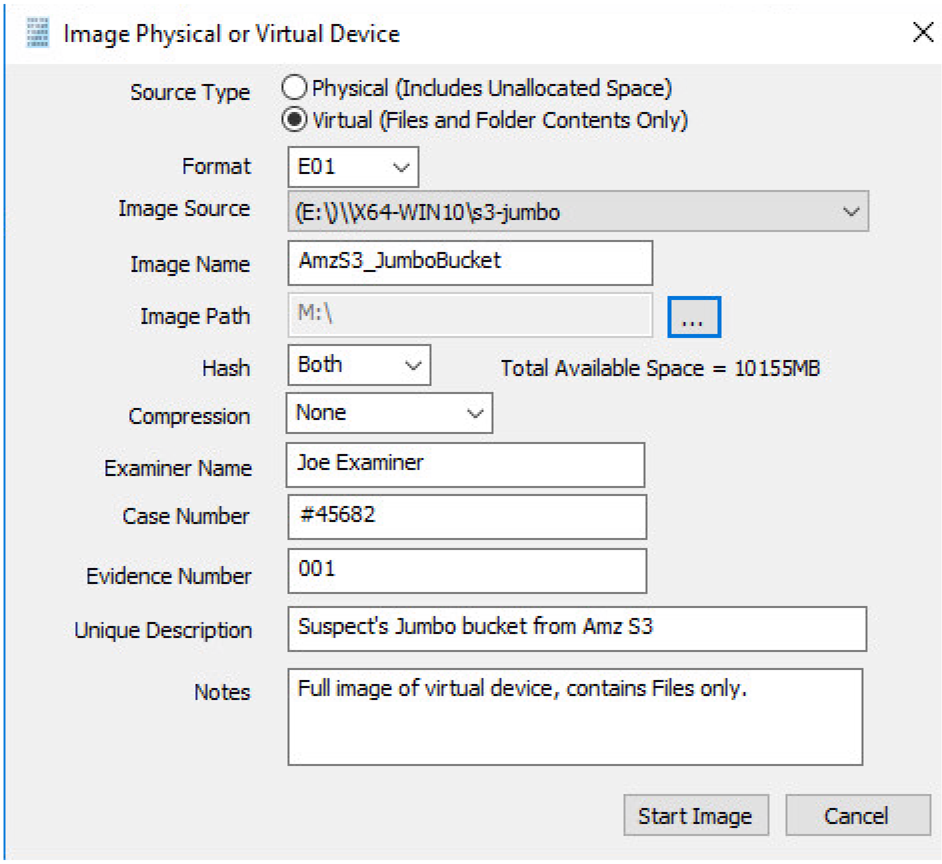


Active Targets

Name	Local Device	Source
s3-jumbo	E:\	

Start Imaging Process…

Step 6: Complete Imaging Options…



Source Type	○ Physical (Includes Unallocated Space) ● Virtual (Files and Folder Contents Only)
Format	E01
Image Source	(E:\)\\X64-WIN10\s3-jumbo
Image Name	AmzS3_JumboBucket
Image Path	M:\
Hash	Both
Compression	None
Examiner Name	Joe Examiner
Case Number	#45682
Evidence Number	001
Unique Description	Suspect's Jumbo bucket from Amz S3
Notes	Full image of virtual device, contains Files only.

Total Available Space = 10155MB

We'll work through this window from the top down. First, the **Source Type** is set to **Virtual** (by default) to be able to create an image of the connected virtual device data.

Next you can select the image **Format**—you have a choice between **E01** (Expert Witness), **VHD** (Virtual Hard Disk), or **Both**. This option determines what the Imager will provide at the end of the collection.

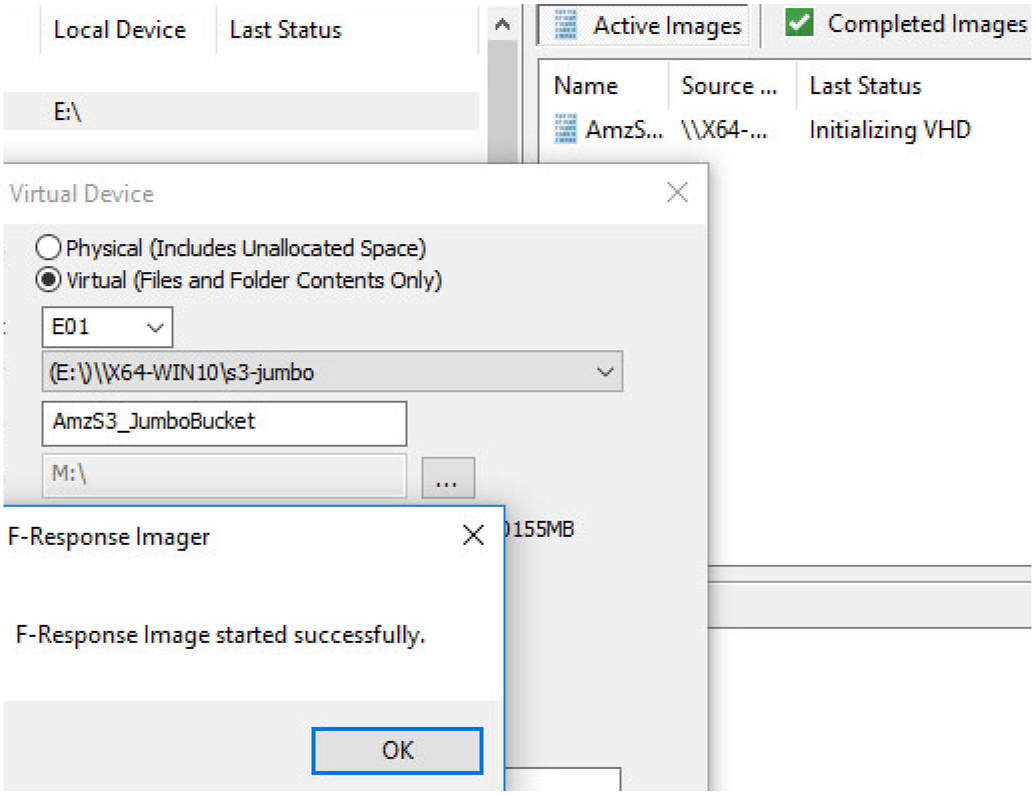
Image Source should be populated if we opened this window from Windows Explorer, just verify that the drive letter is correct from Step 1. For **Image Path** we need to choose our destination drive—this must be a physical drive attached to our examiner machine (we cannot image to a network share).

Next we can choose a **Hash** format and the **Compression** level if you wish to compress the resulting image file. The remaining fields are specific to your case and can be filled out accordingly. These fields will be included in the resulting log file for the image.

Once you have all your information entered simply click the **Start Image** button to begin the process.

Step 7: Review the Image

Once started the dialog will close and you'll be able to monitor the image using the Active Images. When the Image completes you will see it move to Completed Images.



Name	Source ...	Last Status
AmzS...	\\X64-...	Initializing VHD

Virtual Device

○ Physical (Includes Unallocated Space)
● Virtual (Files and Folder Contents Only)

E01

(E:\)\\X64-WIN10\s3-jumbo

AmzS3_JumboBucket

M:\

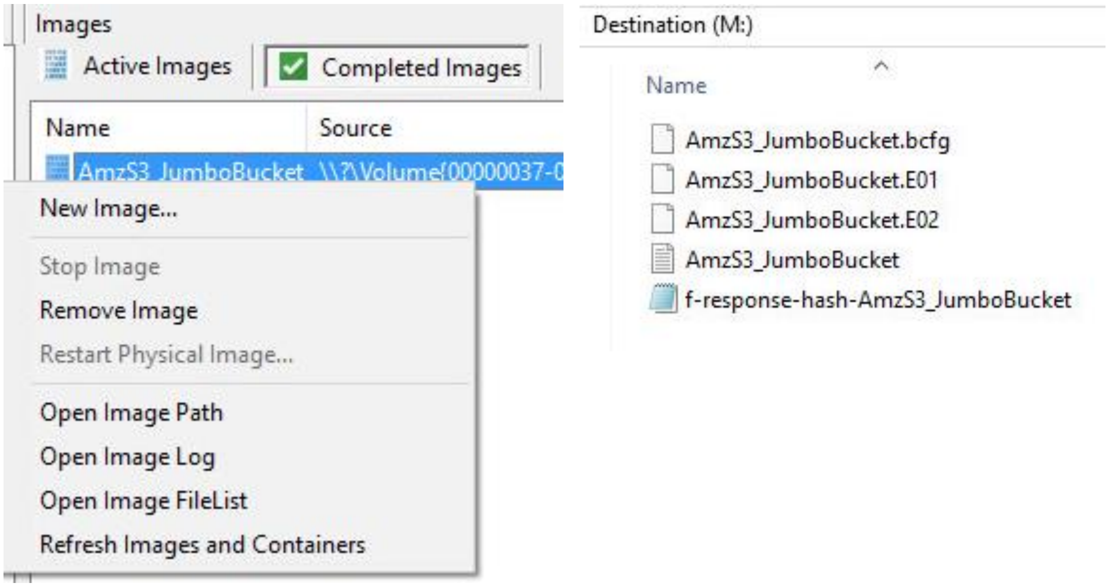
F-Response Imager

F-Response Image started successfully.

Imaging started and running…

Step 8: Review the Completed Image

Right click on the completed image to access the Image Path, Log, and File List. These logs and listings contain details about the image, the image itself, and a file listing of files collected.



Reviewing the completed image.

Troubleshooting

I have valid S3 Credentials however I get no buckets returned, why?

Most likely your computer's clock is too far skewed from the current time. Your examiner machine's clock must be accurate to within 15 minutes of actual time. The time zone is un-important.