REVERSINGLABS

VERSION 1.0.1
May 2023

ReversingLabs API Offer Activation Instructions

Technical Documentation

Last updated: 2023-05-19

Change Log

Version	Changes	Published
1.0.1	Instructions regarding Multi-subscription credentials feature	2023-5-19
1.0	ReversingLabs Enrichment APIs For Sentinel Subscription Activation Instructions	2023-1-26

Table of Contents

Overview

This document is designed to help users install and set up an API subscription for ReversingLabs in the Microsoft Azure Marketplace. The ReversingLabs API allows users to easily integrate threat intelligence data into their existing security systems and workflows. This document will guide users through the process of subscribing to the ReversingLabs API in the Azure Marketplace, including information on prerequisites and any necessary configuration steps. By following the instructions in this document, users will be able to quickly and easily access the powerful threat intelligence capabilities provided by the ReversingLabs API.

Prerequisites

When subscribing to a SaaS offer in the Microsoft Azure Marketplace, some common questions that may be asked include:

Which Azure subscription should I use to purchase this SaaS offer?
You will have to select the subscription you wish to use. If you have multiple subscriptions, you'll have to select the one you want to use.

What are the costs associated with this SaaS offer?
You will have to check the cost of the SaaS offer before subscribing. You can check the pricing details in the offer's page.

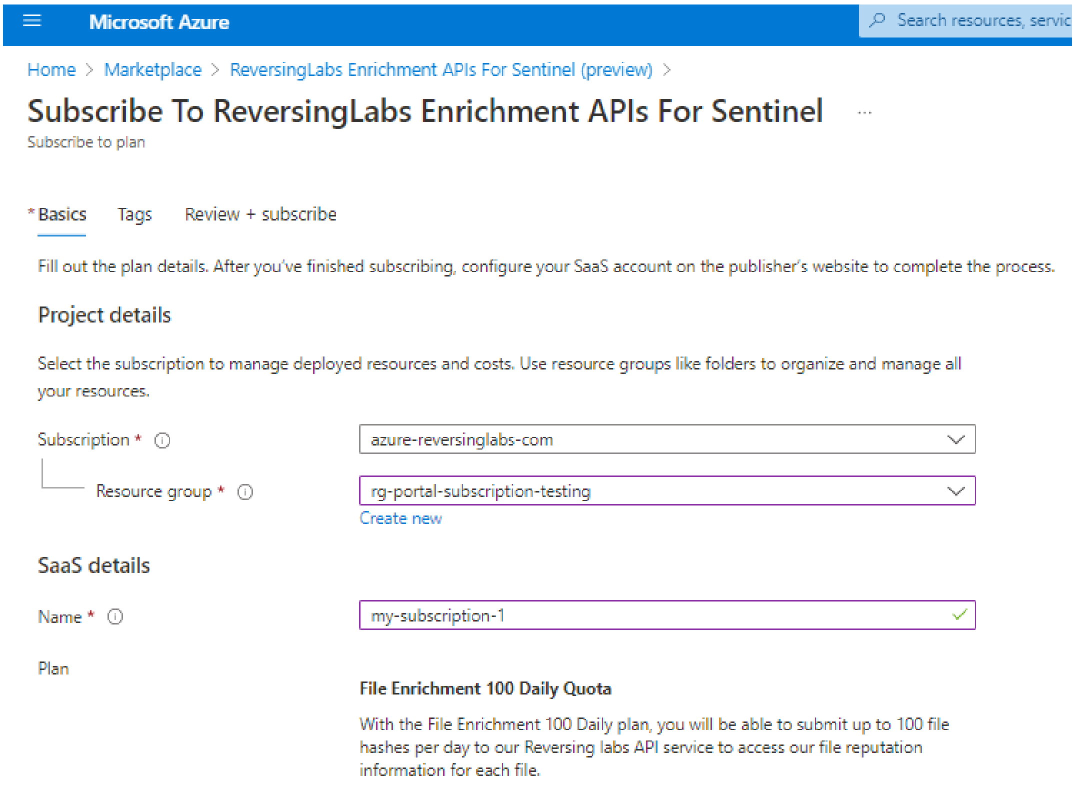
Are there any prerequisites or additional services required for this SaaS offer?
Some SaaS offers may require additional Azure services or configurations to work properly. Make sure to check the requirements for the specific SaaS offer before subscribing.

Are there any limitations or usage restrictions for this SaaS offer?
Some SaaS offers may have usage restrictions or quota limitations, such as limits on the number of daily or monthly calls, files, records or storage. Make sure to check the terms of use for the specific SaaS offer before subscribing.

How can I manage and cancel my subscription?
Once you have subscribed to a SaaS offer, you will be able to manage it through the Azure portal. You'll be able to cancel the subscription by going to the subscription's details page and cancel it.

Getting Started

Subscribing to the Marketplace Offer



Subscribe To ReversingLabs Enrichment APIs For Sentinel

Subscribe to plan

Fill out the plan details. After you've finished subscribing, configure your SaaS account on the publisher's website to complete the process.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : azure-reversinglabs-com

Resource group * : rg-portal-subscription-testing

SaaS details

Name * : my-subscription-1 ✓

Plan

File Enrichment 100 Daily Quota

With the File Enrichment 100 Daily plan, you will be able to submit up to 100 file hashes per day to our Reversing labs API service to access our file reputation information for each file.

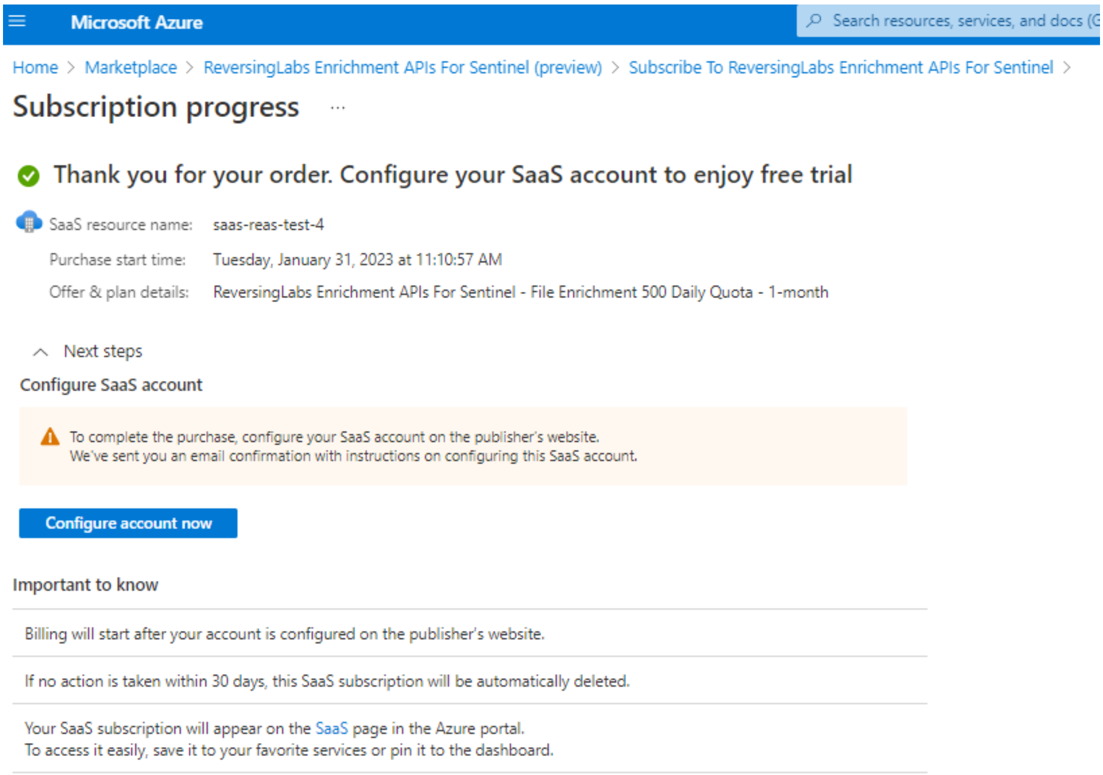
Here are the general steps for subscribing to a SaaS offer in the Microsoft Azure Marketplace:

1. Sign in to the Azure portal (https://portal.azure.com/) using your Microsoft account.
2. In the left-hand navigation menu, click on "Marketplace."
3. Use the search bar at the top of the page to find the SaaS offer you want to subscribe to, such as "ReversingLabs Enrichment APIs For Sentinel."
4. Click on the offer to view its details and then click "Get it now."
5. On the "Subscribe to Plan" page, select a plan and click "Subscribe."
6. Choose the Azure subscription and resource group you want to use for the SaaS offer or create new ones if necessary. (see image above)

7. Enter a unique resource name to identify the SaaS subscription (e.g. *my-saas-subscription-1*).
8. Follow the prompts to complete the subscription process and any necessary configuration steps.
9. Click "Review and Subscribe" and/or "Subscribe" when ready.
10. Follow the Activating Subscription instructions below.

Once the process is complete, you can access the SaaS offer through the Azure portal.

Activating a New Subscription



Home > Marketplace > ReversingLabs Enrichment APIs For Sentinel (preview) > Subscribe To ReversingLabs Enrichment APIs For Sentinel >

Subscription progress ...

Thank you for your order. Configure your SaaS account to enjoy free trial

SaaS resource name: saas-reas-test-4

Purchase start time: Tuesday, January 31, 2023 at 11:10:57 AM

Offer & plan details: ReversingLabs Enrichment APIs For Sentinel - File Enrichment 500 Daily Quota - 1-month

Next steps

Configure SaaS account

To complete the purchase, configure your SaaS account on the publisher's website.
We've sent you an email confirmation with instructions on configuring this SaaS account.

Important to know

Billing will start after your account is configured on the publisher's website.

If no action is taken within 30 days, this SaaS subscription will be automatically deleted.

Your SaaS subscription will appear on the SaaS page in the Azure portal.
To access it easily, save it to your favorite services or pin it to the dashboard.

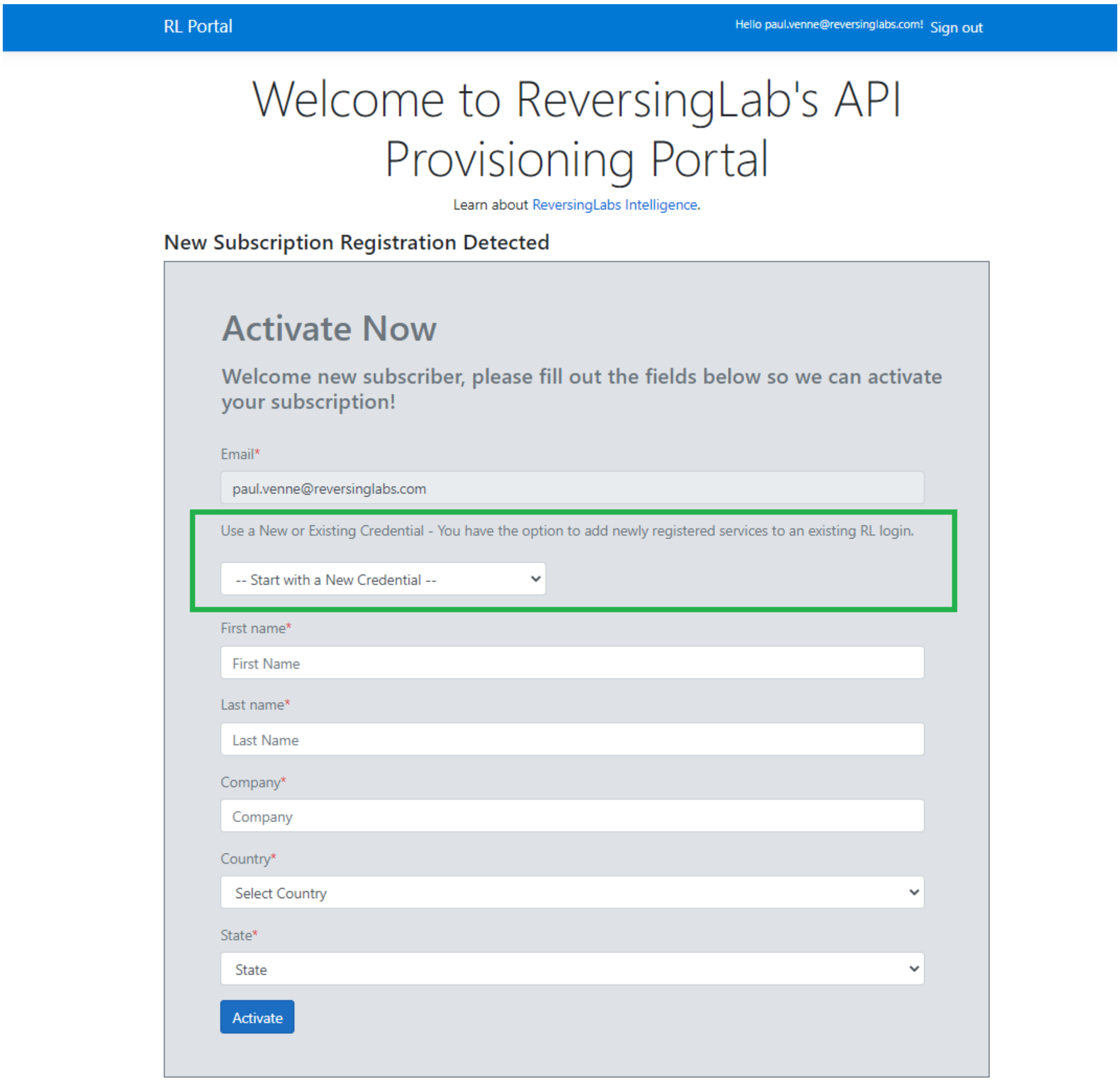
To activate your SaaS subscription after subscribing to an offer in the Microsoft Azure Marketplace:

1. Click "Configure account now" from the SaaS subscription's Azure Marketplace portal, which will launch the **ReversingLab's API Provisioning Portal** in a new tab or page. (see image below).

2. Log in using the same **Microsoft account** used to purchase the SaaS subscription offer.

3. Activate the subscription by following the prompts on the provisioning portal by providing the required information and pressing the **Activate** button. (see image below)

4. If you already have an Azure Microsoft Subscription linked to RL login credentials, you will see a dropdown with options (as shown in the green box below) to add the newly subscribed subscription services to an existing RL Login account or select "Create New Credential" to start fresh with a new RL login unlinked to any previous subscriptions. These options are available during the registration process. To remove services from a credential, simply unsubscribe from the relevant Azure Marketplace subscriptions.



RL Portal

Hello paul.venne@reversinglabs.com! Sign out

Welcome to ReversingLab's API Provisioning Portal

Learn about ReversingLabs Intelligence.

New Subscription Registration Detected

Activate Now

Welcome new subscriber, please fill out the fields below so we can activate your subscription!

Email*

paul.venne@reversinglabs.com

Use a New or Existing Credential - You have the option to add newly registered services to an existing RL login.

-- Start with a New Credential --

First name*

First Name

Last name*

Last Name

Company*

Company

Country*

Select Country

State*

State

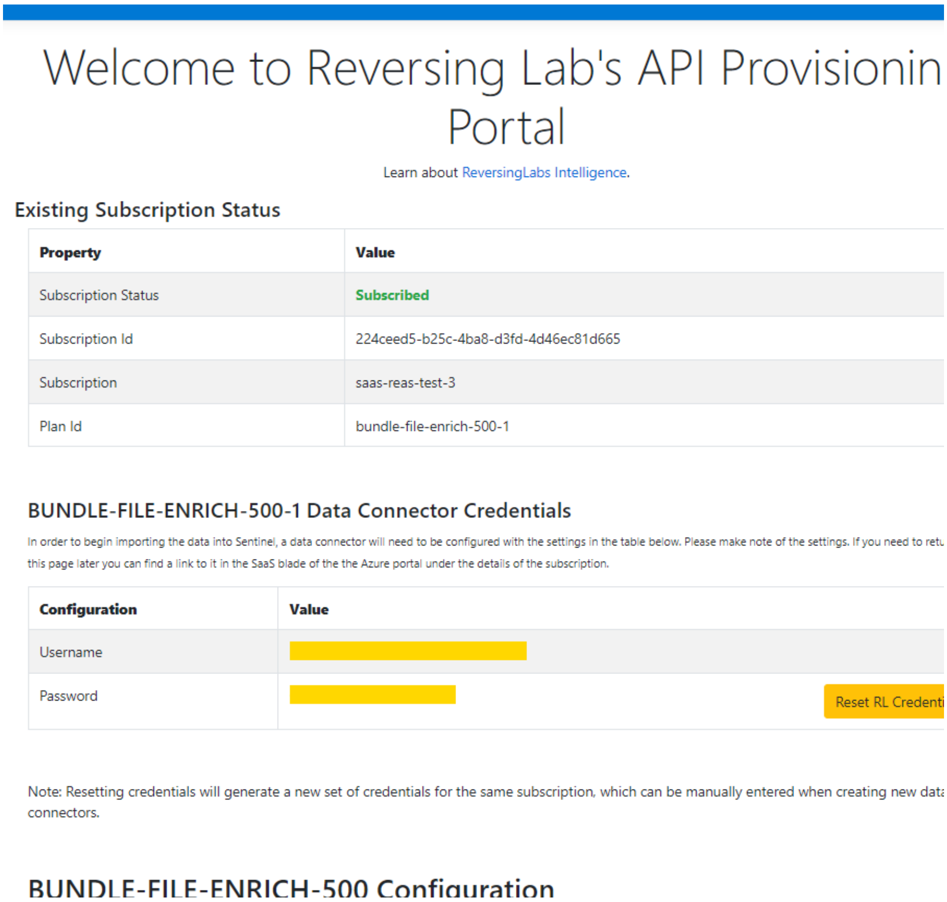
Activate

5. Review the status page, which should include the subscription status, plan chosen, and credential information needed to access the API services. A green “Subscribed” status indicates the activation process is complete. A page refresh may be required to update the status. (see image below).

6. You may choose to use the credential for all the products/services within the offer or you can reset the password if needed by pressing the “Reset RL Password” button to the right.

7. Access your subscriptions and their details, including the offer subscribed to, from the Azure Portal. From there, manage, cancel, and renew your subscription.

Using the ReversingLabs API Credentials



Welcome to Reversing Lab's API Provisionin
Portal

Learn about ReversingLabs Intelligence.

Existing Subscription Status

Property	Value
Subscription Status	Subscribed
Subscription Id	224ceed5-b25c-4ba8-d3fd-4d46ec81d665
Subscription	saas-reas-test-3
Plan Id	bundle-file-enrich-500-1

BUNDLE-FILE-ENRICH-500-1 Data Connector Credentials

In order to begin importing the data into Sentinel, a data connector will need to be configured with the settings in the table below. Please make note of the settings. If you need to retu
this page later you can find a link to it in the SaaS blade of the the Azure portal under the details of the subscription.

Configuration	Value
Username	[redacted]
Password	[redacted] Reset RL Credenti

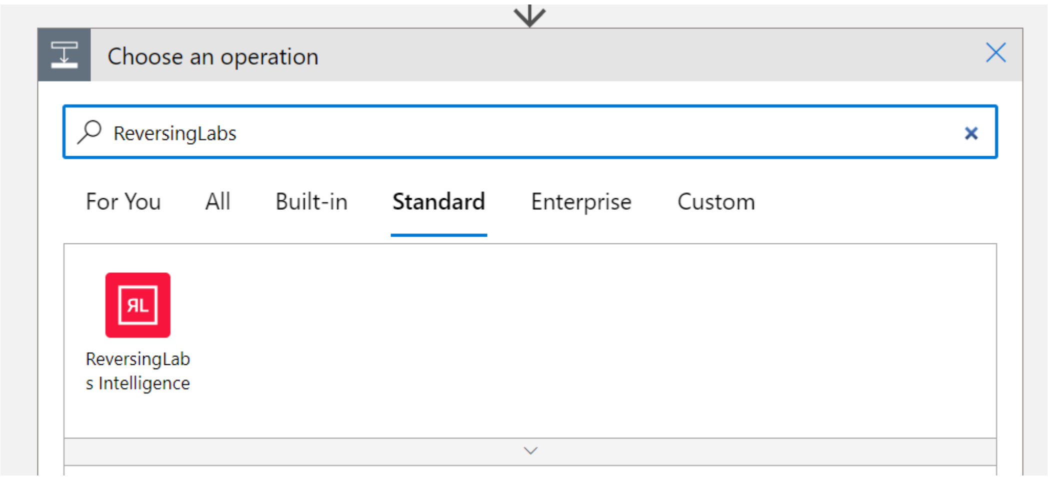
Note: Resetting credentials will generate a new set of credentials for the same subscription, which can be manually entered when creating new data
connectors.

BUNDLE-FILE-ENRICH-500 Configuration

Use the username and password on the ReversingLabs subscription status page to access the API services you have subscribed to. The page will also have information about each product and service, including instructions if available.

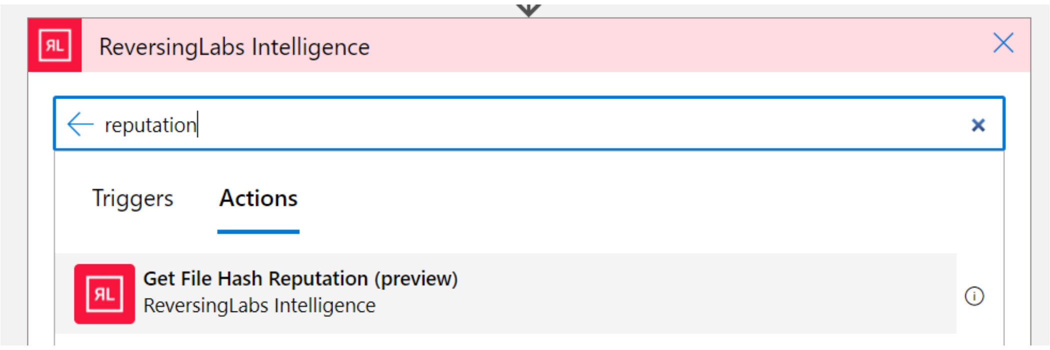
RECOMMENDED: It is strongly suggested to install the free "ReversingLabs Sentinel Content Hub" in order to fully utilize the API services and gain valuable insights into your threat intelligence implementation and the impact of ReversingLabs intelligence and automation on your operations located here: https://reversinglabs-marketplace.azureedge.net/help/ReversingLabsSentinelContentHubInstall.pdf

To integrate the enrichment APIs into your own playbooks, you'll need to configure a new API Connection for the ReversingLabs Intelligence Logic App connector. To do this, open the playbook designer in a new or existing playbook, add a new step, and select the ReversingLabs Intelligence connector.



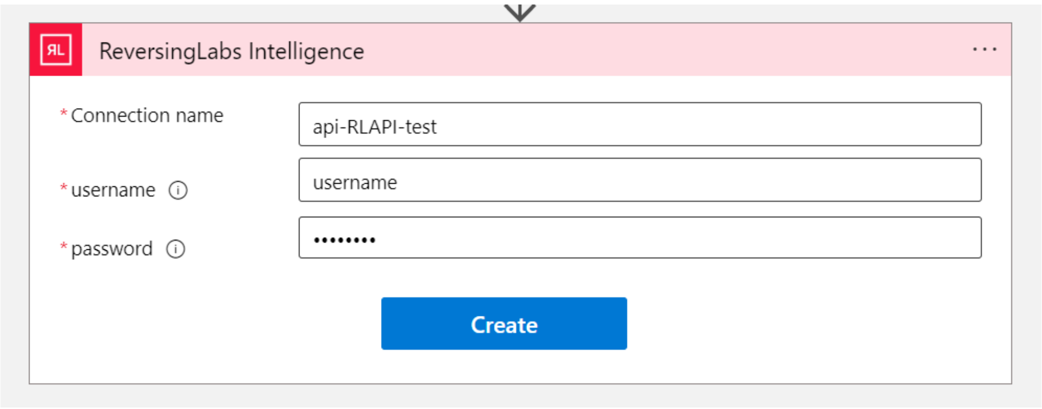
ReversingLabs

Next, select the “Get File Hash Reputation (preview)” action (this uses the TCA-0101 API):


ReversingLabs Intelligence
Triggers
Actions
Get File Hash Reputation (preview)
ReversingLabs Intelligence

reputation

After selecting the action, you’ll need to create the API connection. Provide a name for the connection, enter the username and password provided after activating your subscription in the steps above, then click the “create” button.

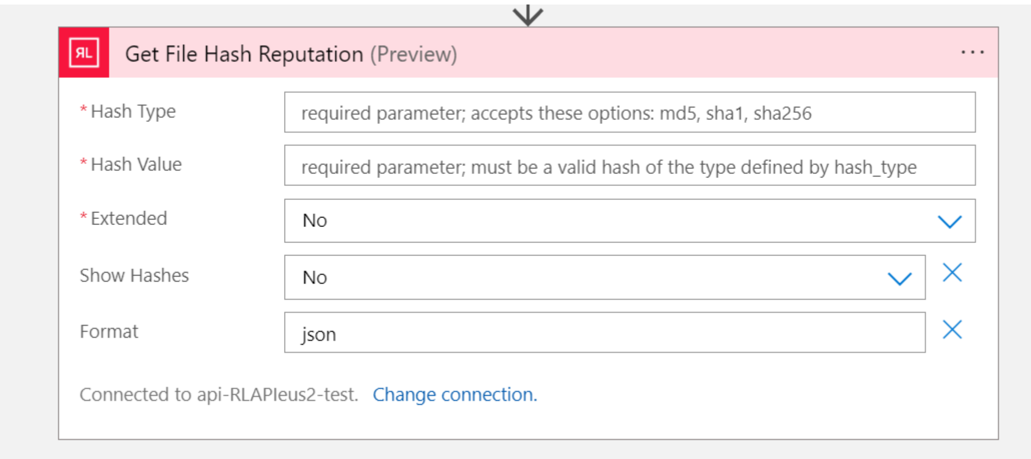


*Connection name	api-RLAPI-test
*username	username
*password	••••••••

TCA-0101 / Get File Hash Reputation

The "Get File Hash Reputation" action takes the following input:

Field	Description	Required
Hash Type	a string that matches the algorithm for the submitted hash (md5/sha1/sha256)	Yes
Hash Value	a string matching the file hash to be submitted	Yes
Extended	select the default value "No" to only return the file reputation classification value. Select "Yes" to return additional information such as trust factor and threat level values; malware type, family name, and platform; first and last seen times, and more	Yes
Show Hashes	select the default value "No" to exclude hash values in the associated results. Select "Yes" to include the submitted hash values in the returned results.	No
Format	a string matching the format for the results to be returned in. Accepted values are "json" or "xml"	No

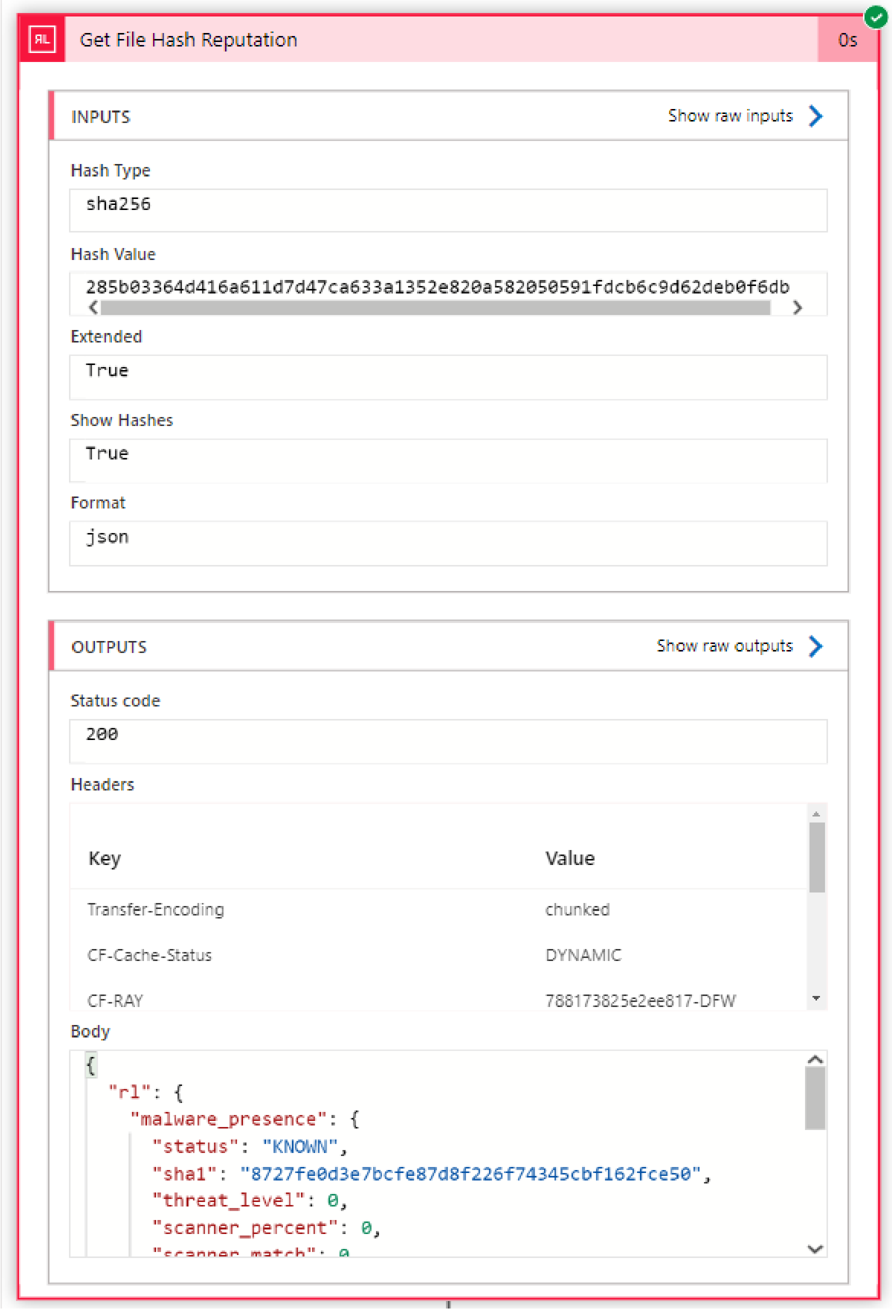


Get File Hash Reputation (Preview)

* Hash Type	required parameter; accepts these options: md5, sha1, sha256
* Hash Value	required parameter; must be a valid hash of the type defined by hash_type
* Extended	No
Show Hashes	No
Format	json

Connected to api-RLAPIeus2-test. Change connection.

The expected output of a successful action returns a 200 status code:



Hash Type
sha256

Hash Value
285b03364d416a611d7d47ca633a1352e820a582050591fdcb6c9d62deb0f6db

Extended
True

Show Hashes
True

Format
json

Status code
200

Headers

Key	Value
Transfer-Encoding	chunked
CF-Cache-Status	DYNAMIC
CF-RAY	788173825e2ee817-DFW

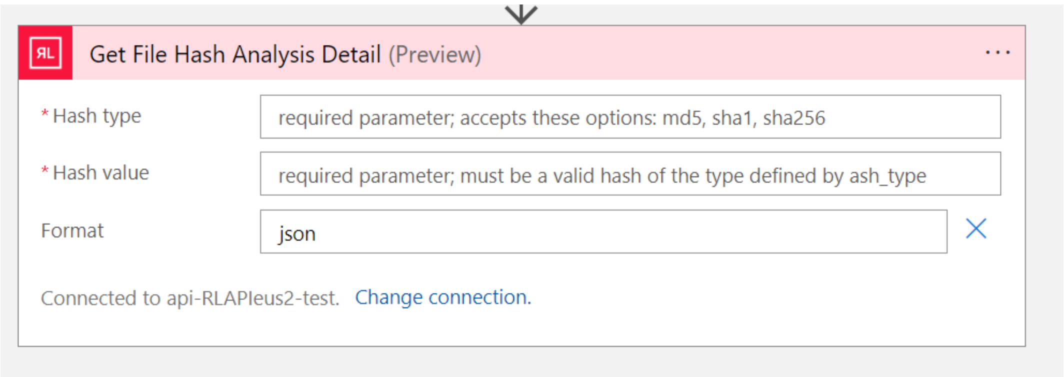
Body

```
{
  "rl": {
    "malware_presence": {
      "status": "KNOWN",
      "sha1": "8727fe0d3e7bcfe87d8f226f74345cbf162fce50",
      "threat_level": 0,
      "scanner_percent": 0,
      "scanner_match": 0
```

TCA-0104 / Get File Hash Analysis Detail

The “Get File Hash Analysis Detail” action takes the following input:

Field	Description	Required
Hash Type	a string that matches the algorithm for the submitted hash (md5/sha1/sha256)	Yes
Hash Value	a string matching the file hash to be submitted	Yes
Format	a string matching the format for the results to be returned in. Accepted values are “json” or “xml”	No



Get File Hash Analysis Detail (Preview)

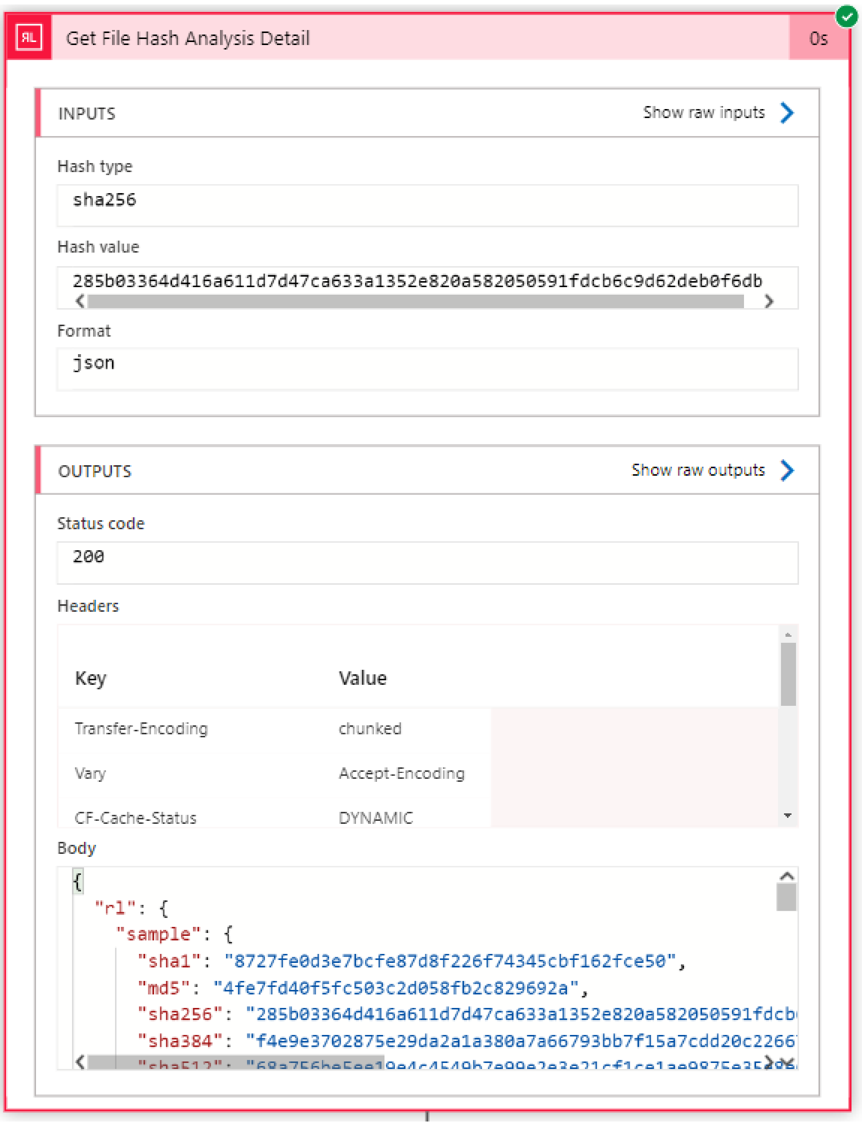
* Hash type: required parameter; accepts these options: md5, sha1, sha256

* Hash value: required parameter; must be a valid hash of the type defined by ash_type

Format: json

Connected to api-RLAPIeus2-test. Change connection.

The expected output of a successful action returns a 200 status code:



Get File Hash Analysis Detail

INPUTS

Hash type
sha256

Hash value
285b03364d416a611d7d47ca633a1352e820a582050591fdcb6c9d62deb0f6db

Format
json

OUTPUTS

Status code
200

Headers

Key	Value
Transfer-Encoding	chunked
Vary	Accept-Encoding
CF-Cache-Status	DYNAMIC

Body

```
{
  "rl": {
    "sample": {
      "sha1": "8727fe0d3e7bcfe87d8f226f74345cbf162fce50",
      "md5": "4fe7fd40f5fc503c2d058fb2c829692a",
      "sha256": "285b03364d416a611d7d47ca633a1352e820a582050591fdcb
      "sha384": "f4e9e3702875e29da2a1a380a7a66793bb7f15a7cdd20c2266
      "sha512": "68a756be5ee19e4c4549b7e99e2e3e21cf1ce1ae9875e35
```

Common errors

The following describes some of the common errors seen when using the playbooks actions listed above:

Error	Description	Resolution
400	The 400 response typically means there was an issue with the request format.	Check the request for any typos, missing/incorrect fields
404	The 404 response means reputation information for the submitted file hash does not yet exist in TitaniumCloud.	N/A - we recommend submitting the file for static and dynamic analysis.

Frequently Asked Questions

When subscribing to a SaaS offer in the Microsoft Azure Marketplace, some common questions that may be asked include:

Which Azure subscription should I use?
You can select the subscription you wish to use from the available options.

What are the costs associated with this SaaS offer?
The pricing details can be found on the offer's page before subscribing.

Are there any prerequisites or additional services required for this SaaS offer?
Some SaaS offers may require additional Azure services or configurations. Make sure to check the requirements for the specific SaaS offer before subscribing.

Are there any limitations or usage restrictions for this SaaS offer?
Some SaaS offers may have usage restrictions or limitations, such as limits on the number of users or data storage. Make sure to review the terms of use for the specific SaaS offer before subscribing.

How can I manage and cancel my subscription?
You can manage and cancel your subscription through the Azure portal. Go to the subscription's details page and cancel it.

How do I know if an offer is compatible with my current Azure setup?
You can check the system requirements and compatibility information for the specific SaaS offer before subscribing.

Can I try the SaaS offer before subscribing?
Some SaaS offers may have a free trial or demo version available. Make sure to check the offer's page for any such options.

How will I be billed for the SaaS offer?
The billing method and frequency for the SaaS offer will be specified on the offer's page before subscribing. Billing will be prorated based on daily usage.

Can I scale my subscription as my usage needs change?
Some SaaS offers may allow you to scale your subscription up or down as your usage needs change. Make sure to check the offer's page for any such options.

Can I transfer my subscription to another Azure tenant or account?
Some SaaS offers may allow you to transfer your subscription to another tenant or account. Make sure to check the offer's page for any such options.

How will I receive support for the SaaS offer?
The support options and contact information for the SaaS offer will be specified on the offer's page before subscribing.

What should I do if I receive an error message while subscribing?
The error message should provide information on what went wrong and how to resolve the issue. If the error message is not clear, you can reach out to the publisher's support team for assistance.

What should I do if I am unable to complete the subscription process?
Double-check that you've followed all the steps correctly and that you have met all the prerequisites or additional services required for the SaaS offer. You can reach out to the publisher's support team for assistance if the issue persists.

What should I do if I am unable to access the SaaS offer after subscribing?
Make sure that your subscription is active and that you are logged in with the correct credentials. Double-check that your subscription is associated with the correct resource group and subscription instance name. You can reach out to the publisher's support team for assistance if the issue persists.

What should I do if I am experiencing unexpected behavior or errors when using the SaaS offer? Check the offer's documentation and troubleshooting guides for potential solutions. You can also reach out to the publisher's support team for assistance.

What should I do if I am experiencing performance issues with the SaaS offer?
Check the offer's documentation and troubleshooting guides for potential solutions. You can also reach out to the publisher's support team for assistance.

What should I do if I need to see my RL credentials / login username and password again?
Go to the subscription's details page and click on the "*Open SaaS Account on publisher's site*" link to view the **ReversingLab's API Provisioning Portal**. Your RL login credentials will be visible by clicking or hoving your cursor on the yellow **username** and **password** fields in the middle of the page.

What should I do if I need to reset my RL login password?
Go to the subscription's details page and click on the "*Open SaaS Account on publisher's site*" link to view the **ReversingLab's API Provisioning Portal**. The **Reset RL Password** button is to the right of the RL login credentials fields in the middle of the page.

Support

If you have any questions, please contact ReversingLabs support at: support@reversinglabs.com.