RiskIQ-Data-PassiveDns playbook (From RiskIQ Illuminance Solution)

Last updated by | Paulo Santana | Mar 30, 2023 at 7:51 PM CDT

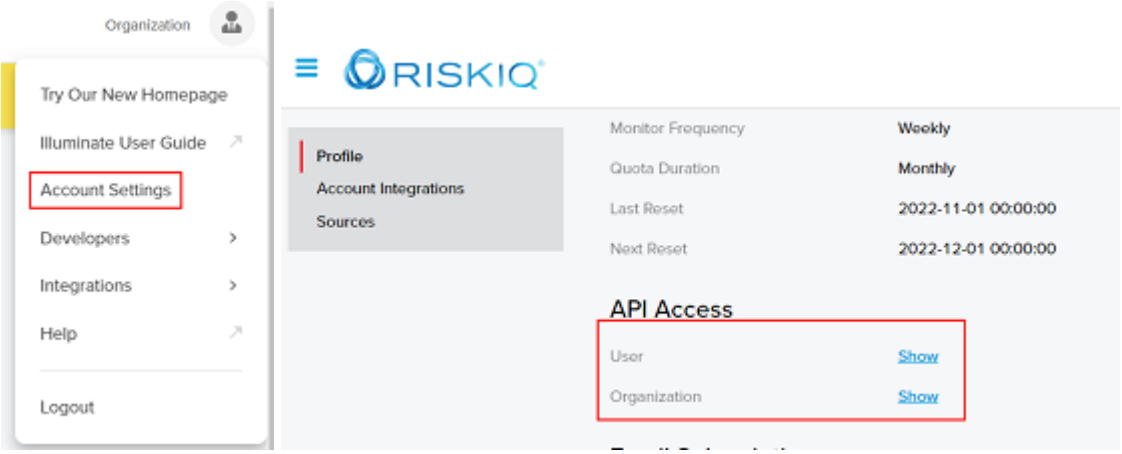
Summary:
When customers install the RiskIQ Illuminance Sentinel solution, it will create the RiskIQ-Data-PassiveDns playbook. This connector requires API credentials from RiskIQ (now DefenderTI).

There is no documentation in the solution or connector on how to get the API credentials, so customers might google RiskIQ API and be directed to the wrong website (riskiq.net)

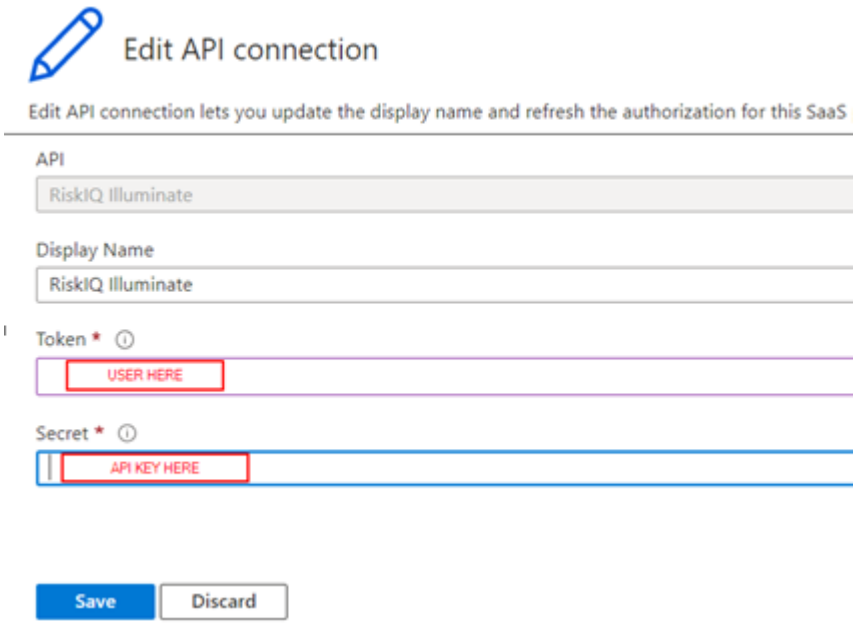
Solution:
Create a RiskIQ PassiveTotal free account using the link below (make sure there is a "/" at the end):

https://community.riskiq.com/registration/

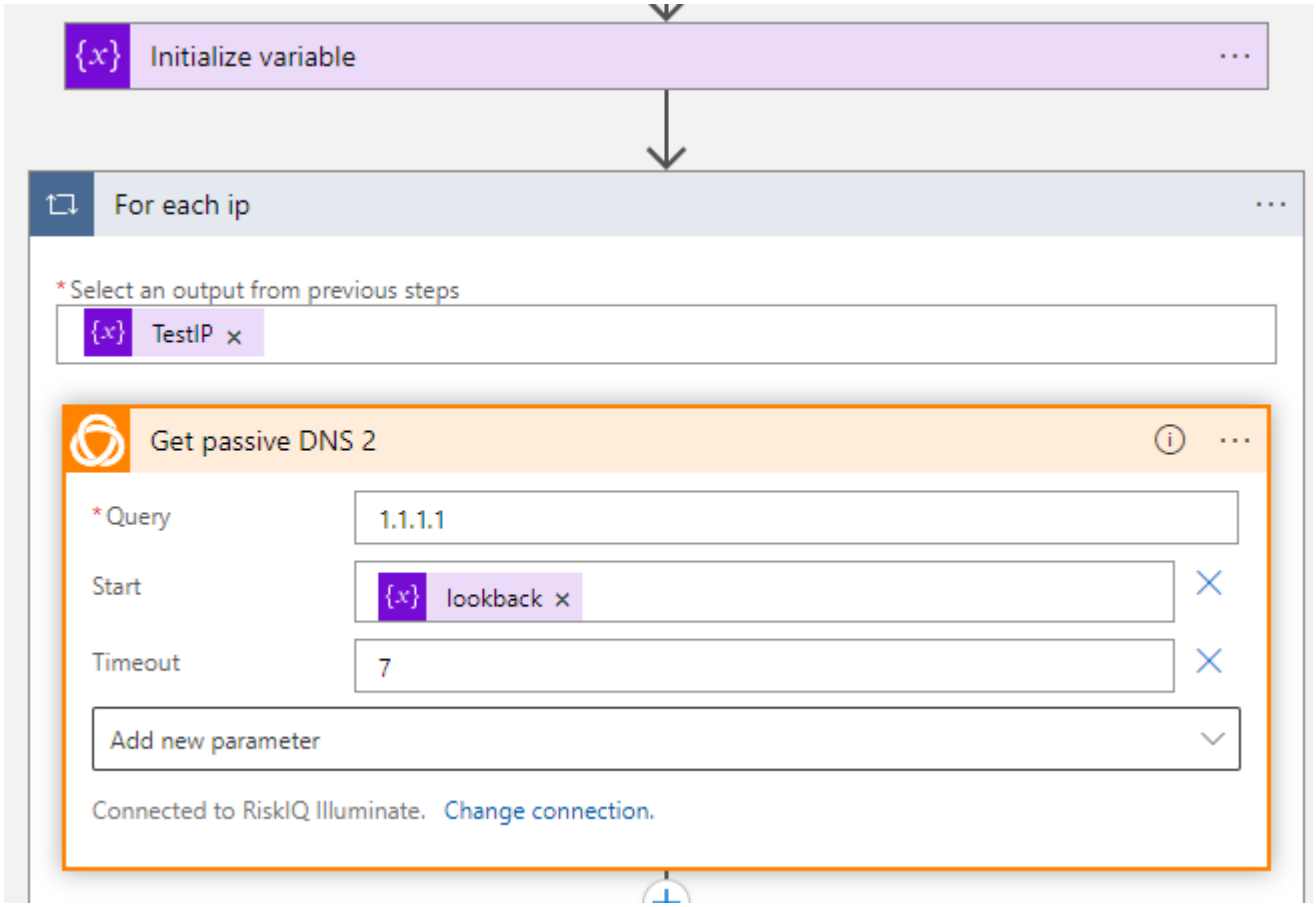
Once you have the account, navigate to Organization > Account Settings > API



Navigate to **Azure Portal > Logic Apps > RiskIQ-Data-PassiveDns > API Connections > riskiq-shared > Edit API connection > enter new API credentials as below:**



Testing:
An easy way to test this playbook is to attach it to an Analytic rule and edit the Logic App to check for a sample IP like below:



Contributor Name	Details	Date
Paulo Santana	Created this section	2022-11-10