# THREAT STACK

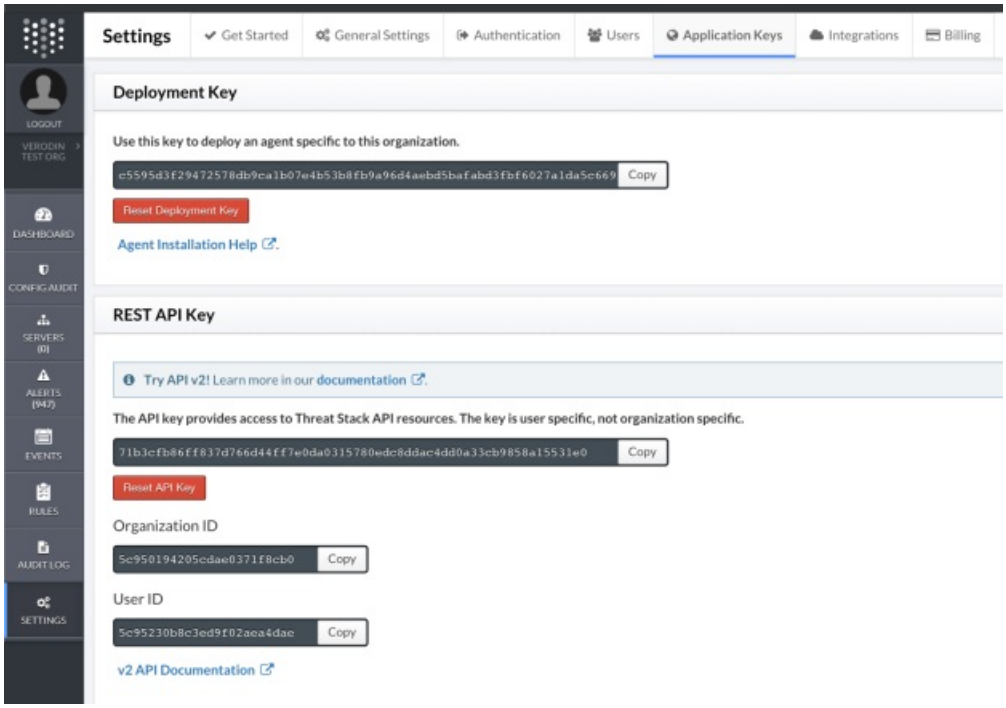
> This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview (https://docs.mandiant.com/home/msv-integrations-overview)**.

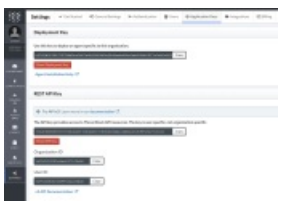
## Generate an API key for Threat Stack

API tokens are tied to user accounts and inherit the user's privileges. When capturing the API key, use an account with the necessary privileges. Read permissions are required, at minimum.

***TO GENERATE AN API KEY FOR THREAT STACK***

1. Log into Threat Stack and bring up the main settings.
2. Select **Application Keys** from the menu.
3. From the **Rest API Key** section, copy the API Key, Organization ID, and User ID for use when creating the Validation Platform integration.
    a. Each user receives their own, unique API token.
    b. This token has the same power and privileges attached to your user and does not expire.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cec35e07dc756be50aa1d/n/threatstack-keys.png)

Threat Stack REST API key

## Update the Validation Platform

### Prerequisites

Information to gather before you start:

- API key for Threat Stack.
- IP address or FQDN used to access Threat Stack.

### Configuration

***TO ADD THE THREAT STACK INTEGRATION***

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Threat Stack**.
3. Complete the general information to add the Threat Stack integration.

   The Host, Port, and Protocol have default values. Do not change these unless directed to do so by Threat Stack or Validation Platform.

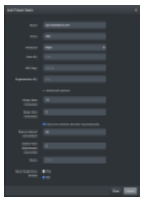
   a. Enter the **User ID** you copied from Threat Stack.
   b. Enter the **API Key** you copied from Threat Stack.
   c. Enter the **Organization ID** you copied from Threat Stack.

4. Expand **Advanced options**.
5. (Optional) Update **Query time** and **Delay time**.

   The **Query time** is the amount of time (minutes) before and after the query runs that the looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the query after a Job Action. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

   If your monitors are set to run more frequently than the query time, it will impact the pass/fail results for AEDA monitors.

6. (Optional) Clear **Discover network devices automatically**.
7. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
8. (Optional) Assign a **Name**.
9. (Optional) Choose **Yes** to save suspicious events.
10. Click **Submit**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629cec35e07dc756be50aa1b/n/threatstack.png)

Threat Stack Integration

## Verify connectivity

***TO VERIFY CONNECTIVITY TO THREAT STACK***

Click **Test** to verify that:

- The Director can communicate with the Threat Stack host on the port specified.
- The API key is working and has the necessary privileges .