Mandiant

F5 THREAT STACK INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to F5 Threat Stack to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to F5 Threat Stack to test the efficacy and configuration of security controls using Security Validation jobs

Use this document to configure the integration using one of the following methods:

- MSI (Supported and recommended for new integration configurations)
- Legacy (Supported for existing integration configurations)

Configure MSI Integration

This method is the recommended approach for configuring new integrations in Security Validation.

API Calls

API	Usage
`/help/hawk/self-test`	Used to test connectivity and authentication settings
`/v2/alerts`	Retrieve a list of alerts from F5 Threat Stack
`/v2/alerts/{alert_id}/events`	Retrieve a list of events for a specific alert from F5 Threat Stack
`/v2/agents/{agent_id}`	Retrieve detailed information about a specific agent

Supported Versions

F5 Threat Stack API v2

Before You Begin

To configure this integration, you need:

- The hostname or IP address of your F5 Threat Stack instance
- API Key
- Organization ID
- User ID

Retrieve API Key and IDs

1. Log into the Threat Stack app.
2. Navigate to Settings, then to the Application Keys tab.

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > F5 Threat Stack**.

   You can add this as either a Direct or Remote Integration.
3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all

outbound connections go through a proxy, first, set up a **Proxy Rule** (https://docs.mandiant.com/home/msv-proxy-rules).

5. Change the **HttpProtocols** to use for requests. (**Https** or **Http**.)
6. For the **Host**, enter the hostname of your F5 Threat Stack instance.
7. Enter a **Port** value. The default is **443**.
8. Enter the **Api Key**, **Organization Id**, and **User Id** values that you retrieved from the Threat Stack app.
9. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
10. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
11. Optional: Modify the **Field Map** values, as necessary.

    - Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
    - When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

12. Optional: Expand **Advanced options** and update the information as necessary.
    a. Update **Query Time** and **Delay Time**.

    The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. 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, this configuration impacts the pass/fail results for AEDA monitors.

    b. Update **Query Interval** (seconds).
    c. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    d. Modify the **Correlation Query Interval**, if necessary (minutes).
    e. Select **Discover network devices automatically**, the default and recommended option.

    If unselected, reported events won't include product information for any matching network security technology.

    f. Select **Save Suspicious Events**.
    g. Modify the **Event Time Adjustment** (seconds). The default is **0**.
    h. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

13. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click ⋮ **> Test** to verify that:
    - The Director can communicate with the integration host on the port and protocol specified.
    - The integration credentials are valid and working.

For more information on setting up queries, see **Manage Integrations (https://docs.mandiant.com/home/msv-managing-integrations)**.

Configure Legacy Integration

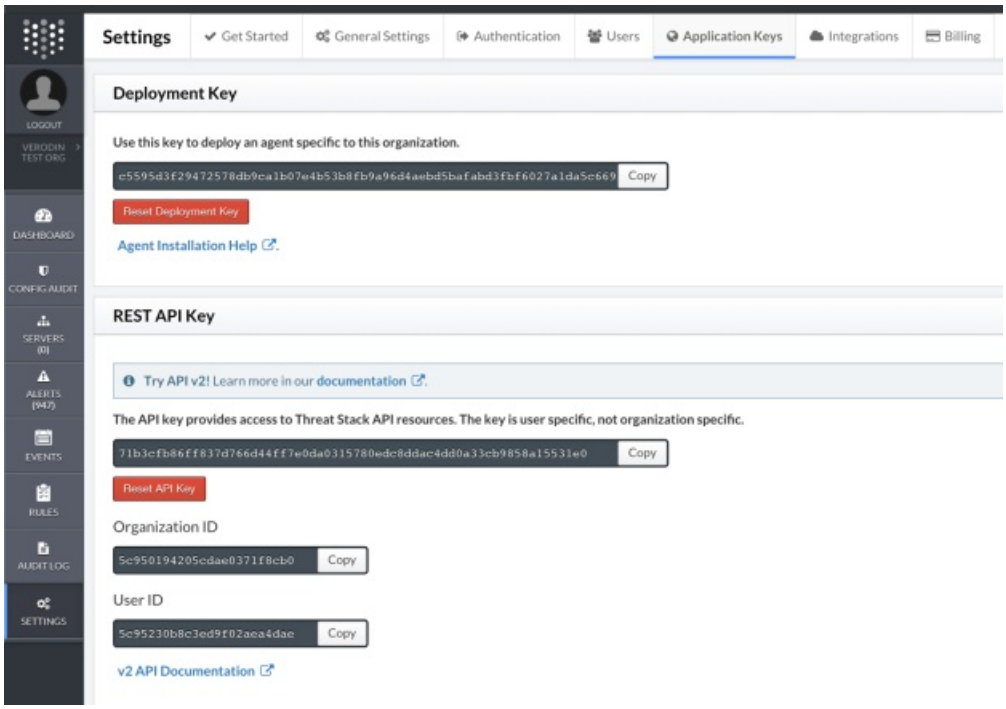
> This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support 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)**.

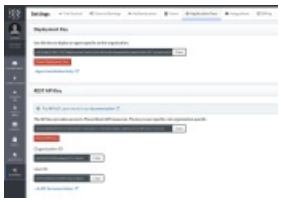
Generate an API key for Threat Stack

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.

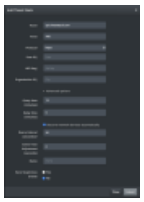
   a. Enter the **User ID** you copied from Threat Stack.
   b. Enter the **API Key** you copied from Threat Stack.
   c. Enter the **Organization ID** you copied from Threat Stack.

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 .