

ENDGAME INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validate that security tools are writing log events to Endgame to ensure compliance with security policies and regulations
- Collect events generated by security tools that write to Endgame 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
<code>/api/v1/alerts</code>	Retrieve a list of alerts from Endgame

Supported Versions

Endgame API v1

Before You Begin

To configure this integration, you need:

- A valid username and password for a user with permissions to use the API endpoints described in the previous step
- The hostname or IP address of your Endgame instance

Configure Security Validation

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



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. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
6. Enter the **Username** and **Password** for the account with permissions to use the API endpoints.
7. Change the **HttpProtocols** to use for requests. (**Https** or **Http**.)
8. For the **Host**, enter the hostname of your Endgame instance.
9. Enter a **Port** value. The default is **443**.
10. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
11. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **500**.

12. 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.

13. 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.

14. 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 \(https://docs.mandiant.com/home/msv-managing-integrations\)](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 \(https://docs.mandiant.com/home/msv-integrations-overview\)](https://docs.mandiant.com/home/msv-integrations-overview).

The Endgame Integration requires that the time on the Director and Actor to be kept synchronized. If there is a time skew, the integration will not be able to retrieve the proper data.



This integration is remote capable.

Update Endgame

TO UPDATE ENDGAME

1. Define a username with a user role that allows access to Alerts in Endgame.
2. Configure the Actor in the Validation Platform to match the name shown as the Endgame Sensor in the Endgame Portal.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the Sensor Transceiver Address in the endgame Portal and verify that the Validation Platform Actor can access it.
- Identify the Endgame Host.
- Identify the Port used by Endgame.
- Obtain credentials that allows access to Alerts in Endgame.

Configuration

TO ADD THE ENDGAME INTEGRATION

1. Go to **Settings > Integrations**.
2. Click **Add Integration > Endgame**.
3. Enter information for the **Host, Port, Username, and Password**.
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**.

Add Endgame

Host*	example.com
Port*	443
Username*	Username
Password*	Password
▼ Advanced options	
Query time (minutes)	15
Delay time (minutes)	0
<input checked="" type="checkbox"/> Discover network devices automatically	
Query Interval (seconds)*	30
Event Time Adjustment (seconds)	0
Name	Name
Save Suspicious Events	<input type="radio"/> Yes <input checked="" type="radio"/> No

Set up Proxy Assignment

If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. For information on setting up your proxy rules, see [Proxy Rules \(https://docs.mandiant.com/home/msv-proxy-rules\)](https://docs.mandiant.com/home/msv-proxy-rules).

Verify Connectivity

TO VERIFY CONNECTIVITY TO ENDGAME

Click **Test** to verify that:

- The Director can communicate with the Endgame Host on the port specified.
- The Username and Password are valid.

