Mandiant

ENDGAME

> 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).

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

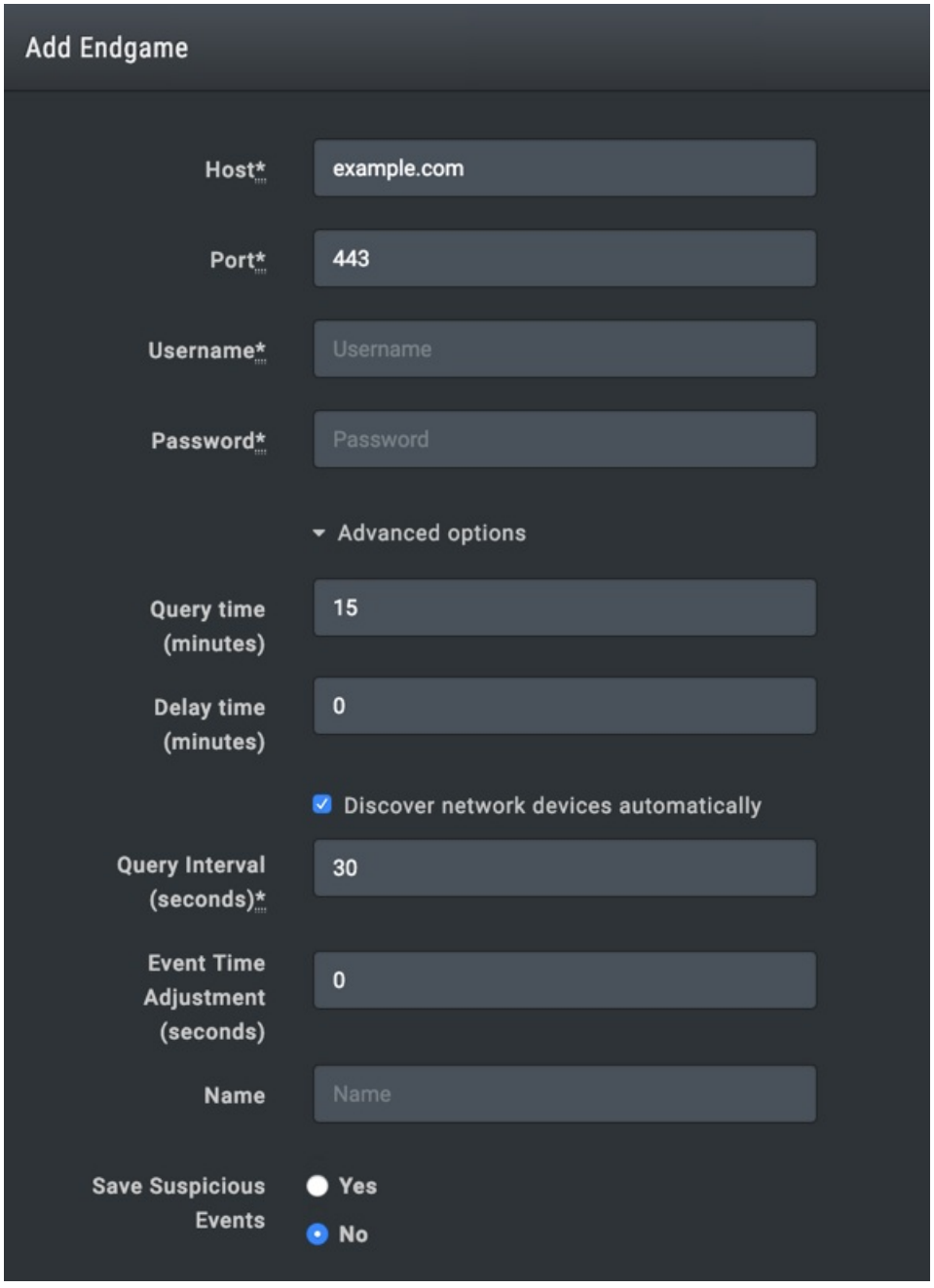
TO ADD THE ENDGAME INTEGRATION

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**.



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)**.

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.