# PALO ALTO NETWORKS FIREWALLS/PANORAMA

> 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)**.

This integration enables the Security Validation Director to pull events from individual Palo Alto Networks firewalls or from a Panorama management console managing multiple firewalls. Events may be pulled from the Threat, Wildfire, Data Filtering, and Traffic modules. A single integration is recommended if Panorama is available rather than connecting to each firewall individually.

This integration is remote capable.

The Time zone field in the Integration is very important. If you do not set it to match the time zone of the PA firewall or Panorama, all events will be marked as UTC, not local time. This means your events may not appear when you run Actions.

## Update Palo Alto

Palo Alto recommends setting up a separate admin account for API access:

1. Go to **https://docs.paloaltonetworks.com/pan-os**.
2. Search for "enable-api-access". In the results, you can open the most recent document version or access other versions.

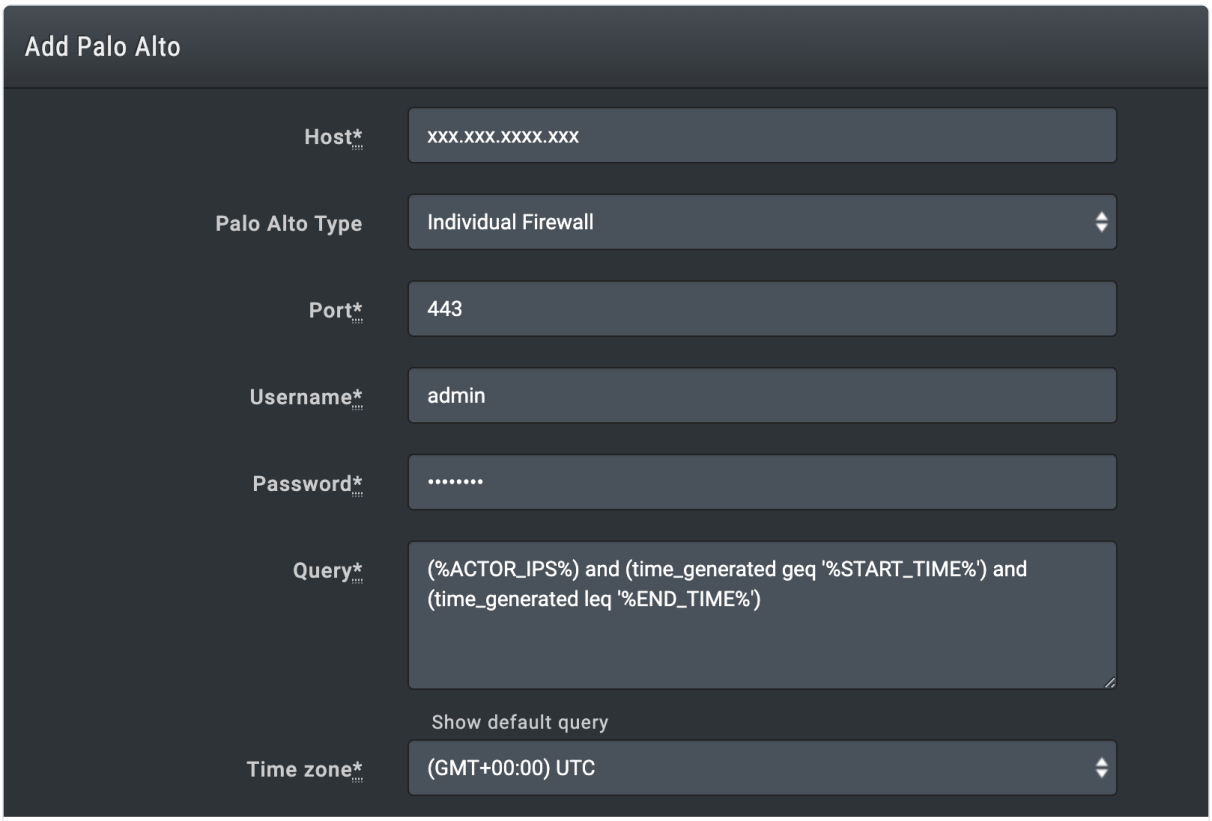
### Supported Palo Alto and Panorama Versions

- Palo Alto Networks versions 7.x, 8.x
- Panorama versions 7.x, 8.x, 9.x

## Update the Security Validation Platform

***TO ADD THE PALO ALTO INTEGRATION***

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Palo Alto**.

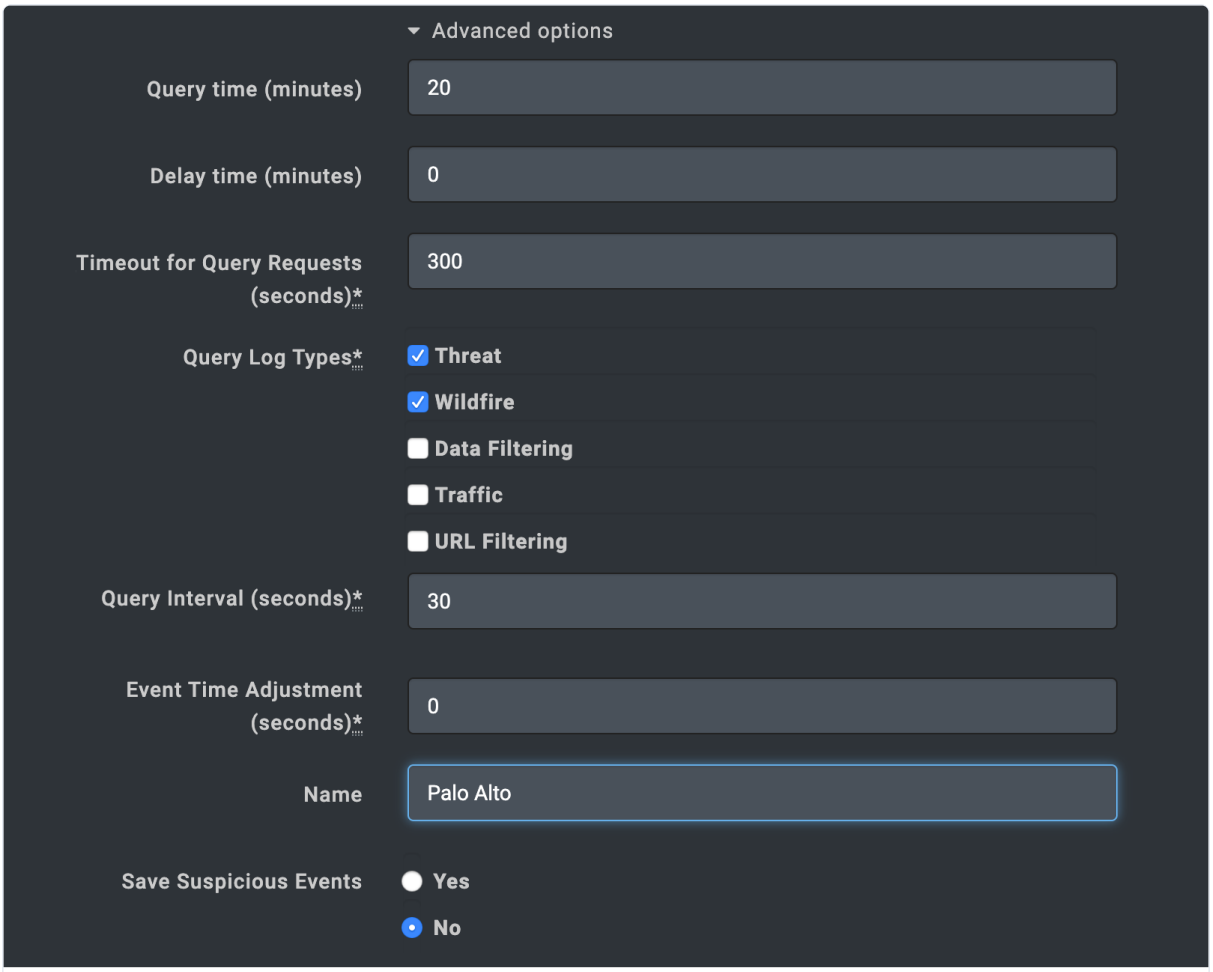



Palo Alto Integration

3. Enter information for the **Host**, **Port**, **Username**, and **Password**.
4. Change the **Palo Alto Type** to match your configuration.
5. Modify the **Query**, as necessary.
6. Update the **Time zone**.

> The time zone needs to match the time zone of the PA firewall or Panorama; if it doesn't, all events are assumed to be in UTC, not local time

7. Expand **Advanced options**.




Palo Alto Integration - Advanced options

8. (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.
9. (Optional) Update **Timeout for Query Requests**.
10. Select the **Log Types**.
11. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
12. (Optional) Assign a **Name**.
13. (Optional) Choose **Yes** to save suspicious events.
14. 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 PALO ALTO / PANORAMA***

Click **Test** to verify that:

- The Director can communicate with the Panorama console or individual firewalls on the port specified.
- Credentials are valid and working.
- Appropriate Logs are coming in.