Mandiant

PALO ALTO NEXT-GEN FIREWALL INTEGRATION WITH SECURITY VALIDATION

This integration collects events generated by Palo Alto Networks Next-Gen Firewall to test the efficacy and configuration of the security control 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

This integration uses the XML API.

API	Usage
/api	Collect events

Supported Versions

PAN-OS / Panorama v8.1-11.2

Preparation

To configure this integration, you need:

- The hostname of your Palo Alto Networks Next-Gen Firewall instance
- A valid username and password for a user with permissions to use the API endpoints described in the previous step

Configure full IPs and names in logs

When a role-based administrator account is used, logs and reports will display without usernames or IP addresses (1.2.3.4), instead networks will show (1.2.3.0/24).

To configure full IPs and names in the logs and reports, go to **Device > Admin Roles**, and under **Privacy**, there are two items:

- **Show Full IP Address**
- **Show User Names In Logs And Reports**

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > Palo Alto Networks Next-Gen Firewall** .

   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 Palo Alto Networks Next-Gen Firewall instance.
7. Enter a **Port** value. The default is **443**.
8. For **PaloAltoApplianceTypesV1**, select **Panorama Console** or **Individual Firewall**.
9. Enter the **Username** and **Password** for the account with permissions to use the API endpoints.
10. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
11. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
12. Optional: Change the **Timezones value**, if needed.
13. Optional: Modify the log types in **PaloAltoLogTypesV1** entries, if needed. Default values are provided and you can add or remove entries.
14. Optional: Modify **Queries**, as needed. A default value is provided.
15. Optional: Select **Use And IP Joiner** if you want to determine how IPs are combined in queries:
    - When selected, all queries consistently use the `AND` joiner.
    - When deselected, When unchecked, all queries use the `OR` joiner by default.

    The `AND` joiner can be specified on a per-query basis by using the `#USE_AND_JOINER` prefix, even if the setting is not selected.

16. Optional: Modify the **Page Size** to change the request for the upstream server. The default is **1000**.
17. Optional: Modify the **Query Max Pages**, if needed. The default is **10**.
18. 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.

19. 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.

20. 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).

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.

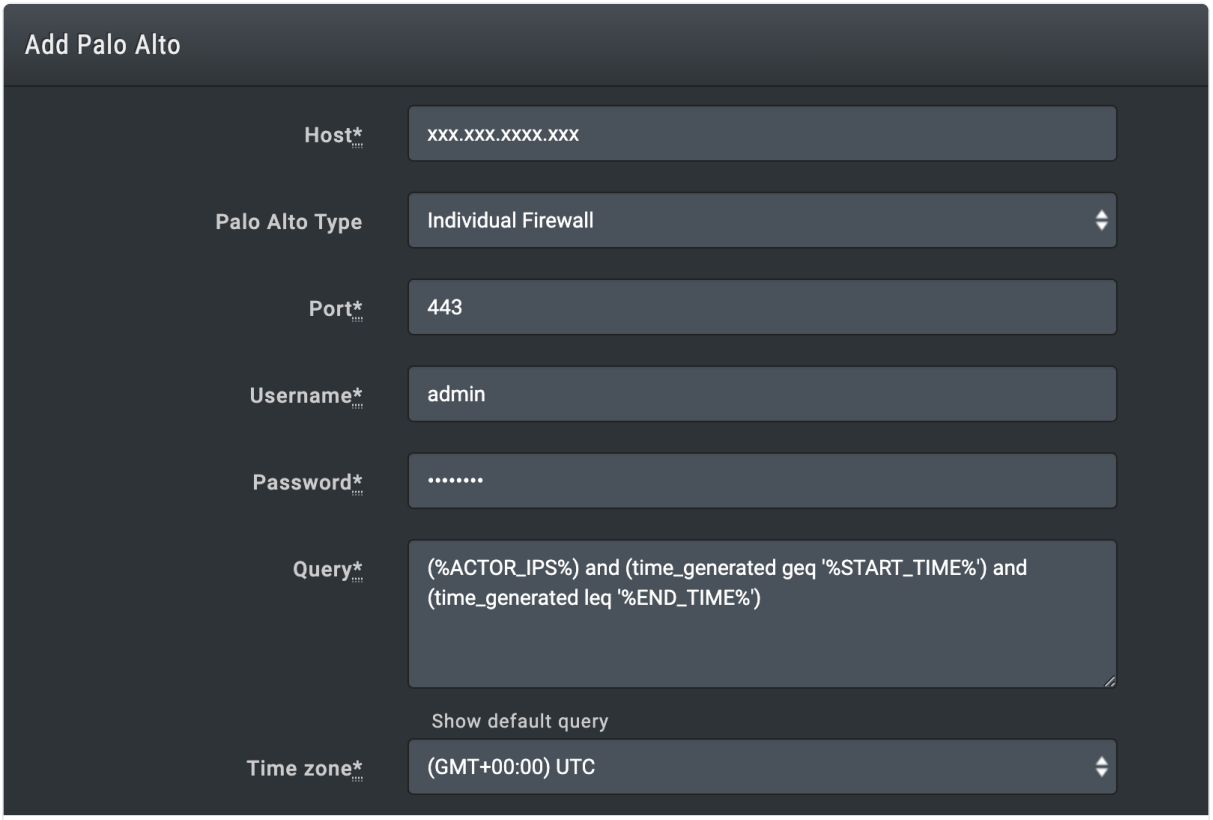
Supported Palo Alto and Panorama Versions

- 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**.

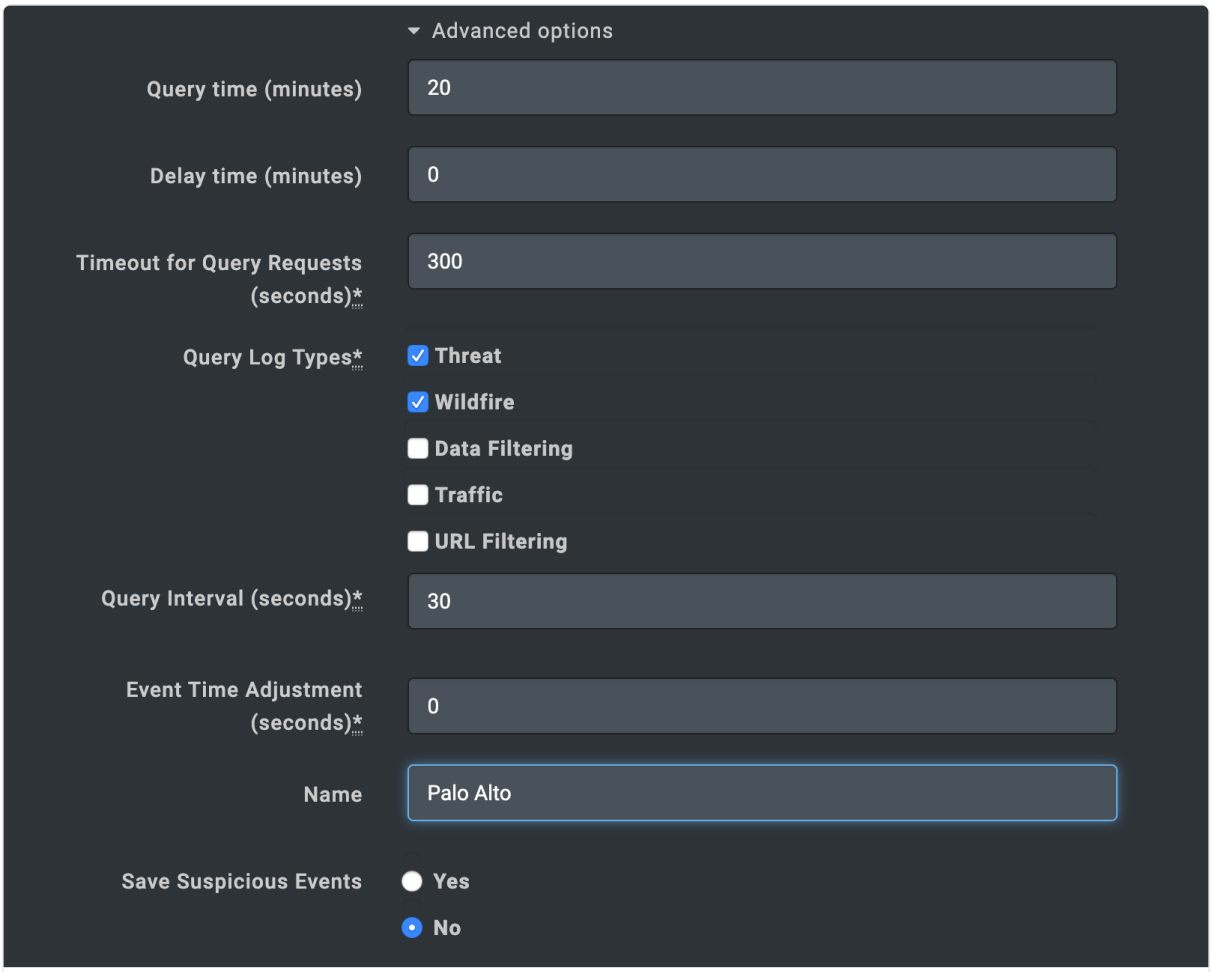


Palo Alto Integration

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.