

JUNIPER JSA INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to Juniper JSA to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to Juniper JSA 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/ariel/searches</code>	Query for events from Juniper JSA
<code>/api/siem/offenses</code>	Query for Offense IDs from Juniper JSA
<code>/api/help/versions</code>	Used to test connectivity and authentication settings

Supported Versions

- Juniper JSA 7.2.x
- Juniper JSA 7.3.x

Before You Begin

To configure this integration, you need:

- The hostname or IP address of your Juniper JSA instance
- A username and password OR an API token

Configure Security Validation

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



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. For the **Host**, enter the hostname of your Juniper JSA instance.
6. Enter a **Port** value. The default is **443**.
7. Change the **HttpProtocols** to use for requests. (**Https** or **Http**.)
8. Choose an authentication method for **JuniperJSAAuthTypes**: either **Basic** or **Token**.
9. Enter the **Username** and **Password** for the user account with permissions to use API endpoints.

10. Optional: If you chose **Token** for the authentication method, enter the generated **Token** value.
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: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
13. Optional: Add or remove **Queries**, as needed. A default value is provided.
14. Optional: Modify the **Offense Query Fields** and **Offense Query Filter**, if needed. Default values are provided.
15. Enter a value in the **Correlated Events Queries** and add more queries, if needed.
16. 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.

17. 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. Configure correlation queries:
 - i. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
 - ii. Modify the **Correlation Query Interval**, if necessary (minutes).
- d. 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.

- e. Select **Save Suspicious Events**.
- f. Modify the **Event Time Adjustment** (seconds). The default is **0**.
- g. 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.

18. 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 is remote capable.

Update Juniper JSA

Set up the credentials that will be used with the Validation Platform.

- Username and password or authentication token.
- Admin permissions are required, at minimum .

Update the Validation Platform

Prerequisites

Information to gather before you start:

1. Identify the IP address.
2. Identify the port communications (default is 443).
3. Identify whether the protocol is HTTP or HTTPS (default is HTTPS).
4. Have the credential information .
5. Identify the timezone of the Juniper host.

Configuration

TO ADD THE JUNIPER JSA INTEGRATION

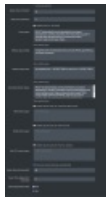
1. Go to **Settings > Integrations**.
2. Click **Add Integration > Juniper JSA**.



(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12e5c9cba0017c2f7e6c/n/juniper-jsa.png>)

Juniper JSA Integration

3. Populate the **Host**, **Port**, and **Protocol** information.
4. Enter information for the **Host**, **Port**, and **Protocol**.
5. Select the **Credential type** and enter the appropriate credentials.
6. Change the **Time Zone** to match that of the Juniper JSA host.
7. Expand **Advanced options**.



(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12edc9cba0017c2f7eae/n/juniper-jsa-advanced.png>)

Juniper JSA 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 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 Action 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.

9. (Optional) Review and update the populated query information (**Flows query**, **Offense query fields**, **Offense query filter**, **Correlated Events Query**).
10. (Optional) Enable the special query for DNS Actions and define the Query.
11. (Optional) Enable the special query for Email Actions and define the Query.
12. (Optional) Enable the special query for Host CLI Actions and define the **Query**.



If you enable the Host CLI Actions query and use the %HOST_CLI_ACTOR_HOSTNAMES% variable, the platform will substitute the plain hostname and the information from the Alternate Hostname field on the Actor configuration page.

13. (Optional) Select **Discover network devices automatically**.

14. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
15. (Optional) Assign a **Name**.
16. (Optional) Choose **Yes** to save suspicious events.
17. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO JUNIPER JSA

Click **Test** to verify that:

- The Director can communicate with Juniper JSA on the port and protocol specified.
- Credentials are valid and working.
- Times match.