Mandiant

RSA NETWITNESS LOGS & PACKETS INTEGRATION WITH SECURITY VALIDATION

This integration provides the following benefits:

- Validates that security tools are writing log events to RSA NetWitness Logs & Packets to ensure compliance with security policies and regulations
- Collects events generated by security tools that write to RSA NetWitness Logs & Packets 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 document covers the the MSI method of creating an integration. This method is the recommended approach for configuring new integrations in Security Validation.

API Calls

API	Usage
/sdk	Query for events from RSA NetWitness Logs & Packets

Supported Versions

RSA NetWitness 11.x

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 RSA NetWitness Logs & Packets instance

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > RSA NetWitness Logs & Packets** .

   

   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. Enter the **Host** for the RSA NetWitness instance.
6. Enter a **Port** value. The default is **50105.**
7. Optional: Change the **Protocol** value to determine what protocol is used for requests (**Https** or **Http**).
8. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
9. Enter the **Domain** value for the Checkpoint instance.
10. Enter the **Username** and **Password** for the account with permissions to use the API endpoints.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

11. Optional: Change the **User Agent**, if needed. The default is **MSI**.
12. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
13. Optional: Modify the **FieldMapModel** 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.

14. 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. If supported by your integration, 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.

15. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

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 the Validation Platform

Prerequisites

Information to gather before you start:

1. IP address used to access the RSA NetWitness concentrator.
2. Port for the concentrator communication (default is 50105).
3. Identify whether the protocol is HTTP or HTTPS for connections to the RSA NetWitness concentrator port.
4. Identify or create the credentials to access RSA NetWitness's concentrator.
5. Identify the field name mappings for the following:



There could be multiple of each, depending on log sources and configuration.

    a. Source IP
    b. Destination IP
    c. Source Port
    d. Destination Port
    e. Event Start Time (timestamp)
    f. Event Unique ID
    g. Event Signature ID
    h. Event Description
    i. Event Source Host

Configuration

TO ADD THE RSA NETWITNESS INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **RSA NetWitness**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62982c7dad331e21d9050edf/n/netwitness.png)

RSA NetWitness Integration

3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
4. (Optional) Enter information in the **Query** dialog box to query for base events. Click **Show default query** to see the default query information.
5. Expand **Advanced options**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/62982c7dad331e21d9050ee2/n/netwitness-adv.png)

RSA NetWitness Integration (Advanced Options)

6. (Optional) Update the **User Agent**.
7. To enable a query for ESA alerts, check the **Enable query for Alerts** check box.
8. (Optional) Enter information in the **Alert Query** dialog box to query for ESA alerts.

> The default time for an alert can be up to 30 minutes off from when the event fired. If this is the case you must add another field to your alerts with the proper time and add that time to the start_time field map for correlations to work properly.

9. Review the field name mappings; update as necessary.
    a. Inputs are enclosed by square brackets `[]`.
    b. Inputs are columns that could contain the info (`["time"]`).
    c. If there could be multiple commas, enclosed in one set of brackets, encompassed in quotes, and separated by commas (`["msg.id","reference.id", "rid"]`).
10. (Optional) Assign a **Name**.
11. (Optional) Choose **Yes** to save suspicious events.
12. Click **Submit**.

Verify Connectivity

TO VERIFY CONNECTIVITY TO RSA NETWITNESS

Click **Test** to verify that:

- The Director can communicate with NetWitness on the port and protocol specified.
- Credentials are valid and working.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.