RSA NETWITNESS RESPOND

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).

Update RSA NetWitness Respond

Identify or create credentials to access NetWitness Respond with read access, at minimum.

API Calls

The following API calls are used by Validation Platform.

Purpose	Call
Generate auth token	/rest/api/auth/userpass
Get incident information	/rest/api/incidents
Get alerts for each incident	/rest/api/incidents/{incident_id}/alerts

Update the Security Validation Platform

Prerequisites

Information to gather before you start:

- Identify the host, port, and protocol associated with your NetWitness Respond server
- Identify your NetWitness Respond username and password

Configuration

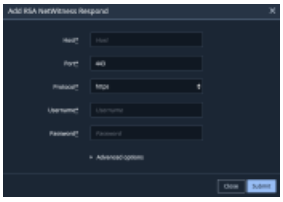
TO ADD THE RSA NETWITNESS RESPOND INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **RSA NetWitness Respond**.
3. Enter information for the **Host**, **Port**, **Protocol**, **Username** and **Password** or **API Token**.
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 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.

6. Modify the **Query Interval** and **Event Time Adjustment**, if necessary.
7. (Optional) Assign a **Name**.
8. (Optional) Choose **Yes** to save suspicious events.
9. Click **Submit**.



(https://dyzz9obi78pm5.cloudfront.net/app/image/id/629a12edc9cba0017c2f7eb3/n/rsa-netwitness-respond.png)

RSA NetWitness Respond

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 RSA NETWITNESS RESPOND

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.