

# RSA NetWitness Platform

Event Source Log Configuration Guide



## Cymulate Integration Guide

Last Modified: Monday, February 22, 2021

**Revision Date:** 14.1.2021

**Partner Name:** [Cymulate](#)

**Website:** <https://cymulate.com>

**Product Name:** Cymulate Continuous Security Validation

**Partner Contact:** [yahavl@cymulate.com](mailto:yahavl@cymulate.com)

**Support Contact:** [Support@cymulate.com](mailto:Support@cymulate.com)

**Supported On:** NetWitness Platform 11.5.0 and later

# Introduction

---

Cymulate SaaS-based Continuous Security Validation automates security risk assessments end-to-end, enabling them to challenge, assess and optimize their cyber-security posture simply and continuously.

## Use case for Integration with RSA NetWitness Platform

---

Cymulate Purple Team module enables security teams to automate red and purple team exercises, launch full kill chain APT scenarios, and create customized attack simulations. Whatever the playbook, attack scenarios exercise the effectiveness of incident management processes and threat hunting capabilities. Integration with the RSA NetWitness platform validates the effectiveness of each layer involved in the detection process. Attacks are correlated with SIEM findings to simplify the validation of the events and alerts they create from within the Cymulate platform.

- Verifies Alerts arriving to the RSA Netwitness platform by running Cymulate attack simulations.
- Verify Events arriving to the RSA Netwitness by running Cymulate attack simulations.

## Integrate Cymulate with RSA Netwitness Platform

Before you begin integration, you require the following on the RSA NetWitness Platform

### RSA Netwitness Requirements

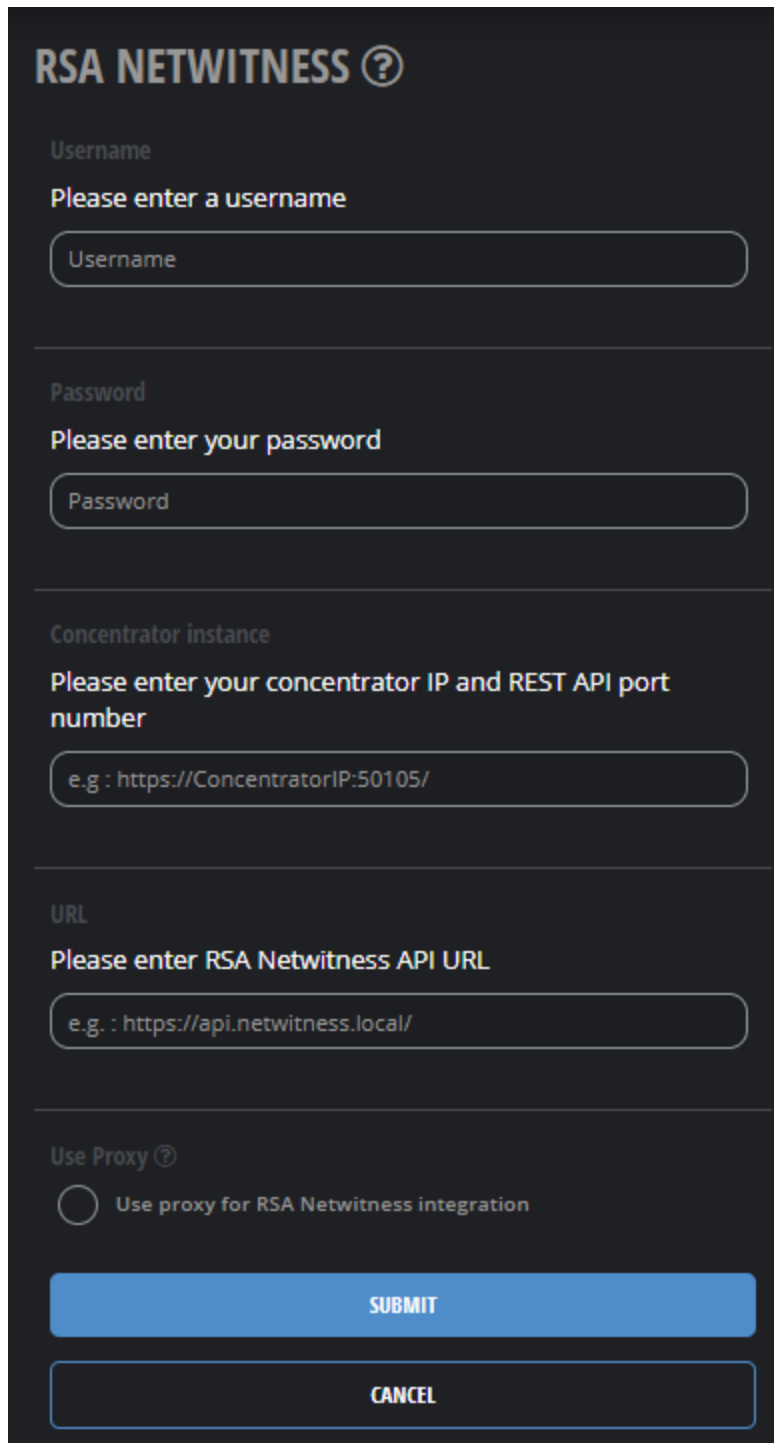
- URL of the Netwitness API platform
- Concentrator IP & Port
- Username & Password with the right permissions
- Port 80 or 443 from Cymulate agent to the RSA Netwitness platform

### User permissions for RSA Netwitness Configuration

- Access to the concentrator (Read)
- Access to incidents (Read)
- Access to alerts (Read)

## Partner Product Configuration

- RSA Netwitness Settings



The image shows a configuration form for RSA Netwitness. The form is titled "RSA NETWITNESS" with a help icon. It contains several input fields and a checkbox, followed by "SUBMIT" and "CANCEL" buttons.

**RSA NETWITNESS** ⓘ

Username  
Please enter a username

---

Password  
Please enter your password

---

Concentrator instance  
Please enter your concentrator IP and REST API port number  
e.g. : https://ConcentratorIP:50105/

---

URL  
Please enter RSA Netwitness API URL  
e.g. : https://api.netwitness.local/

---

Use Proxy ⓘ  
 Use proxy for RSA Netwitness integration

**SUBMIT**

**CANCEL**

### Troubleshooting

- Verify if the required communication is open
- Verify if required permissions are provided
- Verify access to the concentrator by the user

### Permissions required from NetWitness

- rest/api/auth/userpass
- rest/api/incidents
- rest/api/incidents/{id}/alerts
- sdk : msearch, query

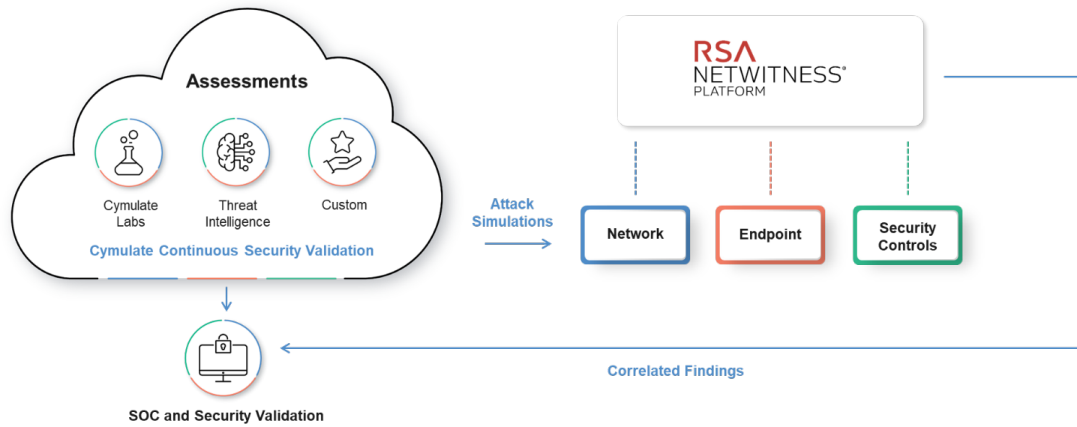
### To integrate Cymulate with RSA NetWitness Platform:

1. Go the Cymulate platform and login with your user.
2. Click on the “**Integrations**” tab, to open the integration page.
3. Scroll to RSA Netwitness integration and click “**Edit**”.
4. Fill in the details provided
  - a. Username
  - b. Password
  - c. Concentrator IP & Port
  - d. RSA API Url
  - e. Proxy – Yes/No
5. Click '**Submit**'
6. Verify the connection- it should show a green 'V' near the Cymulate agent on the integration page.
7. Start running attack simulations

## Integration Benefits

Integrating Cymulate with RSA NetWitness platforms simplifies the process by correlating the SIEM findings to attack simulations in the Cymulate platform. This enables security teams to assess and validate events and alerts effortlessly.

- It validates events showing on the RSA Netwitness platform
- It validates alerts showing on the RSA Netwitness platform



© 2021 RSA Security LLC or its affiliates. All Rights Reserved.

November 2020

### Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.