



AttackIQ Configuration Guide

for RSA NetWitness® Platform 11.4



Contact Information

RSA Link at <https://community.rsa.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

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.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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

January 2021

Contents

- Introduction** **4**
- Setting up the Integration Manager** **5**
 - Setting up Role Permissions 5
 - Configuring Users 6
- Integrating AttackIQ with RSA NetWitness Platform** **8**
 - Configuring NetWitness Integration 8
 - Enabling NetWitness Integration 9
 - Viewing Logs 10
- Reviewing Results** **12**
- AttackIQ SIEM Management** **14**
 - SIEM Management Configuration 14

Introduction

The AttackIQ platform provides capabilities for organizations to validate their security controls and verify their assumptions about the functionality and configurations of the security technologies that are deployed in their production environments. Establishing and maintaining communication with the existing security infrastructure is an important aspect for validating security controls.

Once you install AttackIQ on a customer-provided system, the Integrations Manager establishes communication with the AttackIQ Platform server. It can be configured to perform the following functions:

- Send details of all AttackIQ activity to on-premise security infrastructure.
- Execute queries of the security technology present using published APIs to verify the response from AttackIQ activities.
- Execute queries of the security technology present using published APIs to verify the presence of alerts based on AttackIQ activities.

This document provides information on:

- Configuring the RSA NetWitness Integration
- Identifying existing limitations

Note: For information regarding installation of the AttackIQ Integration Manager, see the AttackIQ Integration Deployment Guide.

Setting up the Integration Manager

Configure the Integration Manager in NetWitness Platform.

Prerequisites

- Ensure AttackIQ agents have been deployed to the environment.
- Confirm that data from the security infrastructure is fed into RSA NetWitness.

Setting up Role Permissions

Perform the following steps to set up the role permissions.

1. Login to the RSA NetWitness, and navigate to the **ADMIN** page.
2. Click **Services** > **[nwadmin]-broker**.
3. Select **System** > **Security**
4. Click the **Roles** tab.
5. Click + and enter the name of the role.
Example: aiq_api
6. Select the following role permissions for the new role:
 - sdk.content
 - sdk.manage
 - sdk.meta
7. Click **Apply**.

The screenshot displays the RSA NetWitness Platform's configuration interface. The top navigation bar includes 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. Below this, a secondary navigation bar shows 'HOSTS', 'SERVICES', 'EVENT SOURCES', 'ENDPOINT SOURCES', 'HEALTH & WELLNESS', 'SYSTEM', and 'SECURITY'. The 'SERVICES' section is expanded to show 'Change Service', 'SA - Broker', and 'Security'. The 'Users' tab is selected, and the 'Roles' sub-tab is active. A list of roles is shown on the left, with 'aiq_api' selected. The main area is titled 'Role Information' and contains a 'Name' field with 'aiq_api' entered. Below this is the 'Role Permissions' table:

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	aggregate	Allows aggregation of data
<input type="checkbox"/>	concentrator.manage	Allows users to manage the broker server
<input type="checkbox"/>	connections.manage	Allows users to manage connections to the service
<input type="checkbox"/>	everyone	Special system role that includes all users
<input type="checkbox"/>	index.manage	Allows users to manage the system index
<input type="checkbox"/>	logs.manage	Allows users to manage logs
<input type="checkbox"/>	owner	Special system role that includes only the owner
<input checked="" type="checkbox"/>	sdk.content	Allows users to access sdk content
<input checked="" type="checkbox"/>	sdk.manage	Allows users to manage queries and the sdk subsystem
<input checked="" type="checkbox"/>	sdk.meta	Allows users to access sdk metadata
<input type="checkbox"/>	sdk.packets	Allows users to access raw packets or logs
<input type="checkbox"/>	services.manage	Allows users to manage connections to other services
<input type="checkbox"/>	storedproc.execute	Allow users to execute stored procedures
<input type="checkbox"/>	storedproc.manage	Allow users to manage stored procedures
<input type="checkbox"/>	sys.manage	Allows users to manage the system
<input type="checkbox"/>	users.manage	Allows users to manage users and groups on the system

At the bottom of the permissions table are 'Apply' and 'Reset' buttons.

Configuring Users

Perform the following steps to configure users in NetWitness Platform.

1. Click on the **Users** tab.
2. Click **+** to create a custom user.
3. In the **Auth Type** pull down menu, select **NetWitness Platform**.
4. Select the role that you want to assign to the user from the **Role Membership** menu.
5. Complete the appropriate user information as per the requirement.
6. Click **Apply**.

Note: Ensure that you save the username and password for future use.

RSA Investigate Respond Users Hosts Files Dashboard Reports

HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY

Change Service | SA - Broker | Security

Users Roles Settings

User Information

Name: aiq_api Username: aiq_api

Password: Confirm Password:

Email: Description:

User Settings

Auth Type: Core Query Timeout: 5

Query Prefix: Session Threshold: 0

Role Membership

- Groups
- Administrators
- Aggregation
- Analysts
- Data_Privacy_Officers
- Malware_Analysts
- Operators
- SOC_Managers
- aiq_api

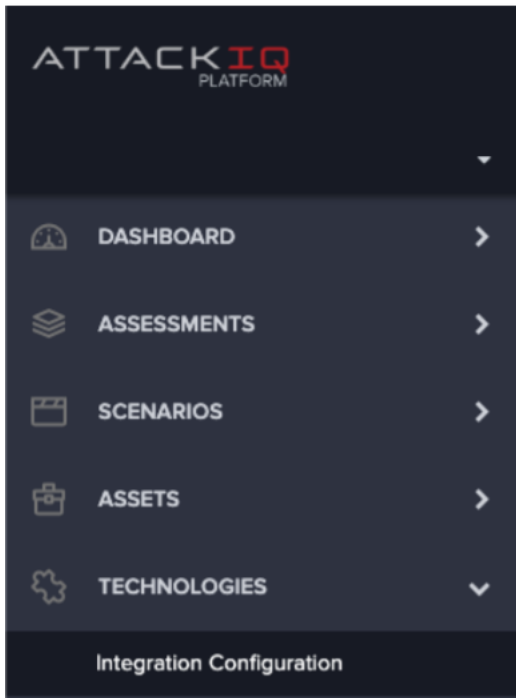
RSA NETWITNESS PLATFORM

Integrating AttackIQ with RSA NetWitness Platform

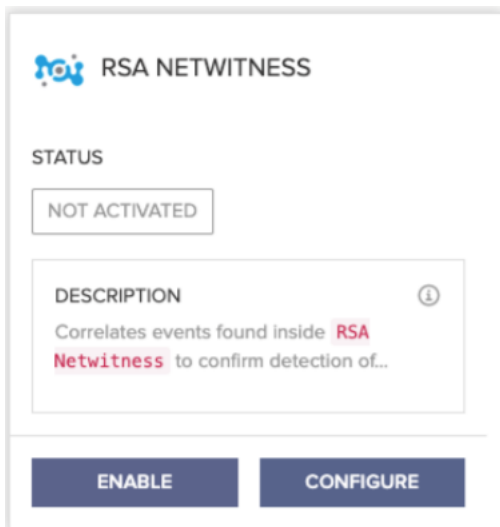
Configuring NetWitness Integration

Perform the following steps to configure NetWitness in AttackIQ.

1. Login to the Attack IQ platform.
2. In the menu, click **TECHNOLOGIES > Integration Configuration**.



3. In the Integrations page, locate the **RSA NETWITNESS** and click **CONFIGURE**.



4. Enter the configuration information as per the requirement.

The following table provides information on the various configuration parameters and its description.

Parameter	Description
API Endpoint	Enter the IP address / host name of the broker / concentrator / decoder.
API Port	Enter the port number of the broker / concentrator / decoder.
Username	Enter the user name of the broker /concentrator / decoder.
Password	Enter the password of the broker /concentrator / decoder.
Scenario Detection Delay	Enter the delay in minutes. AttackIQ recommends a 10 minute delay detection.
Smart Query Time Buffer	AttackIQ recommends a 2 second time buffer.
Enable debug logs	Select True to get debug logs.

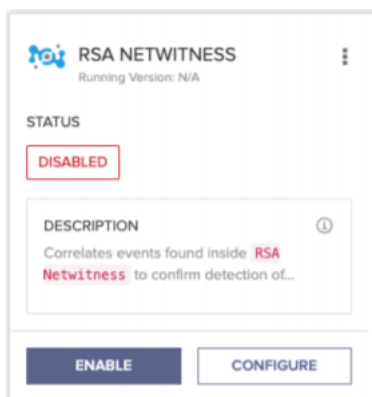
5. Click **SAVE CONFIGURATION**.

Note: Once you save the configuration, you can access the RSA NetWitness integration menu from the **CONFIGURED INTEGRATIONS** tab.

Enabling NetWitness Integration

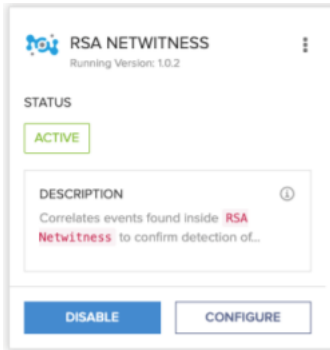
Perform the following steps in AttackIQ to enable NetWitness Platform integration.

1. Click **CONFIGURED INTEGRATIONS** in the RSA NetWitness menu.
The **RSA NetWitness** page is displayed.
2. Click **ENABLE**.



The integration confirmation pop-up message is displayed.

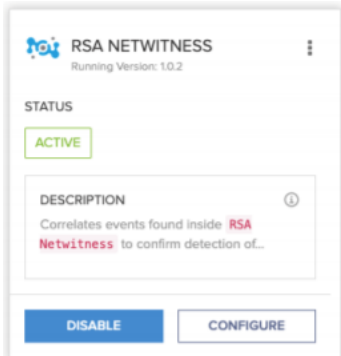
- The configuration status changes from pending to active.



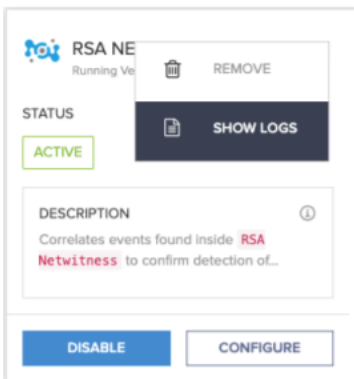
Viewing Logs

Perform the following steps in Attack IQ to view the RSA NetWitness logs.

- Click ... in the RSA NetWitness menu.



- Click **SHOW LOGS**.



The RSA NetWitness Logs page is displayed.



Reviewing Results

AttackIQ prevention results display information on the attack from the defender's perspective. Select any completed assessment from the Assessment page to review the results.

Table 2: AttackIQ Reports

Findings	Description
Prevention Results	A prevented attack is highlighted in green color, and an allowed attack is highlighted in red. In addition to the configured integration, Detection results provide you insights to determine if the configured integration was effective enough to detect the attack.
Overall Historical Results	The aggregate Scenario pass rate over time. For each time an Assessment is run, pass rate percentage equals the number of scenarios passed across all assets versus number of all scenarios run across all assets.
Assessment Test Results	The results of each individual test within the assessment. Selecting these results will reveal a list of scenarios and their results that were selected for each test.
Detection Results	Historical detection results by technology measures the efficacy of integrated security controls within the AttackIQ Platform. This visualizes what scenarios were detected by the technologies chosen to integrate with AttackIQ over time.
Results	Allows an analyst to determine if their security tools are blocking and detecting activity from AttackIQ Scenario runs.

Prevention Results	Shows the raw results within an assessment. Use filters to can narrow down the prevention results for a specific scenario on an asset at a given time. AttackIQ scenarios are designed to cause any vulnerabilities, security technologies may not block all scenarios.
Detection Results	AttackIQ Platform initiates queries to the configured SIEM to identify and match the emulated attack activities to alerts or logs. This page enable users to determine if the configured integration detect activities from AttackIQ scenarios.
Reports	Enables a user to view different types of reports available from the assessment. Reports can be configured to be sent across as emails from assessment to the team members on a specific schedule.

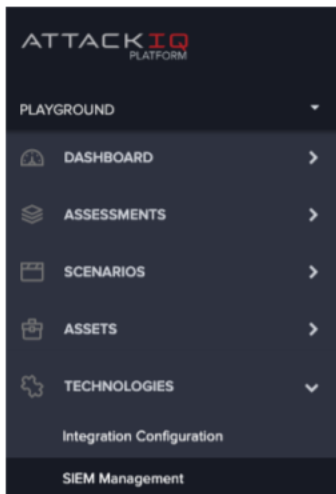
AttackIQ SIEM Management

SIEM integrations, such as RSA NetWitness, require additional configuration for detections to work efficiently. The SIEM Management page allows you to map the data to security technologies as per the requirement.

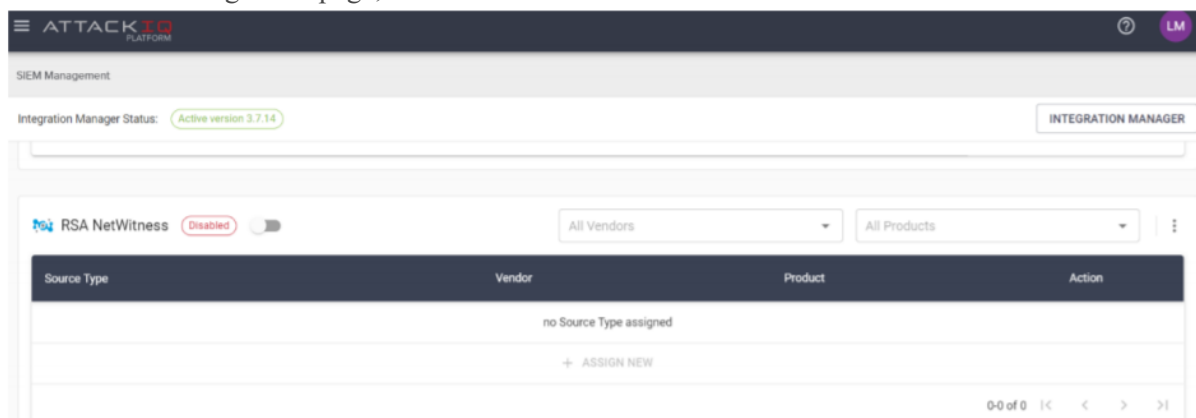
Prior to mapping the source types to corresponding security technologies, ensure that you execute an assessment. If a source type is not automatically identified and mapped to a specific technology, the source type remains in the **Unassigned** state until it is manually assigned in the SIEM Management page.

SIEM Management Configuration

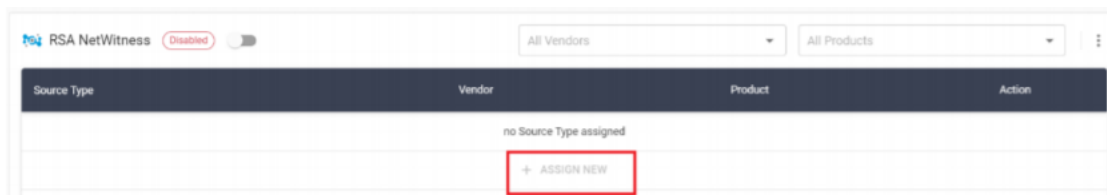
1. Login to the AttackIQ Platform.
2. Go to **TECHNOLOGIES > SIEM Management**.
The SIEM Management page is displayed.



3. In the SIEM Management page, locate **RSA NetWitness**.



4. Click + ASSIGN NEW .



Note: If there are multiple EDR solutions, you can select specific integration vendors and products from the pre-configured options. You can also add them (to match the source type) within the AttackIQ platform.