RSA NetWitness Platform

Event Source Log Configuration Guide

Securaa Integration Guide

Last Modified: Wednesday, October 13, 2021

Integration Product Information:

Partner Name: Securaa
Website: https://www.securaa.io/
Versions: API v1.0

Partner Product Information:

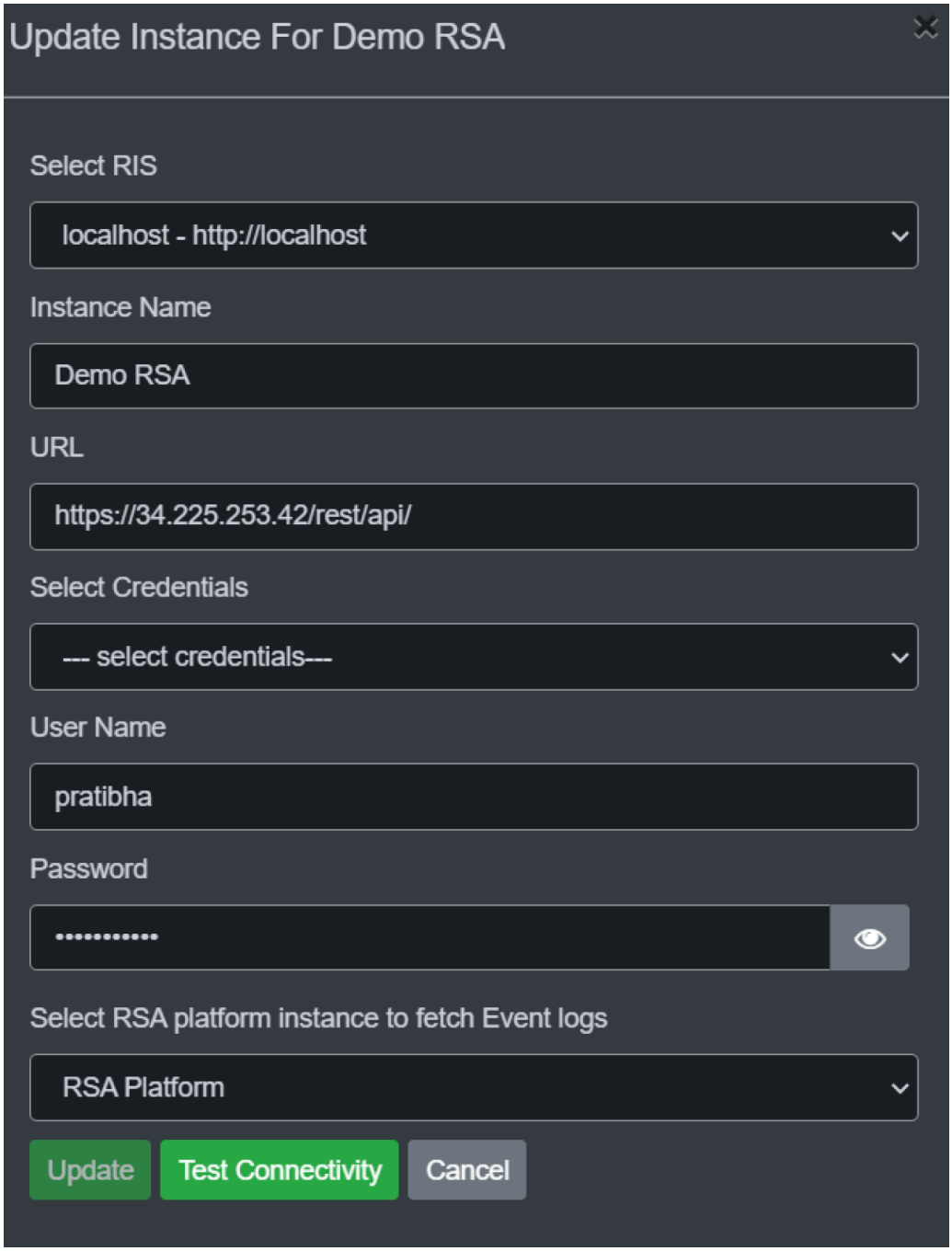
Supported On: NetWitness Platform 11.2.x and later

Note: Securaa supports investigative actions to collect incident details, logs, and packet capture from NetWitness Platform. To access NetWitness Platform, the configured user must be a System Administrator.

Configuration Variables for RSA NetWitness

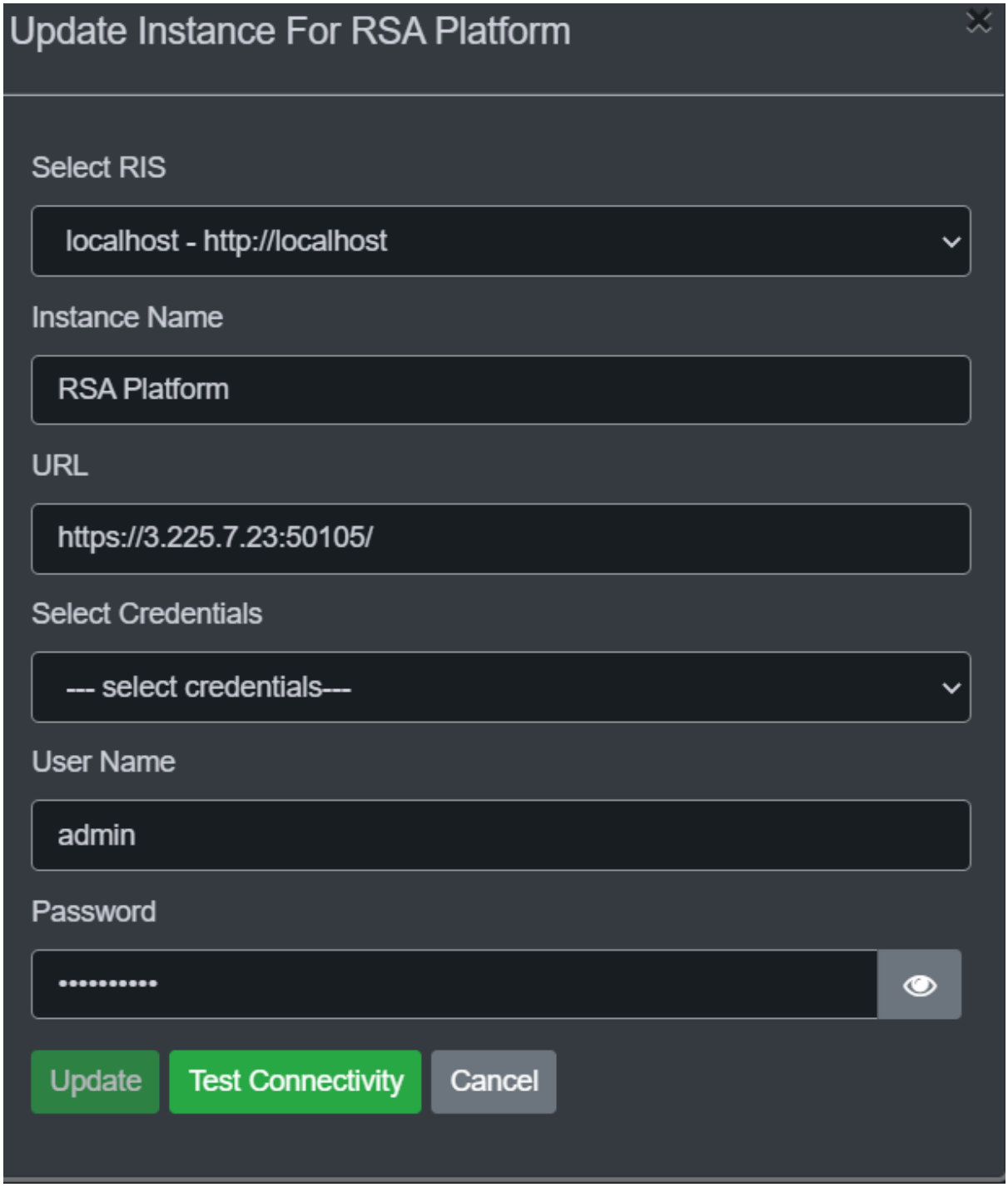
Before you begin integration, you require the following on the RSA NetWitness Platform. Securaa requires the configuration variables below to operate on NetWitness Platform.

Variable	Required	Type	Description
Select RIS	Yes	String	Remote Integration Server (Default - localHost).
Instance Name	Yes	String	RSA NetWitness Manager.
URL	Yes	String	RSA NetWitness Instance Name (https://{{IP Address}}/rest/api/).
Select Credentials	No	Selection	Choose Saved Credentials.
User Name	Yes	String	RSA NetWitness Platform Username.
Password	Yes	String	RSA NetWitness Platform Password.
Select RSA platform instance to fetch Event logs	Yes	String	Select Instance Name.


Update Instance For Demo RSA
Select RIS
localhost - http://localhost
Instance Name
Demo RSA
URL
https://34.225.253.42/rest/api/
Select Credentials
--- select credentials---
User Name
pratibha
Password
Select RSA platform instance to fetch Event logs
RSA Platform
Update
Test Connectivity
Cancel

Configuration Variables for RSA Platform

Variable	Required	Type	Description
Select RIS	Yes	String	Remote Integration Server (Default - localHost).
Instance Name	Yes	String	RSA Platform Instance Name.
URL	Yes	String	RSA Platform URL(https://{{IP Address}}:port/).
Select Credentials	No	Selection	Choose Saved Credentials.
User Name	Yes	String	RSA Platform Username.
Password	Yes	String	RSA Platform Password.



Supported Tasks

The following table provides the details about the tasks that are supported after integrating Securaa with NetWitness Platform.

Task Name	Description
Get Incident Details	It is used to get details of a particular incident.
Get Incident Alert	It is used to get alert of a particular incident.
Delete Incident	It is used to delete a particular incident.
Update Incident	It is used to update already existing particular incident.
Get Incident Time Range	It is used to get those incidents which happened in a particular time range.
Run Query	It is used to run a query.
Get Meta Value	It is used to get a meta value.
Get Logs	It is used to download a log capture file.
Get Pcap	It is used to download a packet log file.
Get Pcap by Query	It is used to download a packet log file.

Task Parameters

The table below includes parameters for each of the Supported Tasks.

Task Name	Parameter	Required	Allowed Parameters	Type	Description
Get Incident Details	Incident ID	Yes	Incident ID	Integer	Incident ID to Investigate.
Get Incident Alert	Incident ID	Yes	Incident ID	Integer	Incident ID to Investigate.
Delete	Incident ID	Yes	Incident ID	Integer	Incident ID to

Task Name	Parameter	Required	Allowed Parameters	Type	Description
Incident					Investigate.
Update Incident	Incident ID	Yes	Incident ID	Integer	Incident ID to Investigate.
Update Incident	Status	Yes	Assigned, In Progress, Remediation Requested, Remediation Complete, Closed, Closed false positive	String	Status of incident
Update Incident	Assignee	Yes	Name of the user	String	Name of assignee
Get Incident Time Range	From	Yes	Date from which	String	Start date
Get Incident Time Range	Up to	Yes	Till this date	String	End date
Run Query	Query (select*)	Yes	Query	String	Query to select
Run Query	ID1	Yes	IP.src	Numeric	ID1
Run Query	ID2	Yes	ID2	Numeric	ID2

Task Name	Parameter	Required	Allowed Parameters	Type	Description
Run Query	Size	Yes	Default (100)	Numeric	Size
Get Meta Value	Field Name	Yes	Query(ip.dst)	String	The field name
Get Meta Value	ID1	Yes	IP.src	String	ID1
Get Meta Value	ID2	Yes	ID	String	ID2
Get Meta Value	Size	Yes	Size (Default (100))	Numeric	Size
Get Logs	Session ID	Yes	Session ID	Integer	The ID used for the session
Get Pcap	Session ID	Yes	Session ID	Integer	The ID used for the session
Get Pcap by Query	Field Name	Yes	Query(ip.dst)	String	The field name
Get Pcap by Query	ID1	Yes	IP.src	String	ID1
Get Pcap by Query	ID2	Yes	ID	String	ID2

Task Name	Parameter	Required	Allowed Parameters	Type	Description
Get Pcap by Query	Size	Yes	Size (Default (100))	Numeric	Size

Get Incident Details Features

The table below lists the UI features displayed when you try to fetch the Incident details using NetWitness Platform.

Field Name	Type	Example Output Values
ID	String	INC-1
Title	String	ENDPOINT INCIDENT Manual
Summary	String	
Priority	String	Critical
Risk Score	Integer	50
Status	String	Remediation Request
Created	String	Creation Date
Last Updated	String	2018-12-07T09:12:26.071Z
Last Updated By	String	Admin
Event Count	Integer	6
Source IP	String	10.10.10.11
Destination IP	String	10.10.10.10

Get Incident Alert Features

The table below lists the UI features in the **Incident Alerts** window (**Incidents** tab).

Field Name	Type	Example Output Values
Title	String	Manual Alert
Source	String	NetWitness Investigate
Score	Integer	50
Type	String	Log

The table below lists the UI features in the **Incident Alerts** window (**Alerts** tab).

Field Name	Type	Example Output Values
Source IP	String	117.10.10.10
Source Username	String	Null
Destination IP	String	172.31.10.10
Destination Username	String	Administration
Domain	String	Symantec Server

Delete Incident Features

There are no features in this window.

Update Incident Features

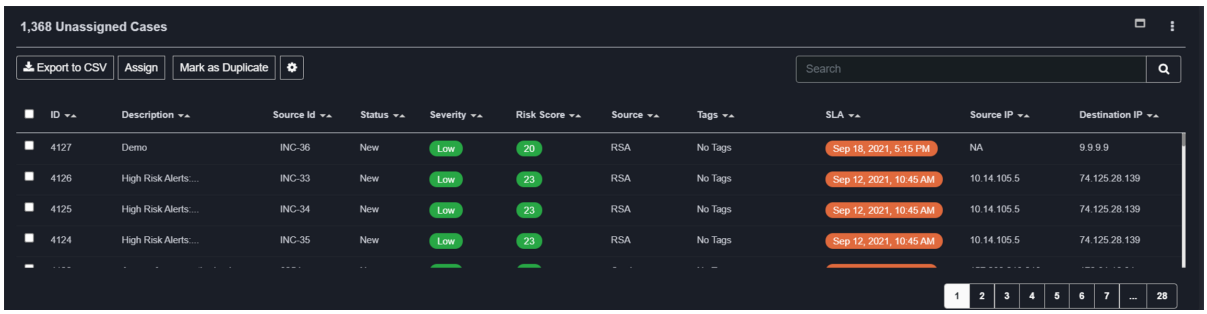
There are no features in this window.

Get Incident Time Range Features

The table below lists the UI features in the **Get Incident Time Range** window.

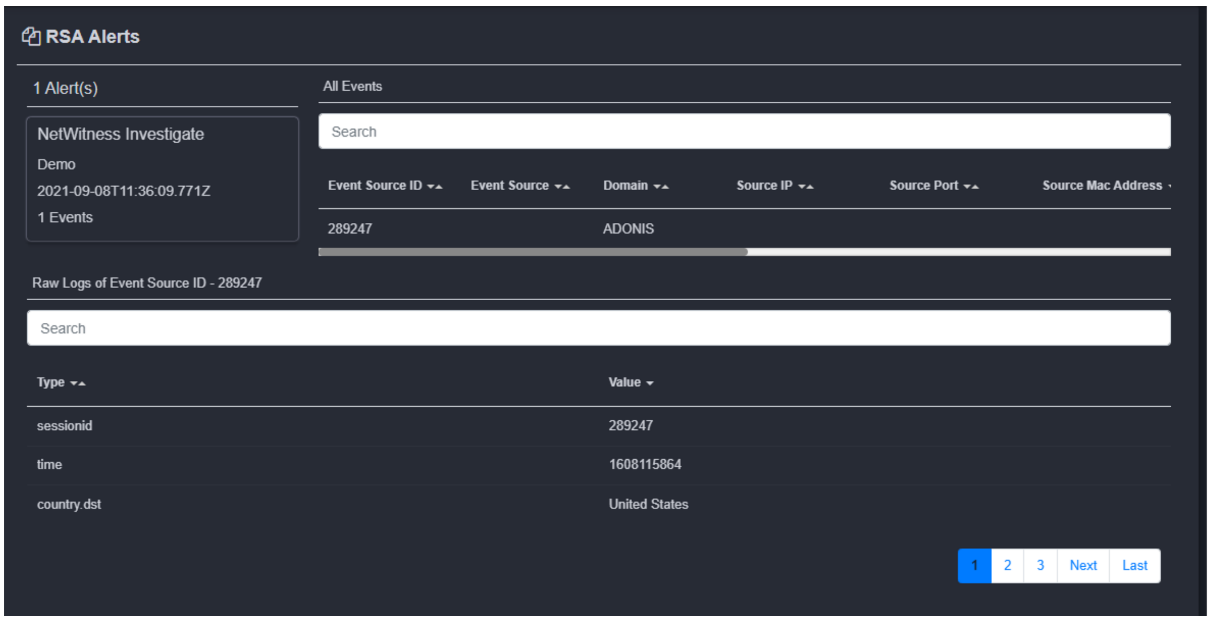
Field Name	Type	Example Output Values
ID	String	INC-1
Title	String	ENDPOINT INCIDENT Manual
Priority	String	Critical
Risk Score	Integer	50
Status	String	Critical
Created	String	2018-11-01T06:14:53.887Z
Event Count	Integer	6

The NetWitness Platform incidents will be displayed in the dashboard as shown below.



When you click an incident, the incident details are displayed. Select Raw data. The below image depicts the raw alerts.

When you click the Events Source ID, the Raw Logs detail of the Event ID will be fetched by the Securaa UI.



Run Query Features

The table below lists the UI features (in the **Results** Tab) displayed when you try to run the query using NetWitness Platform.

Field Name	Type	Example Output Values
ID1	Integer	5226745
ID2	Integer	5226745
Format	Integer	8
Type	String	Session ID, Time, Size, Medium
Flags	Integer	0
Group	Integer	173095
Size	Integer	8
Content	Integer	173095
Count	Integer	0

The table below lists the UI features (in the **Results Info** Tab) displayed when you try to run the query using NetWitness Platform.

Field Name	Type	Example Output Values
Content	Integer	0
Name	String	Offline device count

Get Meta Value Features

The table below lists the UI features in the **Get Meta Value** window.

Field Name	Type	Example Output Values
IP.Dest	String	188.10.10.10

Get Logs Features

The table below lists the UI features in the **Get Logs** window. A log file is generated with the below parameters.

Field Name	Type	Example Output Values
File Size	Integer	No of bytes
SHA1	String	a39a3ee5e6b4b0d3255bfsnxbsxjsjxksj1213
SHA256	String	Dsdajdkawj2232hdj1jn3n4n4jdkxnsjskxd
SHA512	String	4b4n4nkx8jwi921mjxysakaiaiqmqnsgxxyaammki

Get Pcap Features

The table below lists the UI features in the **Get Pcap** window. A packet log file is generated with the below parameters.

Field Name	Type	Example Output Values
File Size	Integer	No of bytes
SHA1	String	a39a3ee5e6b4b0d3255bfsnxbsxjsjxksj1213
SHA256	String	Dsdajdkawj2232hdj1jn3n4n4jdkxnsjskxd
SHA512	String	4b4n4nkx8jwi921mjxysakaiaiqmqnsgxxyaammki

Get Pcap by Query Features

The table below lists the UI features in the **Get Pcap by Query** window. A packet log file is generated with the below parameters.

Field Name	Type	Example Output Values
File Size	Integer	No of bytes
SHA1	String	a39a3ee5e6b4b0d3255bfsnxbsxjsjxksj1213
SHA256	String	Dsdajdkawj2232hdj1jn3n4n4jdkxnsjskxd
SHA512	String	4b4n4nkx8jwi921mjxysakaiaiqmqnsgxxyaammki

November 2020

Trademarks