RSA NetWitness Platform

Event Source Log Configuration Guide

Cyware Integration Guide

Last Modified: Friday, December 17, 2021

Integration Product Information:

Partner Name: Cyware
Website: https://cyware.com/
Versions: API v1.0

Partner Product Information:

Supported On: NetWitness Platform 11.2.x and later

About RSA NetWitness

The RSA NetWitness Platform accelerates threat detection and response by collecting and analyzing data across an array of capture points (logs, packets, netflow, and endpoint) and computing platforms (physical, virtual, and cloud). The platform enriches this data with threat intelligence and business context. With RSA NetWitness Platform, security analysts can prioritize, investigate, and respond to the threats in their environment quickly and precisely.

Configure RSA NetWitness Platform with Cyware Orchestrate

Configure RSA NetWitness Platform with Cyware Orchestrate application to perform the following actions:

Action Name	Description
Release from Network Isolation	This action restores the network connection and removes IP addresses added to the exclusion list for the host with the specified agent ID.
Request Network Isolation	This action isolates the host with the specified agent ID from the network.
Request Process Dump Download	This action initiates the download of the process dump to the Endpoint server.
Request System Dump Download	This action can be used to initiate the download of the system dump to the Endpoint Server.
Request Multiple Files Download to Server	This action downloads multiple files and can be used for incident investigation.
Request File Download to Server	This action downloads a particular file and can be used for incident investigation.
Get Alerts for File	This action retrieves all alerts triggered for a given file.
Get Alerts for Host	This action retrieves all alerts triggered for a given host.

Action Name	Description
Request Scan	This action starts a scan for the host with the specified agent ID.
Get File Information	This action retrieves information about a particular file and can be used for incident investigation. This information is specific to the unique file and does not include any host information.
Snapshot Details for Host	This action retrieves snapshot details of the given host for the specified snapshot time.
List Snapshots for Host	This action retrieves a list of snapshots, which are IDs to fetch the snapshot details of the host.
Get Host	The action retrieves the list of all hosts' information from a particular Endpoint Server.
Get Incident Alerts	This action retrieves all alerts that are associated with an incident using the incident’s unique identifier.
Add Journal Entry	This action adds a Journal entry or a note to an existing incident.
Delete Incident	This action deletes an incident using the incident’s unique identifier.
Update Incident	This action updates an incident status and assignee details using the incident’s Endpoint.
Get Incident by Date Range	This action retrieves incidents by the date and time they were created.
Get Incident	This action retrieves details of an incident using an incident's unique identifier.
Get Service IDs of all Services	This action retrieves the list of all service IDs of all services.

Configuration Parameters

The following configuration parameters are required for the RSA NetWitness Platform to communicate with the RSA NetWitness enterprise application. The parameters can be configured by creating instances in the RSA NetWitness Platform.

Parameter	Description	Field Type	Required/Optional	Comments
Base URL	Enter the base URL for your RSA NetWitness platform. For Example: https://rsa.domain.corp	Text	Required	
Username	Enter the username to access the RSA NetWitness Platform. For Example: **exampleusername**	Text	Required	
Password	Enter the password to access the RSA NetWitness Platform. For Example: **examplePassword**	Password	Required	

Release from Network Isolation

The below table lists the various input parameters associated with the action **Release from Network Isolation**.

Parameter	Description	Field Type	Required/Optional	Comments
Agent ID	Specify the unique ID for the host. For Example: **FFXXXXX8-266C-5871-**	Text	Required	

Parameter	Description	Field Type	Required/Optional	Comments
	6BAACACDXXXXX942			
Service ID	Specify the unique service ID for the host. For Example: **axxxxxff-ce95-4xx3-ab51-e93xxxxx67**	Text	Required	
Allow DNS Only By System	Specify if you want to allow the DNS by system. For Example: **True**	Boolean	Required	Allowed values: • **True** • **False**
Exclusions	Enter any networks you want to exclude from this task. For Example: **Null**	Any	Optional	Default value: **Null**
Comment	Enter the comment to be added to the network isolation. For Example: **ExampleComment**	Text	Optional	

Example Request

```
[
{
"agentId": "FFXXXXX8-266C-5871-6BAA-CACDXXXXXX942",
"serviceId": "21xx75-691e-4df1-8d4f-52xxx0f5d",
"allowDnsOnlyBySystem": true
}
]
```

Request Network Isolation

The below table lists the various input parameters associated with the action **Request Network Isolation**.

Parameter	Description	Field Type	Required/Optional	Comments
Agent ID	Specify the unique ID for the host. For Example: **FFXXXXX8-266C-5871-6BAACACDXXXXX942**	Text	Required	
Service ID	Specify the unique service ID for the host. For Example: **axxxxxff-ce95-4xx3-ab51-e93xxxxx67**	Text	Required	
Allow DNS Only By System	Specify if you want to allow the DNS by system. For Example: **True**	Boolean	Required	Allowed values: • **True** • **False**
Exclusions	Enter any networks you want to exclude from this task. For Example: **Null**	Any	Optional	
Comment	Enter the comment to be added to the network isolation. For Example: **ExampleComment**	Text	Optional	

Example Request

```
[
```

```
{
"agentId": "FFXXXXX8-266C-5871-6BAA-CACDXXXXXX942",
"serviceId": "21xx75-691e-4df1-8d4f-52xxx0f5d",
"allowDnsOnlyBySystem": true
}
]
```


Request Process Dump Download

The below table lists the various input parameters associated with the action **Request Process Dump Download**

Parameter	Description	Field Type	Required/Optional	Comments
Agent ID	Specify the unique ID for the host. For Example: **FFXXXXX8-266C-5871-6BAACACDXXXXX942**	Text	Required	
Service ID	Specify the unique service ID for the host. For Example: **axxxxxff-ce95-4xx3-ab51-e93xxxxx67**	Text	Required	
Process ID	Specify the unique process ID for the host. For Example: **5756**	Text	Required	
E Process	Specify the unique process ID for the host. For Example: **0xFFFFE10DC62C6440**	Text	Required	
File Name	Specify the file name to dump the download. For Example: **example.txt**	Text	Required	

Parameter	Description	Field Type	Required/Optional	Comments
Path	Enter the file path of the dump file location. For Example: **C:\Windows\ReportServer\PolicyDefinitions**	Text	Required	
Hash	Enter the hash file value of the system script file For Example: **687685b7531648c39fbb24fa81312b7fd2e3ece1bf1347b386f8725783767e5c**	Text	Required	
Process Create Utc Time	Enter the UTC time for the process creation. For Example: **1595496025034**	Text	Optional	

Example Request

```
[
{
"hash": "5f9axx928f7xxxxxf84fd2c8xxxxca0",
"path": "C:\Windows\ReportServer\PolicyDefinitions",
"agentId": "FFxx08-2xxC-5xx1-6BAA-CACDCxxxx942",
"fileName": "amazon-ssm-agent.exe",
"e_process": "0xFFFF800718FC0080",
"processId": "444",
"serviceId": "21xxxe75-691e-4df1-8d4f-52axxxxx0f5d"
}
]
```

Request System Dump Download

The below table lists the various input parameters associated with the action **Request System Dump Download**

Parameter	Description	Field Type	Required/Optional	Comments
Agent ID	Specify the unique ID for the host. For Example: **FFXXXXX8-266C-5871-6BAACACDXXXXX942**	Text	Required	
Service ID	Specify the unique service ID for the host. For Example: **axxxxxff-ce95-4xx3-ab51-e93xxxxx67**	Text	Required	

Example Request

```
[
{
"agentId": "FFxx08-2xxC-5xx1-6BAA-CACDCxxxx942",
"serviceId": "21xxxe75-691e-4df1-8d4f-52axxxxx0f5d",
}
]
```

Request Multiple Files Download to Server

The below table lists the various input parameters associated with the action **Request Multiple Files Download to Server**

Parameter	Description	Field Type	Required/Optional	Comments
Agent ID	Specify the unique ID for the host. For Example: **FFXXXXX8-266C-5871-6BAACACDXXXXX942**	Text	Required	

Parameter	Description	Field Type	Required/Optional	Comments
Service ID	Specify the unique service ID for the host. For Example: **axxxxxff-ce95-4xx3-ab51-e93xxxxx67**	Text	Required	
Path	Enter the file path of the dump file location. For Example: **C:\Windows\ReportServer\PolicyDefinitions**	Text	Required	
Count Files	Specify the maximum number of files returned by the host matching the wildcard path. For Example: **8**	Integer	Optional	
Max File Size	Specify the maximum size of every file for download. For Example: **50**	Integer	Optional	

Example Request

```
[
{
"path": "C:\Windows\ReportServer\PolicyDefinitions",
"agentId": "FXXXXX08-2XXC-5XX1-6XXA-CACDXXX65942",
"serviceId": "2xxxxx75-691e-4df1-8d4f-52aefxxxxd",
}
]
```

Request File Download to Server

The below table lists the various input parameters associated with the action **Request File Download to Server**

Parameter	Description	Field Type	Required/Optional	Comments
Agent ID	Specify the unique ID for the host. For Example: **FFXXXXX8-266C-5871-6BAACACDXXXXX942**	Text	Required	
Service ID	Specify the unique service ID for the host. For Example: **axxxxxff-ce95-4xx3-ab51-e93xxxxx67**	Text	Required	
Path	Enter the file path of the dump file location. For Example: **C:\Windows\ReportServer\PolicyDefinitions**	Text	Required	

Example Request

```
[
{
"path": "C:\Windows\ReportServer\PolicyDefinitions",
"agentId": "FFCB8C08-266C-5871-6BAA-CACDCB765942",
"serviceId": "213b6e75-691e-4df1-8d4f-52aef2970f5d",
}
]
```

Get Alerts for File

The below table lists the various input parameters associated with the action **Get Alerts for File**

Parameter	Description	Field Type	Required/Optional	Comments
Check Sum	Enter the checksum ID for the file. The file can be SHA256 and MD5. For Example: **d1c79a36593f0d5f7d07502b963c0291f4556ce8f110a58a48fda4**	Text	Required	
Service ID	Enter the service ID Endpoint Server to be connected. For Example: **aexxxff-ce95-46b3-ab51-e9xxxx7**	Text	Required	
Alert Category	Specify the alert category to retrieve alerts. For Example: **Critical**	Text	Optional	Allowed values: • **Critical** • **High** • **Medium** • **Low**

Example Request

```
[
{
"checksum": "b30xxxxc92a989a6557c6xxx8d2",
"serviceId": "21xxx75-691e-4df1-8d4f-52aexxx5d",
}
]
```

Get Alerts for Host

The below table lists the various input parameters associated with the action **Get Alerts for Host**

Parameter	Description	Field Type	Required/Optional	Comments
Agent ID	Specify the unique ID for the host. For Example: **FFXXXXX8-266C-5871-6BAACACDXXXXX942**	Text	Required	
Service ID	Specify the unique service ID for the host. For Example: **axxxxxff-ce95-4xx3-ab51-e93xxxxx67**	Text	Required	
Alert Category	Specify the alert category for the alerts. For Example: **Critical**	Text	Optional	Allowed values: • **Critical** • **High** • **Medium** • **Low**

Example Request

```
[
{
"agentId": "FXXXX8-266C-5871-6BAA-CAXXXX42",
"serviceId": "21xx75-691e-4df1-8d4f-52xxxxx5d",
}
]
```

Request Scan

The below table lists the various input parameters associated with the action **Request Scan**

Parameter	Description	Field Type	Required/Optional	Comments
Agent ID	Specify the unique ID for the host. For Example: **FFXXXXX8-266C-5871-6BAACACDXXXXX942**	Text	Required	
Service ID	Specify the unique service ID for the host. For Example: **axxxxxff-ce95-4xx3-ab51-e93xxxxx67**	Text	Required	
Scan Type	Specify the scan type for the request. For Example: **QUICK_SCAN**	Text	Required	Allowed values: • **QUICK_SCAN** • **CANCEL_SCAN**
CPU Max	Specify the amount of CPU the agent can use to run the scan. You can choose a value from 5 to 100. If you do not specify a value, the agent uses the default value.	Integer	Optional	Default value: • **25%**

Example Request

```
[
{
"agentId": "FXXXX8-266C-5871-6BAA-CAXXXX42",
"scanType": "QUICK_SCAN",
"serviceId": "21xxx5-691e-4df1-8d4f-52axxxxd",
}
]
```

Get File Information

The below table lists the various input parameters associated with the action **Get File Information**

Parameter	Description	Field Type	Required/Optional	Comments
Page Number	Specify the page number to get the file. For Example: **6**	Integer	Optional	
Service ID	Specify the unique service ID for the host. For Example: **axxxxxff-ce95-4xx3-ab51-e93xxxxx67**	Text	Required	
Page Size	Specify the page size to retrieve the file results. For Example: **40**	Integer	Optional	

Example Request

```
[
{
"serviceId": "213b6e75-691e-4df1-8d4f-52aef2970f5d",
}
]
```

Snapshot Details for Host

The below table lists the various input parameters associated with the action **Snapshot Details for Host**

Parameter	Description	Field Type	Required/Optional	Comments
Host Agent ID	Enter the host ID to get the snapshot details. For Example: **FXXXX8-266C-5871-6BAACAXXXX2**	Text	Required	
Service ID	Enter the service ID of the Endpoint Server to be connected. For Example: **axxxxxff-ce95-4xx3-ab51-e93xxxxx67**	Text	Required	
Snapshot Time	Enter the snapshot time to get the details. For Example: **2020-12-22T14:34:05.985Z**	Text	Required	

Example Request

```
[
{
"serviceId": "213b6e75-691e-4df1-8d4f-52aef2970f5d",
"host_agent_id": "FFCB8C08-266C-5871-6BAACACDCB765942",
"snapshot_time": "2020-12-22T14:34:05.985Z"
}
]
```

List Snapshots for Host

The below table lists the various input parameters associated with the action **List Snapshots for Host**

Parameter	Description	Field Type	Required/Optional	Comments
Host Agent ID	Enter the unique agent ID for the host. For Example: **FFXXX8-266C-5871-6BAACXXX942**	Text	Required	
Service ID	Specify the unique service ID for the host. For Example: **axxxxxff-ce95-4xx3-ab51-e93xxxxx67**	Text	Required	

Example Request

```
[
{
"serviceId": "213b6e75-691e-4df1-8d4f-52aef2970f5d",
"host_agent_id": "FFCB8C08-266C-5871-6BAA-CACDCB765942",
}
]
```

Get Host

The below table lists the various input parameters associated with the action **Get Host**

Parameter	Description	Field Type	Required/Optional	Comments
Page Number	Enter the page number to get the host. For Example: **3**	Integer	Optional	

Parameter	Description	Field Type	Required/Optional	Comments
Service ID	Specify the unique service ID for the host. For Example: **axxxxxff-ce95-4xx3-ab51-e93xxxxx67**	Text	Required	
Page Size	Enter the number of items to return on a single page. For Example: **80**	Integer	Optional	
Filters	Enter filters in the required JSON format.	Any	Optional	

Example Request

```
[
{
"serviceId":"213b6e75-691e-4df1-8d4f-52aef2970f5d"
}
{
"criteria":{
"criteriaList":[
{
"criteriaList":[
],
"expressionList":[
{
"propertyName":"hostName",
"restrictionType":"LIKE",
"propertyValues":[
{
"value":"WIN-854PACLCQ07-VC",
"relative":false
}
```

```
]
}
],
"predicateType":"AND"
},
{
"criteriaList":[
],
"expressionList":[
{
"propertyName":"riskScore",
"restrictionType":"BETWEEN",
"propertyValues":[
{
"value":0,
"relative":false
},
{
"value":100,
"relative":false
}
]
}
],
"predicateType":"OR"
}
],
"expressionList":[
],
"predicateType":"AND"
},
"sort":{
"keys":[
"riskScore"
],
"descending":true
```

```
}
}
]
```

Get Incident Alerts

The below table lists the various input parameters associated with the action **Get Incident Alerts**

Parameter	Description	Field Type	Required/Optional	Comments
Page Number	Enter the page number to get the incident alerts. For Example: **3**	Integer	Optional	
Incident ID	Enter the unique ID for the incident. For Example: **INC-100**	Text	Required	
Page Size	Enter the page size to get the maximum number of items on a page. For Example: **8**	Integer	Optional	

Example Request

```
[
{
"incident_id": "INC-34"
}
]
```

Add Journal Entry

The below table lists the various input parameters associated with the action **Add Journal Entry**

Parameter	Description	Field Type	Required/Optional	Comments
Incident ID	Enter the unique ID for the incident to add a journal entry. For Example: **INC-100**	Text	Required	
Author	Enter the NetWitness user ID of the user creating the journal entry. For Example: **exampleuser**	Text	Required	
Notes	Enter the notes and observations about the incident. For Example: **sampletext**	Text	Required	
Milestone	Enter the incident milestone classification. For Example: **Containment**	Text	Required	Allowed values: • **Containment** • **Delivery** • **Exploitation** • **Installation** • **Action on Objective** • **Eradication** • **Closure** • **Command and Control**

Example Request

```
[
{
```

```
"notes": "sampletext",
"author": "exampleuser",
"milestone": "Containment",
"incident_id": "INC-100"
}
]
```

Delete Incident

The below table lists the various input parameters associated with the action **Delete Incident**

Parameter	Description	Field Type	Required/Optional	Comments
Incident ID	Enter the unique ID for the incident. For Example: **INC-100**	Text	Required	

Example Request

```
[
{
"incident_id": "INC-28"
}
]
```

Update Incident

The below table lists the various input parameters associated with the action **Update Incident**

Parameter	Description	Field Type	Required/Optional	Comments
Status	Specify the status of the incident to update.	Text	Optional	Allowed values: • **New**

Parameter	Description	Field Type	Required/Optional	Comments
	For Example: **New**			• **Assigned** • **InProgress** • **RemediationRequested** • **RemediationComplete** • **Closed** • **ClosedFalsePositive**
Incident ID	Enter the unique ID for the incident. For Example: **INC-28**	Text	Required	
Assignee	Specify the user/assignee working on the incident. For Example: **exampleuser**	Text	Optional	

Example Request

```
[
{
"status": "Assigned",
"incident_id": "INC-28"
}
]
```

Get Incident by Date Range

The below table lists the various input parameters associated with the action **Get Incident by Date Range**

Parameter	Description	Field Type	Required/Optional	Comments
Page No	Enter the page number to get the incident details. For Example: **2**	Integer	Optional	
Since Date and Time	Enter the start time after which you want to retrieve the incidents. The timestamp should be in **ISO 8601** format. For Example: **1018-01-01T14:00:00.000Z**	Text	Required	
Page Size	Enter the maximum number of items to return on a single page. For Example: **10**	Integer	Optional	
Until Date and Time	Enter the start time after which you want to retrieve the incidents. The timestamp should be in **ISO 8601** format. For Example: **1019-01-01T14:00:00.000Z**	Text	Required	

Example Request

```
{
"since": "2021-01-01T00:00:00.000Z",
Page 32 of 35
"until": "2021-07-09T05:35:45.578Z"
}
]
```

Get Incident

The below table lists the various input parameters associated with the action **Get Incident**

Parameter	Description	Field Type	Required/Optional	Comments
Incident ID	Enter the unique ID of the incident to retrieve the details. For Example: **INC-100**	Text	Required	

Example Request

```
[
{
"incident_id": "INC-28"
}
]
```

Get Service IDs of All Services

The below table lists the various input parameters associated with the action **Get Service IDs of All Services**

Parameter	Description	Field Type	Required/Optional	Comments
Service Name	Enter the service name to retrieve the ID. For Example: **Endpoint-Server**	Text	Optional	

Example Request

```
[
{
"service_name": "Endpoint-Server"
}
]
```

© 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.