RSA NETWITNESS® SUITE

NetWitness Suite API Documentation

for Version 11.1.0.0

Contact Information

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

Trademarks

For a list of RSA trademarks, go to http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, 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 EMC.

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

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

February 2018

Table of Contents

Overview

The NetWitness Suite API can be accessed using the same host and port as the NetWitness user interface.

Current Version

By default, all requests to the REST API will automatically use the latest version of the API available. To provide API stability, clients can specify the API version to use by adding the `NetWitness-Version` HTTP header:

```
NetWitness-Version: 1.0
```

Schema

All data is sent and received as JSON. Any resources containing fields without values will have those fields included with `null` as the value instead of being omitted.

Any fields containing timestamps or dates will be in ISO 8601 format:

```
YYYY-MM-DDTHH:MM:SS.SSSZ
```

HTTP Usage

The RSA NetWitness API tries to adhere as closely as possible to standard HTTP and REST conventions in its use of HTTP verbs and status codes.

HTTP Verbs

Verb	Usage
`GET`	Used to retrieve a resource.
`POST`	Used to create a new resource.
`PATCH`	Used to update an existing resource, including partial updates. Only fields that are modified should be included in the request.
`PUT`	Used to replace an existing resource.
`DELETE`	Used to delete an existing resource.

HTTP Status Codes

Status code	Usage
`200 OK`	The request completed successfully.

`201 Created`	A new resource has been created successfully. The resource's URI is available from the response's `Location` header.
`204 No Content`	An update to an existing resource has been applied successfully.
`400 Bad Request`	The request was malformed. The response body will include an error providing further information. See Error Response.
`401 Unauthorized`	Similar to `403 Forbidden`, but specifically for use when authentication is required and has failed or has not yet been provided. See Authentication and Authorization.
`403 Forbidden`	The request was valid, but the server is refusing the action. The user might not have the necessary permissions for a resource.
`404 Not Found`	The requested resource does not exist.
`500 Internal Server Error`	An unexpected error has occurred. The response body will include a message providing further information.

Case Sensitive

All URLs, request parameters and JSON fields are case sensitive.

Error Response

A common JSON structure is always returned for errors:

Path	Type	Description
`status`	`Number`	The HTTP status code returned.
`timestamp`	`String`	The timestamp of the request.
`errors[]`	`Array`	An array of errors for the given request.
`errors[].message`	`String`	A user-friendly error message explaining what went wrong.
`errors[].field`	`String`	The field or parameter containing the error.

```
{
  "status" : 400,
  "timestamp" : "2018-02-23T18:40:52.660Z",
  "errors" : [ {
    "message" : "Value must be less than or equal to \"10\"",
    "field" : "start"
  }, {
    "message" : "Invalid range"
  } ]
}
```

Pagination

A common JSON structure is always used for paginated results:

Path	Type	Description
`items`	`Array`	An array containing the requested resources.
`pageNumber`	`Number`	The requested page number.
`pageSize`	`Number`	The requested number of items to return in a single page.
`totalPages`	`Number`	The total number of pages available.
`totalItems`	`Number`	The total number of items available.
`hasNext`	`Boolean`	Indicates if there is a page containing results after this page.
`hasPrevious`	`Boolean`	Indicates if there is a page containing results before this page.

```
{
  "items" : [ ],
  "pageNumber" : 0,
  "pageSize" : 10,
  "totalPages" : 3,
  "totalItems" : 25,
  "hasNext" : true,
  "hasPrevious" : false
}
```

Authentication and Authorization

All requests must include the `NetWitness-Token` HTTP header containing a valid JSON Web Token (JWT):

```
NetWitness-Token:
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1MTEyNDczODYyNjMsImlzcyI6InNlY3VyaXR5L
XNlcnZlci0zODA1NTA0OS0xZWMyLTQ0MDAtOTUwYS0zZTVkMmJiYTljMjIiLCJpYXQiOjE1MTEyMTEzODYyNjM
sImF1dGhvcml0aWVzIjpbIkFkbWluaXN0cmF0b3JzIl0sInVzZXJfbmFtZSI6ImFkbWluIn0.StBjg9ruIX4Fr
yfCX8qvrSBGZHF8DN3qHZM0Ei9-
thFndm1q_DLP_cnh8Fpm43fdKcs1ErcVRTqhaYvVULYmsF9ShUaSThpLts6zbJVEKlq3ldUGWWCY9bfVGRH3n5
KmWzITPi7xZ-
Rf_Kp2Sj8ecVAip3qDwha7TxYrReXefCnUj0UxgaaXjeZIFjwxFmK6NPZ7TAK9OcvcVhozaR8V92g1kUVP8_54
x7iZ2jL4JvDPaScWBjBTvVEffHNbX9_iLNoRmKqvDELSla6E_trkSREogCt6pZh709Qh70uoC3BsKwNQKbHNEO
U1tRPFaUFfRH7bCdp8v3Aeh3PTaKEuQA
```

The JSON Web Token is defined in RFC-7519. Tokens can be obtained using the methods outlined below.

In the remainder of this document, the token will be truncated to just `eyJ...AT` for brevity.

Obtaining a Token

A JSON Web Token can be obtained using the methods below.

Using a Username and Password

Users can retrieve an access token using their username and password credentials. Since the API gateway is secured using TLS, all credentials will be encrypted in transit.

```
POST /rest/api/auth/userpass
```

Request Parameters

Parameter	Description
`username`	The username of the account to authenticate.
`password`	The password of the account.

Response Fields

Path	Type	Description
`id`	`String`	The account identifier.
`roles`	`Array`	The roles assigned to the user.

Path	Type	Description
accessToken	String	A digitally signed access token that is acceptable as proof of authentication at any Launch service that trusts the public key of this service. The string holds a JSON web-token. See RFC-7519.
refreshToken	String	A digitally signed refresh token that can be used to refresh an expired access token. Refresh tokens have longer expiry periods and can be used by services to re-authenticate users without (storing and) presenting credentials.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/auth/userpass' -i -X POST \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'Content-Type: application/x-www-form-urlencoded; charset=ISO-8859-1' \
    -d 'username=ian&password=changeMe'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 23 Feb 2018 18:39:38 GMT
Content-Length: 106
```

```
{
  "id" : "ian",
  "roles" : [ "Analyst" ],
  "accessToken" : "eyJ...AT",
  "refreshToken" : "eyJ...AT"
}
```

Using a Refresh Token

Users can also retrieve an access token using a refresh token.

```
POST /rest/api/auth/token
```

Request Parameters

Parameter	Description
token	A refresh token.

Response Fields

Path	Type	Description
id	String	The account identifier.
roles	Array	The roles assigned to the user.
accessToken	String	A digitally signed access token that is acceptable as proof of authentication at any Launch service that trusts the public key of this service. The string holds a JSON web-token. See RFC-7519.
refreshToken	String	A digitally signed refresh token that can be used to refresh an expired access token. Refresh tokens have longer expiry periods and can be used by services to re-authenticate users without (storing and) presenting credentials.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/auth/token' -i -X POST \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'Content-Type: application/x-www-form-urlencoded; charset=ISO-8859-1' \
    -d
'token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1MjIwMDMxNzk3MTQsImlzcyI6InNlY3
VyaXR5LXNlcnZlci00Yzk3MDlmYS0yODYwLTQ3MTQtODQwMC0xNTZmMTA5YmI1YjciLCJpYXQiOjE1MTk0MTEx
Nzk3MTQsInJlZnJlc2giOnRydWUsInVzZXJfbmFtZSI6ImlhbiJ9.k8K8IXjnF0NGHl8tnlK5EHXKQWGljrThL
pZQGYgo0t_wFpMsfawQcZ_jo5DdFnuo6HsFb62KNXVN-
5IW1D4xwms7O4oSwLQ3tHHgLpR8qAklPuRHUC46wKcoMFv-
LVPJ7asLs3wgheWnDsSaPpD04nZmkqloDSfvSPG9LWKpLp5Xo0ibtN9owYhpxguiRdxf6GIXK50TBQRE83xdXU
0s1TcYpa8gKqxQjy1koH-bKxxACcoQ7wR76uD0Lx-
fn2y0X53k9C87JjmctYQsSv45exv8C6vuAFPyuwIuqqkNPAmHJ2dqO4Y930ipiV3IR4MKgBQW-
W4If27aZyQzEFs3hw'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 23 Feb 2018 18:39:39 GMT
Content-Length: 106
```

```
{
  "id" : "ian",
  "roles" : [ "Analyst" ],
  "accessToken" : "eyJ...AT",
  "refreshToken" : "eyJ...AT"
}
```

Authorization

In order to make requests through the NetWitness Suite API, users must belong to roles that have the `integration-server.api.access` permission, as well as any underlying permissions required to fulfill the request.

Incidents

An Incident is a logically grouped set of alerts created automatically by the Incident Aggregation Engine and grouped by a specific criteria. An Incident, available in the Respond Interface, allows an Analyst to triage, investigate, and remediate these groups of alerts. Incidents can be moved between users, notated, and explored via the nodal graph. Incidents allow users to ensure they understand the full scope of an attack or event in their NW system and then take action.

Attributes

The incident resource is comprised of the following attributes:

Path	Type	Description
`id`	`String`	The unique identifier of the incident.
`title`	`String`	The title of the incident.
`summary`	`String`	The summary of the incident.
`priority`	`String`	The incident priority. See the valid values.
`riskScore`	`Number`	The incident risk score is calculated based on the associated alert's risk score. Risk score ranges from 0 (no risk) to 100 (highest risk).
`status`	`String`	The current status. See the valid values.
`alertCount`	`Number`	The number of alerts associated with an incident.
`averageAlertRiskScore`	`Number`	The average risk score of the alerts associated with the incident. Risk score ranges from 0 (no risk) to 100 (highest risk).
`sealed`	`Boolean`	Indicates if additional alerts can be associated with an incident. A `sealed` incident cannot be associated with additional alerts.
`totalRemediationTaskCount`	`Number`	The number of total remediation tasks for an incident.
`openRemediationTaskCount`	`Number`	The number of open remediation tasks for an incident.
`created`	`String`	The timestamp of when the incident is created.
`lastUpdated`	`String`	The timestamp of when the incident was last updated.
`lastUpdatedBy`	`String`	The NetWitness user identifier of the user who last updated the incident.
`assignee`	`String`	The NetWitness user identifier of the user currently working on the incident.
`sources`	`Array`	Unique set of sources for all of the alerts in an incident.

Path	Type	Description
`ruleId`	`String`	The unique identifier of the rule that created the incident.
`firstAlertTime`	`String`	The timestamp of the earliest occurring Alert in this incident.
`categories`	`Array`	The list of categories this incident is categorized under.
`categories[].id`	`String`	The unique category identifier.
`categories[].parent`	`String`	The parent name of the category.
`categories[].name`	`String`	The friendly name of the category.
`journalEntries`	`Array`	Set of notes about the incident investigation, also known as the JournalEntry.
`journalEntries[].id`	`String`	The unique journal entry identifier.
`journalEntries[].author`	`String`	The author of this entry.
`journalEntries[].notes`	`String`	Notes and observations about the incident.
`journalEntries[].created`	`String`	The timestamp of the journal entry created date.
`journalEntries[].lastUpdated`	`String`	The timestamp of the journal entry last updated date.
`journalEntries[].milestone`	`String`	Incident milestone classifier. See the valid values.
`createdBy`	`String`	The NetWitness user id or name of the rule that created the incident.
`deletedAlertCount`	`Number`	The number of alerts that are deleted from the incident.
`eventCount`	`Number`	The number of events associated with incident.
`alertMeta`	`String`	An object containing unique set of meta values, by type, across all alerts associated with this incident.
`alertMeta.SourceIp`	`Array`	Unique source IP addresses.
`alertMeta.DestinationIp`	`Array`	Unique destination IP addresses.

Incident Priority

The `priority` field can contain these values:

Value	Description
`Low`	Low Priority
`Medium`	Medium Priority
`High`	High Priority
`Critical`	Critical

Incident Status

The `status` field can contain these values:

Value	Description
`New`	New incident.
`Assigned`	Incident is assigned to a user.
`InProgress`	Incident response is in progress.
`RemediationRequested`	Remediation tasks have been requested.
`RemediationComplete`	Remediation tasks are complete.
`Closed`	Incident is closed.
`ClosedFalsePositive`	Incident is closed as it was created due to false positive.

Milestone

Each journal entry can contain a `milestone` consisting of these values:

Value	Description
`Reconnaissance`	Intruder is in the initial phase of the attack where targets and vulnerabilities are identified.
`Delivery`	Intruder transmitted malware to the target.
`Exploitation`	Malware code triggers, which takes action on target network to exploit vulnerability.
`Installation`	Malware weapon installs access point usable by intruder.
`CommandAndControl`	Malware enables intruder to have persistent access to target network.
`ActionOnObjective`	Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.
`Containment`	Incident is contained.
`Eradication`	Necessary actions taken to eliminate components of incident and restore the system status.
`Closure`	Incident is addressed.

Requests

Get a Single Incident

A single incident can be retrieved using an incident's unique identifier.

```
GET /rest/api/incidents/{id}
```

Path Parameters

Parameter	Description
`id`	The unique identifier of the incident.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-100' -i \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 23 Feb 2018 18:42:20 GMT
Content-Length: 1329
```

```
{
  "id" : "INC-100",
  "title" : "Suspected C&C with suspicious-domain.com",
  "summary" : "Security Analytics detected communications with suspicious-domain.com
that may be command and control malware.",
  "priority" : "Critical",
  "riskScore" : 100,
  "status" : "InProgress",
  "alertCount" : 1,
  "averageAlertRiskScore" : 100,
  "sealed" : true,
  "totalRemediationTaskCount" : 4,
  "openRemediationTaskCount" : 5,
  "created" : "2018-01-01T04:49:27.870Z",
  "lastUpdated" : "2018-02-23T18:42:21.147Z",
  "lastUpdatedBy" : "norm",
  "assignee" : "ian",
  "sources" : [ "Malware Analysis" ],
  "ruleId" : "55e49a79e4b01a1d2be502bc",
  "firstAlertTime" : "2017-08-04T16:49:22Z",
  "categories" : [ {
    "id" : "55e49a79e4b01a1d2be5022e",
    "parent" : "Malware",
    "name" : "Password dumper"
  }, {
    "id" : "55e49a79e4b01a1d2be50228",
    "parent" : "Hacking",
    "name" : "Path traversal"
  } ],
  "journalEntries" : [ {
    "id" : "20",
    "author" : "admin",
    "notes" : "Updated status",
    "created" : "2017-11-15T20:20:54.785Z",
    "lastUpdated" : "2017-11-15T20:20:54.785Z",
    "milestone" : "Containment"
  } ],
  "createdBy" : "norm",
  "deletedAlertCount" : 100,
  "eventCount" : 0,
  "alertMeta" : {
    "SourceIp" : [ "10.11.12.345" ],
    "DestinationIp" : [ "11.11.11.111", "11.22.33.444" ]
  }
}
```


Get Incidents by Date Range

Incidents can be retrieved by the date and time they were created.

```
GET /rest/api/incidents
```

The requested date range can be unbounded, by only supplying either the `since` or `until` parameter, or bounded, by providing both parameters.

Request Parameters

Parameter	Description
`pageNumber`	The requested page number.
`pageSize`	The maximum number of items to return in a single page.
`since`	A timestamp in ISO 8601 format (e.g., `1018-01-01T14:00:00.000Z`). Retrieve incidents created on and after this timestamp.
`until`	A timestamp in ISO 8601 format (e.g., `1018-01-01T14:00:00.000Z`). Retrieve incidents created on and before this timestamp.

All results will be returned using the paginated response payload sorted by the `created` date, in descending order.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents?since=2018-01-
01T04%3A00%3A00.000Z&until=2018-01-01T05%3A00%3A00.000Z&pageSize=100&pageNumber=0' -i
\
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 23 Feb 2018 18:42:18 GMT
Content-Length: 1560
```

```
{
  "items" : [ {
    "id" : "INC-100",
    "title" : "Suspected C&C with suspicious-domain.com",
    "summary" : "Security Analytics detected communications with suspicious-domain.com
that may be command and control malware.",
    "priority" : "Critical",
    "riskScore" : 100,
    "status" : "Assigned",
    "alertCount" : 1,
    "averageAlertRiskScore" : 100,
```

```
    "sealed" : true,
    "totalRemediationTaskCount" : 4,
    "openRemediationTaskCount" : 5,
    "created" : "2018-01-01T04:49:27.870Z",
    "lastUpdated" : "2017-08-04T16:49:27.870Z",
    "lastUpdatedBy" : "norm",
    "assignee" : "tony",
    "sources" : [ "Malware Analysis" ],
    "ruleId" : "55e49a79e4b01a1d2be502bc",
    "firstAlertTime" : "2017-08-04T16:49:22Z",
    "categories" : [ {
      "id" : "55e49a79e4b01a1d2be5022e",
      "parent" : "Malware",
      "name" : "Password dumper"
    }, {
      "id" : "55e49a79e4b01a1d2be50228",
      "parent" : "Hacking",
      "name" : "Path traversal"
    } ],
    "journalEntries" : [ {
      "id" : "20",
      "author" : "admin",
      "notes" : "Updated status",
      "created" : "2017-11-15T20:20:54.785Z",
      "lastUpdated" : "2017-11-15T20:20:54.785Z",
      "milestone" : "Containment"
    } ],
    "createdBy" : "norm",
    "deletedAlertCount" : 100,
    "eventCount" : 0,
    "alertMeta" : {
      "SourceIp" : [ "10.11.12.345" ],
      "DestinationIp" : [ "11.11.11.111", "11.22.33.444" ]
    }
  } ],
  "pageNumber" : 0,
  "pageSize" : 100,
  "totalPages" : 1,
  "totalItems" : 1,
  "hasNext" : false,
  "hasPrevious" : false
}
```


Update an Incident

Currently an incident's `status` and `assignee` can be modified using the incidents endpoint.

```
PATCH /rest/api/incidents/{id}
```

The `assignee` field must include the unique identifier for a valid NetWitness user. The list of users can be found in the security section of the administration user interface.

Request Fields

Path	Type	Description
`status`	`String`	The current status. See the valid values.
`assignee`	`String`	The NetWitness user identifier of the user currently working on the incident.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-100' -i -X PATCH \
    -H 'NetWitness-Token: eyJ...AT' \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'Content-Type: application/json;charset=UTF-8' \
    -d '{"status":"InProgress"}'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 23 Feb 2018 18:42:20 GMT
Content-Length: 1330
```

```
{
  "id" : "INC-100",
  "title" : "Suspected C&C with suspicious-domain.com",
  "summary" : "Security Analytics detected communications with suspicious-domain.com
that may be command and control malware.",
  "priority" : "Critical",
  "riskScore" : 100,
  "status" : "InProgress",
  "alertCount" : 1,
  "averageAlertRiskScore" : 100,
  "sealed" : true,
  "totalRemediationTaskCount" : 4,
  "openRemediationTaskCount" : 5,
  "created" : "2018-01-01T04:49:27.870Z",
  "lastUpdated" : "2018-02-23T18:42:20.724Z",
  "lastUpdatedBy" : "norm",
  "assignee" : "tony",
  "sources" : [ "Malware Analysis" ],
  "ruleId" : "55e49a79e4b01a1d2be502bc",
  "firstAlertTime" : "2017-08-04T16:49:22Z",
  "categories" : [ {
    "id" : "55e49a79e4b01a1d2be5022e",
    "parent" : "Malware",
    "name" : "Password dumper"
  }, {
    "id" : "55e49a79e4b01a1d2be50228",
    "parent" : "Hacking",
    "name" : "Path traversal"
  } ],
  "journalEntries" : [ {
    "id" : "20",
    "author" : "admin",
    "notes" : "Updated status",
    "created" : "2017-11-15T20:20:54.785Z",
    "lastUpdated" : "2017-11-15T20:20:54.785Z",
    "milestone" : "Containment"
  } ],
  "createdBy" : "norm",
  "deletedAlertCount" : 100,
  "eventCount" : 0,
  "alertMeta" : {
    "SourceIp" : [ "10.11.12.345" ],
    "DestinationIp" : [ "11.11.11.111", "11.22.33.444" ]
  }
}
```


Remove an Incident

A single incident can be removed using the incident's unique identifier.

```
DELETE /rest/api/incidents/{id}
```

Path Parameters

Parameter	Description
id	The unique identifier of the incident.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-100' -i -X DELETE \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 204 No Content
Date: Fri, 23 Feb 2018 18:42:22 GMT
```

```
```

Add a Journal Entry

A journal entry, or note, can be added to an existing incident.

```
POST /rest/api/incidents/{id}/journal
```

Path Parameters

Parameter	Description
id	The unique identifier of the incident.

Request Fields

Path	Type	Description
author	String	The NetWitness user id of the user creating the journal entry.
notes	String	Notes and observations about the incident.
milestone	String	The incident milestone classifier.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-100/journal' -i -X POST \
    -H 'NetWitness-Token: eyJ...AT' \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'Content-Type: application/json;charset=UTF-8' \
    -d '{"author":"duke","notes":"This incident is
contained.","milestone":"Containment"}'
```

Sample Response

```
HTTP/1.1 201 Created
Location: https://api.netwitness.local/rest/api/incidents/INC-100
Date: Fri, 23 Feb 2018 18:42:22 GMT
```

```
```

Get an Incident's Alerts

All the alerts that are associated with an incident can be retrieved using the incident's unique identifier.

```
GET /rest/api/incidents/{id}/alerts
```

Path Parameters

Parameter	Description
id	The unique identifier of the incident.

Request Parameters

Parameter	Description
pageNumber	The requested page number.
pageSize	The maximum number of items to return in a single page.

Response Fields

Path	Type	Description
items	Array	An array containing the requested resources.
pageNumber	Number	The requested page number.
pageSize	Number	The requested number of items to return in a single page.
totalPages	Number	The total number of pages available.
totalItems	Number	The total number of items available.

Path	Type	Description
hasNext	Boolean	Indicates if there is a page containing results after this page.
hasPrevious	Boolean	Indicates if there is a page containing results before this page.
items[].id	String	The unique alert identifier.
items[].title	String	The title or name of the rule that created the alert.
items[].detail	String	The details of the alert. This can be the module name or meta that the module included.
items[].created	String	The timestamp of the alert created date.
items[].source	String	The source of this alert. For example, "Event Stream Analysis", "Malware Analysis", etc.
items[].riskScore	Number	The risk score of this alert, usually in the range 0 - 100.
items[].type	String	The type of alert, "Network", "Log", etc.
items[].events	Array	The events that make up this alert.
items[].events[].source	Object	The source of the event.
items[].events[].source.device	Object	The device contains the endpoint network information.
items[].events[].source.device.ipAddress	String	The IP address.
items[].events[].source.device.port	Number	The port.
items[].events[].source.device.macAddress	String	The ethernet MAC address.
items[].events[].source.device.dnsHostname	String	The DNS resolved hostname.
items[].events[].source.device.dnsDomain	String	The top-level domain from the DNS resolved hostname.
items[].events[].source.user	Object	The user contains the endpoint user information.
items[].events[].source.user.username	String	The unique username.
items[].events[].source.user.emailAddress	String	An email address.
items[].events[].source.user.adUsername	String	An Active Directory (AD) username.
items[].events[].source.user.adDomain	String	An Active Directory (AD) domain.
items[].events[].destination	Object	The destination of the event.
items[].events[].destination.device	Object	The device contains the endpoint network information.
items[].events[].destination.device.ipAddress	String	The IP address.

Path	Type	Description
items[].events[].destination.device.port	Number	The port.
items[].events[].destination.device.macAddress	String	The ethernet MAC address.
items[].events[].destination.device.dnsHostname	String	The DNS resolved hostname.
items[].events[].destination.device.dnsDomain	String	The top-level domain from the DNS resolved hostname.
items[].events[].destination.user	Object	The user contains the endpoint user information.
items[].events[].destination.user.username	String	The unique username.
items[].events[].destination.user.emailAddress	String	An email address.
items[].events[].destination.user.adUsername	String	An Active Directory (AD) username.
items[].events[].destination.user.adDomain	String	An Active Directory (AD) domain.
items[].events[].domain	String	The top-level domain or Windows domain.
items[].events[].eventSource	String	The source of the event. This may be a fully-qualified hostname with a port, or simple name.
items[].events[].eventSourceId	String	The unique identifier of the event on the source. For Network and Log events, this is the Nextgen Session ID.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-
100/alerts?pageSize=10&pageNumber=0' -i \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 23 Feb 2018 18:42:22 GMT
Content-Length: 1301
```


```
{
  "items" : [ {
    "id" : "5a6b81639491573f1e73676c",
    "title" : "LogOn Rule",
    "detail" : "Module_5a5cddb3e4b0ac40016df562_Alert",
```

```
    "created" : "2018-01-26T19:28:35Z",
    "source" : "Event Stream Analysis",
    "riskScore" : 90,
    "type" : "Network",
    "events" : [ {
      "source" : {
        "device" : {
          "ipAddress" : "58.229.117.56",
          "port" : 57429,
          "macAddress" : "00:13:c3:3b:c7:00",
          "dnsHostname" : null,
          "dnsDomain" : null
        },
        "user" : {
          "username" : "wwwrun",
          "emailAddress" : null,
          "adUsername" : null,
          "adDomain" : null
        }
      },
      "destination" : {
        "device" : {
          "ipAddress" : "128.164.35.184",
          "port" : 21,
          "macAddress" : "00:17:df:6b:c8:00",
          "dnsHostname" : null,
          "dnsDomain" : null
        },
        "user" : {
          "username" : "wwwrun",
          "emailAddress" : null,
          "adUsername" : null,
          "adDomain" : null
        }
      },
      "domain" : null,
      "eventSource" : "10.4.61.48:56005",
      "eventSourceId" : "9318"
    } ]
  } ],
  "pageNumber" : 0,
  "pageSize" : 10,
  "totalPages" : 1,
  "totalItems" : 1,
  "hasNext" : false,
  "hasPrevious" : false
}
```