November 2020

SIEM Events API

The SIEM Event API returns a list of event records for an account. You must configure the SIEM connector in the Absolute console to use the SIEM Event API. For information about the SIEM connector, see *Setting up integration with a SIEM application* in the online Help.

For more information about using Absolute APIs, see *Working with Absolute APIs* (https://www.absolute.com/media/2221/abt-api-working-with-absolute.pdf).

siem/events

The /v2/siem/events RESTful resource returns a list of event records and their corresponding data for events in your account during a specified time period. Each object in the list is an event record with its attributes.

Request method and URI

```
GET /v2/siem/events
```

Header	Notes	Description
Host	Required	The domain name of the server where the request is sent
Content-Type	Required	The media type of the resource
X-Abs-Date	Required	The automatically generated header that indicates the time (in UTC) the request was made encoded in a special header Formatted as: **<*YYYY*><*MM*><*DD*>T<*HH*><*MM*><*SS*>Z**
Authorization	Required	The HTTP authorization header **<*algorithm*> Credential=<*token id*>/CredentialScope, SignedHeaders=SignedHeaders, Signature=signature**

Query string parameters

The request accepts some query string parameters. The following table describes the keys defined in the request parameters.

Parameter	Type	Notes	Description
fromDate	DateTime	Required	The oldest timestamp from which events are provided. Date and time (in UTC) are formatted as **<*yyyy*>-<*MM*>-<*dd*>**T**<*HH*>:<*mm*>:<*ss*>.<*SSS*>**Z. For example: 2020-01-01T00:00:00.000Z
toDate	DateTime	Required	The latest, most recent timestamp from which events are provided. Date and time (in UTC) are formatted as **<*yyyy*>-<*MM*>-<*dd*>**T**<*HH*>:<*mm*>:<*ss*>.<*SSS*>**Z. For example: 2020-01-31T00:00:00.000Z

Parameter	Type	Notes	Description
limit	Integer	Optional	Returns the first <*n*> elements from the search where <*n*> is an integer that is greater than or equal to zero. The limit parameter has a default value as part of the definition. If the parameter is not included, the default value is used. • limit must be greater than zero • limit has a maximum value of 1000 • limit has a default value of 1000 For example, to limit the number of records to the first ten: GET /v2/siem/events?<fromDate>&**limit=10**&<toDate>
gt	String	Optional	Used as the cursor that the caller can pass to get the next page. Uses an event <*id*>. For example, to get the next page of results starting with the event <*id*> 5e55f7bdf73aa70009cb99a8: GET /v2/siem/events?<fromDate>&**gt=5e55f7bdf73aa70009cb99a8**&<limit>&<toDate>

Example

```
GET https://api.absolute.com/v2/siem/events?fromDate=2020-01-
01T00%3A00%3A00.000Z&gt=5e55f7bdf73aa70009cb99a8&limit=10&toDate=2020-01-
31T00%3A00%3A00.000Z
Host: api.absolute.com
Content-Type: application/json
X-Abs-Date: 20200325T162253Z
Authorization: ABS1-HMAC-SHA-256 Credential=b62182d4-f3b6-410f-8d1b-
2f14bb66645f/20200325/cadc/abs1, SignedHeaders=host;content-type;x-abs-date,
Signature=a799472df4e9fb2830823dc926103cbfaa8f56b1a7b6e51275534c9104bb3998
```

Request body

There is no request body.

Response

A successful request returns an HTTP status code of 200 (OK) and the response body.

Response header

Example

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
```

Response body

The following table describes the available fields for each SIEM event.

Field	Data type	Description
Event		The event that occurred.
id	String	The unique ID associated with the event.
eventDate	DateTime	The timestamp when the event occurred. Date and time (in UTC) are formatted as ***<yyyy>***-***<MM>***-***<dd>***T***<HH>***:***<mm>***:***<ss>***.***<SSS>***Z. For example: 2020-01-26T04:44:45.517Z
eventType	String	Identifies the event that occurred.
Actor		The entity that caused the event to occur.
actorObjectType	String	The type of Actor.
actorDisplayName	String	The display name of the Actor.
actorDisplayId	String	The unique ID associated with the Actor.
Object		The main entity that the Actor intended to affect by the Event.
objectObjectType	String	The type of Object.
objectDisplayName	String	The display name of the Object.
objectDisplayId	String	The unique ID associated with the Object.
objectProperties	String	The Object properties that changed. A list of tuples in one of the following forms: • propertyName, oldValue, newValue • field, value
Verb		The event that occurred.
verb	String	The event that occurred on the object.
Secondary Object		The second entity that the Actor intended to affect by the Event.
secondaryObjectType	String	The type of Secondary Object.
secondaryObjectDisplayName	String	The display name of the Secondary Object.
secondaryObjectDisplayId	String	The unique ID associated with the Secondary Object.
createdUtc	DateTime	The timestamp when the event was recorded in the database. Date and time (in UTC) are formatted as ***<yyyy>***-***<MM>***-***<dd>***T***<HH>***:***<mm>***:***<ss>***.***<SSS>***Z. For example: 2020-01-26T04:44:48.517Z

Example

NOTE The following example has been formatted for clarity. A response is returned as one string.


```
{
    "gt": "5e55f7bdf73aa70009cb99a8",
    "data": [        {
            "id": "5e55f7bdf73aa70009cb99a8",
            "eventDate": "2020-01-26T04:44:45.517Z",
            "eventType": "UserLogin",
            "actorObjectType": "User",
            "actorDisplayName": "bob@absolute.com",
            "actorDisplayId": "511073d2-d5be-4014-a6ed-650dcc1d5c58",
            "objectObjectType": "IdentityProvider",
            "objectDisplayName": "Absolute IDP",
            "objectDisplayId": "Absolute IDP",
            "objectProperties": "PropertyName[1]=IpAddress;OldValue[1]=;NewValue
[1]=10.42.0.0;PropertyName[2]=BrowserAgent;OldValue[2]=;NewValue[2]=Apache-HttpClient/4.5.3
(Java/1.8.0_111);",
            "verb": "LoggedIn",
            "secondaryObjectType": null,
            "secondaryObjectDisplayName": null,
            "secondaryObjectDisplayId": null,
            "createdUtc": "2020-01-26T04:44:48.517Z"
        }
        {
            "id": "5e65f7bdf73aa70108cb79a4",
            "eventDate": "2020-01-26T04:45:21.517Z",
            "eventType": "ScriptRequested",
            "actorObjectType": "User",
            "actorDisplayName": "bob@absolute.com",
            "actorDisplayId": "511073d2-d5be-4014-a6ed-650dcc1d5c58",
            "objectObjectType": "Device",
            "objectDisplayName": ""bob's device"",
            "objectDisplayId": "de94fa2d-0ded-4c86-9740-e955c6ec1cc1",
            "objectProperties": "PropertyName=ScriptName;OldValue=;NewValue=Add File /
Folder Permissions;"
            "verb": "Requested" ,
            "secondaryObjectType": "Request",
            "secondaryObjectDisplayName": "Request",
            "secondaryObjectDisplayId": "4478f8a0-2be1-4a8f-a98e-945cdc22b9c2",
            "createdUtc": "2020-01-27T04:44:48.517Z"
        }
    ]
}
```


Errors

The following table lists the possible status codes and messages that may be returned when using this API.

Status code	Description	Action
400 Bad Request	The ***fromDate*** is missing or invalid.	Verify and input the correct date

400 Bad Request	The ***toDate*** is missing or invalid.	Verify and input the correct date.
400 Bad Request	The ***limit*** is not a number.	Verify and input the correct integer.
400 Bad Request	The ***limit*** is less than or equal to 0.	Verify and input the correct integer.
400 Bad Request	The ***limit*** is over the maximum number of records to return.	Verify and input the correct integer.
400 Bad Request	The ***gt*** is invalid.	Verify and input the correct ***gt*** or remove the ***gt***.
401 Unauthorized	Signatures from the request and generated signature do not match.	Verify that the authorization request and authenticated headers are correct.
500 Internal Server Error	An internal server error occurred.	If the error persists, contact Absolute Technical Support (www.absolute.com/en/support).

Copyright Information