SIEM Events API

www.absolute.com
April 2024

ABSOLUTE®

SIEM Events API — Document revision: 9.0-0

Absolute Software Corporation reserves the right to revise this document and to periodically make changes in the content hereof without obligation of such revisions or changes unless required to do so by prior agreement.

Information contained herein is believed to be correct, but is provided solely for guidance in product application and not as a warranty of any kind. Absolute Software Corporation assumes no responsibility for use of this information, nor for any infringements of patents or other rights of third parties resulting from the use of this information.

Absolute Software Corporation
Suite 1400 Four Bentall Centre
1055 Dunsmuir Street
PO Box 49211
Vancouver, British Columbia
Canada V7X 1K8

NOTE Depending on the permissions associated with your API token and the Absolute product licenses associated with your account, the SIEM Event API may not be available.

The SIEM Events API returns a list of event records for an account.

IMPORTANT Before you can use this resource, you need to log in to the Absolute console, select the events to send to your Security Information and Event Management (SIEM) solution, and enable the SIEM integration. You do not need to download and install the SIEM Connector. For information, see *Setting up integration with a SIEM application* in the online Help.

NOTE SIEM events are only retained for 72 hours.

For more information about using Absolute APIs, see *Working with Absolute APIs*.

The SIEM Events API endpoint requires the following authentication headers in each request:

Authentication header parameters

Header	Notes	Description
Host	required	The domain name of the server where the request is sent Example: ***Host: api.absolute.com***
Content-Type	required	The media type of the resource Example: ***Content-Type: application/json***
X-Abs-Date	required	The automatically generated header that indicates the time (in UTC) the request was made encoded in a special header Format: ***<YYYY><MM><DD>***T***<hh><mm><ss>***Z Example: ***X-Abs-Date: 20210924T202742Z***
Authorization	required	The HTTP authorization header Format: ***<algorithm>*** Credential=***<token id>***/***<CredentialScope>***, SignedHeaders=***<SignedHeaders>***, Signature=***<signature>*** Example: ***Authorization: ABS1-HMAC-SHA-256 Credential=8b2d6fe7-0819-49b7-b29b-f565189d5e95/20210924/cadc/abs1, SignedHeaders=host;content-type;x-abs-date, Signature=f84db5f4b00d1c8beca909fdaca6356546ea6fce8b82874132df13c920d4a2c5***

Example Authentication header parameters

```
Host: api.absolute.com
Content-Type: application/json
X-Abs-Date: 20210924T202742Z
Authorization: ABS1-HMAC-SHA-256 Credential=8b2d6fe7-0819-49b7-b29b-
f565189de95/20210924/cadc/abs, SignedHeaders=host;content-type;x-abs-date,
Signature=f84db5f4b00d1c8beca909fdaca6356546ea6fce8b82874132df13c920d4a2c5
```

See Working with Absolute APIs for more information.

siem/events

The /v2/siem/events endpoint 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
```

Request

Request header

The request header consists of the resource URL, optional query parameters, and the header parameters.

Query parameters

The request accepts some query string parameters. Query string parameters need to be alphabetized and URI encoded. The following table describes the keys defined in the request parameters.

Parameter	Type	Notes	Description
fromDate	string <date-time>	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: ***2022-01-01T00:00:00.000Z***
toDate	string <date-time>	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: ***2022-01-31T00:00:00.000Z***
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>

Header parameters

The Authentication headers are required.

The following example gets the first 10 SIEM events from January 1, 2022 to January 31, 2022, starting at event id 5e55f7bdf73aa70009cb99a8.

Example GET /v2/siem/events request header

```
GET https://https://api.absolute.com/v2/siem/events?fromDate=2022-01-
01T00%3A00%3A00.000Z&gt=5e55f7bdf73aa70009cb99a8&limit=10&toDate=2022-01-
```

Example GET /v2/siem/events request header

```
31T00%3A00%3A00.000Z
Host: api.absolute.com
Content-Type: application/json
X-Abs-Date: 20220808T172059Z
Authorization: ABS1-HMAC-SHA-256 Credential=c11a9b50-1c8f-40af-a9c2-
2ef5fc7d84c3/20220808/cadc/abs1, SignedHeaders=host;content-type;x-abs-date,
Signature=582ffdfae22017e2bdfe1298f0354f79d48bbb49e3d962430d7fe56762c76222
```

Request body

The request body is an empty string.

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 using the following definitions:

- event: the event that occurred
- actor: the entity that caused the *event* to occur
- object: the main entity that the *actor* intended to affect by the *event*
- secondary object: the second entity that the *actor* intended to affect by the *event*

Parameter	Data type	Description
id	string	The unique ID associated with the *event* Example: ***5e55f7bdf73aa70009cb99a8***
eventDate	string <date-time>	The timestamp when the *event* occurred. Date and time (in UTC) are formatted as ***<yyyy>***-***<MM>***-***<dd>***T***<HH>***:***<mm>***:***<ss>***.***<SSS>***Z. Example: ***2020-01-26T04:44:45.517Z***
eventType	string	Identifies the *event* that occurred Example: ***UserLogin***
actorObjectType	string	The type of *actor* Example: ***User***
actorDisplayName	string	The display name of the *actor* Example: ***tjordan@abccompany.com***

Parameter	Data type	Description
actorDisplayId	string	The unique ID associated with the *actor* Example: ***511073d2-d5be-4014-a6ed-650dcc1d5c58***
objectObjectType	string	The type of *object* Example: ***IdentityProvider***
objectDisplayName	string	The display name of the *object* Example: ***Absolute IDP***
objectDisplayId	string	The unique ID associated with the *object* Example: ***Absolute IDP***
objectProperties	string	The *object*'s properties that changed A list of tuples in one of the following forms: • propertyName, oldValue, newValue • field, value Example: ***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	string	The *event* that occurred on the *object* Example: ***LoggedIn***
secondaryObjectType	string	The type of *secondary object* Example: ***Request***
secondaryObjectDisplayName	string	The display name of the *secondary object* Example: ***Request***
secondaryObjectDisplayId	string	The unique ID associated with the *secondary object* Example: ***4478f8a0-2be1-4a8f-a98e-945cdc22b9c2***
createdUtc	string <date-time>	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. Example: ***2020-01-26T04:44:48.517Z***

Example GET /v2/siem/events response body

```
{
    "gt": "5e55f7bdf73aa70009cb99a8",
    "data": [         {
            "id": "5e55f7bdf73aa70009cb99a8",
            "eventDate": "2020-01-26T04:44:45.517Z",
            "eventType": "UserLogin",
            "actorObjectType": "User",
            "actorDisplayName": "tjordan@abccompany.com",
            "actorDisplayId": "511073d2-d5be-4014-a6ed-650dcc1d5c58",
            "objectObjectType": "IdentityProvider",
```

Example GET /v2/siem/events response body

```
            "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": "tjordan@abccompany.com",
            "actorDisplayId": "511073d2-d5be-4014-a6ed-650dcc1d5c58",
            "objectObjectType": "Device",
            "objectDisplayName": "LPTP_Bob",
            "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
	The ***toDate*** is missing or invalid.	
	The ***limit*** is not a number.	Verify and input the correct integer.
	The ***limit*** is less than or equal to 0.	
	The ***limit*** is over the maximum number of records to return.	
	The ***gt*** is invalid.	Verify and input the correct ***gt*** or remove the ***gt***.

Status code	Description	Action
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).